AIX wersja 7.1

Bezpieczeństwo

Uwaga

Przed wykorzystaniem niniejszych informacji oraz produktu, którego one dotyczą, należy przeczytać informacje zawarte w sekcji “Uwagi” na stronie 537.

Niniejsze wydanie dotyczy systemu AIX wersja 7.1 i wszystkich późniejszych wersji i modyfikacji, o ile nowe wydania nie wskazują inaczej.

Spis treści

Informacje o podręczniku

Ta kolekcja tematów udostępnia administratorom systemu komplet informacji na temat bezpieczeństwa plików, systemu oraz sieci. Zawiera ona również informacje dotyczące takich zadań, jak wzmacnianie bezpieczeństwa systemu, modyfikowanie uprawnień oraz konfigurowanie metod uwierzytelniania i opcji Common Criteria Security Evaluation. Ta kolekcja tematów jest dostępna również na dysku CD-ROM dostarczanym razem z systemem operacyjnym.

Tekst wyróżniony

W dokumentacji przyjęto następujące konwencje wyróżniania tekstu:

Pogrubienie	Wyróżnia komendy, procedury, słowa kluczowe, pliki, struktury, katalogi i inne obiekty o nazwach predefiniowanych w systemie. Wyróżnia także obiekty graficzne, takie jak przyciski, etykiety i ikony, które wybiera użytkownik.
Kursywa	Wyróżnia parametry, których bieżące nazwy lub wartości mają zostać podane przez użytkownika.
`Czcionka o stałej szerokości`	Oznacza przykłady określonych wartości danych, przykłady tekstu podobnego do tego, który można zobaczyć na ekranie, przykłady fragmentów kodu programu, który mogą napisać programiści, komunikaty systemowe lub informacje, które należy wpisać.

Rozróżnianie wielkości liter w systemie AIX

W systemie AIX rozróżniane są wielkości liter, co oznacza, że system odróżnia wielkie litery od małych. Na przykład do przeglądania plików można użyć komendy **ls**. Jeśli wprowadzona zostanie komenda LS, system zwróci komunikat `is not found` (nie znaleziono). Podobnie **PLIK_A**, **Plik_A** i **plik_a** są trzema różnymi plikami, nawet jeśli znajdują się w tym samym katalogu. Aby uniknąć niepożądanego działania systemu, należy zawsze upewnić się, że używana jest poprawna wielkość liter.

ISO 9000

Podczas tworzenia i rozwijania tego produktu używano systemów z certyfikatem jakości ISO 9000.

Bezpieczeństwo

System operacyjny AIX umożliwia wykonywanie takich zadań, jak podnoszenie bezpieczeństwa systemu, modyfikowanie uprawnień oraz konfigurowanie metod uwierzytelniania i opcji Common Criteria Security Evaluation.

Informacje pokrewne

Computer Emergency Response Team na uniwersytecie Carnegie Mellon University (CERT)

FIRST (Forum of Incident Response and Security Teams)

CERIAS (Center for Education and Research in Information Assurance and Security)

Bezpieczeństwo — Co nowego

W tym miejscu wskazano nowe i znacznie zmienione informacje dotyczące kolekcji tematów związanych z bezpieczeństwem.

Znajdowanie nowych lub zmienionych informacji

Aby ułatwić rozpoznanie zmian technicznych, w Centrum informacyjnym użyto:

- oznaczenia >| wskazującego miejsce, gdzie się one rozpoczynają,
- oznaczenia |< wskazującego koniec nowych lub zmienionych informacji.

Czerwiec 2019

Poniżej zamieszczono podsumowanie aktualizacji w tej dokumentacji:

- W sekcji “Filtry IP dla systemu AIX” na stronie 260 zaktualizowano informacje na temat używania oprogramowania filtru IP.

Sierpień 2018

Poniżej zamieszczono podsumowanie aktualizacji w tej dokumentacji:

- W następujących tematach zaktualizowano informacje na temat konfigurowania systemu jako serwera informacji o bezpieczeństwie LDAP.
  - Konfigurowanie serwera IBM Security Directory Server
  - Konfigurowanie klienta LDAP
  - Konfigurowanie warstwy SSL na kliencie LDAP
  - Konta tworzone przez komponenty zabezpieczeń
  - Zarządzanie użytkownikami LDAP

Zabezpieczenie podstawowego systemu operacyjnego

Część dotycząca zabezpieczenia podstawowego systemu operacyjnego zawiera informacje na temat sposobów zabezpieczania systemów niezależnie od tego, czy są one podłączone do sieci.

Ta sekcja zawiera opis instalowania systemu z włączonymi opcjami zabezpieczeń oraz sposoby zabezpieczania systemu AIX przed nieuprawnionymi użytkownikami.

Instalowanie i konfigurowanie bezpiecznego systemu

Na bezpieczeństwo instalacji i konfiguracji systemu AIX wpływa kilka czynników.

Zaufana Baza Przetwarzania
Administrator systemu musi ustalić, jak wysoki poziom zaufania przypisać danemu programowi. Decyzja ta obejmuje rozważenie wartości zasobów informacji w systemie i ustalenie, jak wysoki poziom zaufania jest wymagany dla danego programu, aby możliwe było jego zainstalowanie z określonymi uprawnieniami.

Zaufana Baza Przetwarzania (Trusted Computing Base - TCB) jest częścią systemu odpowiedzialną za wprowadzanie w systemie strategii zabezpieczeń informacji. Poprzez zainstalowanie i uruchomienie TCB można zdefiniować dostęp użytkownika do zaufanej ścieżki komunikacyjnej, co umożliwia nawiązanie bezpiecznej komunikacji między użytkownikami a TCB. Funkcje TCB można włączyć tylko wtedy, gdy zainstalowany jest system operacyjny. Aby zainstalować TCB na komputerze z zainstalowanym systemem operacyjnym, należy przeprowadzić instalację zachowującą. Włączenie TCB zapewnia dostęp do zaufanej powłoki, zaufanych procesów i sekwencji przywołania bezpiecznej komunikacji (Secure Attention Key - SAK).

Sprawdzanie bazy TCB
System operacyjny jest narażony na niebezpieczeństwo, gdy pliki Zaufanej Bazy Przetwarzania (Trusted Computing Base - TCB) nie są prawidłowo zabezpieczone lub gdy pliki konfiguracyjne zawierają niezabezpieczone wartości.

Komenda **tcbck** kontroluje stan bezpieczeństwa Zaufanej Bazy Przetwarzania. Komenda **tcbck** kontroluje te informacje przez odczytywanie pliku `/etc/security/sysck.cfg`. Ten plik zawiera opis wszystkich plików bazy TCB, plików konfiguracyjnych i zaufanych komend.

Plik `/etc/security/sysck.cfg` nie znajduje się w trybie bez połączenia i dlatego może zostać zmieniony przez hakera. Każdorazowo po aktualizacji bazy TCB należy utworzyć kopię pliku w trybie bez połączenia i tylko do odczytu. Ponadto przed wykonaniem jakichkolwiek sprawdzeń należy skopiować ten plik z nośnika archiwalnego na dysk.

Struktura pliku sysck.cfg
Komenda **tcbck** odczytuje plik `/etc/security/sysck.cfg` w celu określenia, które pliki muszą zostać sprawdzone. Każdy zaufany program w systemie jest opisany w jednej sekcji w pliku `/etc/security/sysck.cfg`.

W każdej sekcji określone są następujące atrybuty:

Atrybut	Opis
acl	Łańcuch tekstowy oznaczający listę kontroli dostępu do pliku. Musi mieć taki sam format, jak dane wyjściowe z komendy **aclget**. Jeśli nie jest on zgodny z bieżącą listą ACL pliku, komenda **sysck** ustawia tę wartość za pomocą komendy **aclput**. **Uwaga:** Atrybuty SUID, SGID i SVTX muszą odpowiadać atrybutom określonym dla trybu, jeśli zostały podane.
class	Nazwa grupy plików. Ten atrybut umożliwia sprawdzenie kilku plików mających taką samą nazwę klasy przez określenie jednego argumentu w komendzie **tcbck**. Można określić kilka klas, oddzielając je przecinkami.
group	Identyfikator grupy lub nazwa grupy pliku. Jeśli wartość parametru nie jest zgodna z grupą pliku, komenda **tcbck** ustawia identyfikator grupy pliku na tę wartość.
links	Lista nazw ścieżek dowiązanych do tego pliku rozdzielonych przecinkami. Jeśli którakolwiek z nazw ścieżek nie jest do niego dowiązana, komenda **tcbck** utworzy dowiązanie. Jeśli parametr *tree* nie zostanie użyty, komenda **tcbck** wydrukuje komunikat o tym, że istnieją dodatkowe dowiązania, ale nie określi ich nazw. Jeśli parametr *tree* zostanie użyty, komenda **tcbck** wydrukuje również wszelkie dodatkowe nazwy ścieżek dowiązane do tego pliku.

Atrybut	Opis
mode	Lista wartości rozdzielonych przecinkami. Dozwolone wartości to: SUID, SGID, SVTX i TCB. Uprawnienia do pliku muszą być ostatnią wartością i można je określić w postaci liczby ósemkowej lub łańcucha 9-znakowego. Na przykład zarówno uprawnienie 755, jak i rwxr-xr-x jest poprawnym uprawnieniem do pliku. Jeśli wartość parametru nie odpowiada bieżącemu trybowi pliku, komenda **tcbck** ustawi prawidłową wartość.
owner	Identyfikator użytkownika lub nazwa właściciela pliku. Jeśli wartość parametru nie jest zgodna z właścicielem pliku, komenda **tcbck** ustawia jego identyfikator na tę wartość.
program	Lista wartości rozdzielonych przecinkami. Pierwsza wartość jest nazwą ścieżki programu sprawdzającego. Dodatkowe wartości są przekazywane jako argumenty do programu w chwili jego uruchomienia. **Uwaga:** Pierwszym argumentem zawsze jest argument *-y*, *-n*, *-p* lub *-t*, w zależności od tego, z którą opcją została użyta komenda **tcbck**.
source	Nazwa pliku, z którego ma zostać skopiowany ten plik źródłowy przed sprawdzeniem. Jeśli wartość nie zostanie określona, a jest to zwykły plik, katalog lub potok nazwany, zostanie utworzona, jeśli jeszcze nie istnieje, nowa pusta wersja tego pliku. W przypadku plików urządzeń zostanie utworzony nowy plik specjalny dla urządzenia o tym samym typie.
symlinks	Lista nazw ścieżek dowiązanych symbolicznie do tego pliku rozdzielonych przecinkami. Jeśli którakolwiek z nazw ścieżek nie jest dowiązaniem symbolicznym do pliku, komenda **tcbck** utworzy takie dowiązanie. Jeśli argument *tree* zostanie użyty, komenda **tcbck** wydrukuje również wszelkie dodatkowe nazwy ścieżek dowiązanych symbolicznie do tego pliku.

Jeśli w sekcji w pliku `/etc/security/sysck.cfg` jakiś atrybut nie zostanie podany, odpowiadające mu sprawdzenie nie zostanie wykonane.

Korzystanie z komendy tcbck

Celem użycia komendy **tcbck** jest zapewnienie właściwej instalacji plików wykorzystywanych przez zabezpieczenia, zapewnienie, że drzewo systemu plików nie zawiera plików jawnie naruszających bezpieczeństwo systemu, oraz aktualizowanie, dodawanie lub usuwanie zaufanych plików.

Komenda **tcbck** jest używana zazwyczaj do wykonywania następujących zadań:

- zapewnienia prawidłowej instalacji plików wykorzystywanych przez zabezpieczenia,
- zapewnienia, że drzewo systemu plików nie zawiera plików, które jawnie naruszają bezpieczeństwo systemu,
- aktualizacji, dodawania lub usuwania zaufanych plików.

Komenda **tcbck** może zostać użyta w następujący sposób:

- korzystanie normalne
  - nieinteraktywne, podczas inicjowania systemu,
  - przy użyciu komendy **cron**,
- korzystanie interaktywne
  - sprawdzanie indywidualnych plików i klas plików,
- korzystanie paranoiczne
  - przechowywanie pliku `sysck.cfg` w trybie bez połączenia i okresowe jego odtwarzanie w celu sprawdzenia komputera.

Baza TCB używa komendy **sum** do tworzenia sum kontrolnych, mimo iż nie jest to bezpieczne z punktu widzenia kryptografii. Bazy danych TCB mogą zostać skonfigurowane ręcznie przy użyciu innych komend sum kontrolnych, na przykład komendy **md5sum** (dostarczonej razem z pakietem textutils RPM Package Manager na dysku CD *Toolbox for Linux Applications*).

Sprawdzanie zaufanych plików
Komenda **tcbck** umożliwia sprawdzenie i naprawę wszystkich plików w bazie danych tcbck oraz naprawę i zaprotokołowanie wszystkich błędów.

Aby sprawdzić wszystkie pliki w bazie danych tcbck, a następnie naprawić i wydrukować wszystkie błędy, należy wpisać:

```
tcbck -y ALL
```

Spowoduje to, że komenda **tcbck** sprawdzi instalację każdego pliku w bazie danych tcbck, który jest opisany w pliku `/etc/security/sysck.cfg`.

Aby wykonać tę czynność automatycznie podczas inicjowania systemu i utworzyć protokół błędów, należy dodać powyższy łańcuch komendy do komendy **/etc/rc**.

Sprawdzanie drzewa systemu plików
W przypadku podejrzenia, że integralność systemu mogła zostać naruszona, należy uruchomić komendę **tcbck**, aby sprawdzić drzewo systemu plików.

Aby sprawdzić drzewo systemu plików, należy wpisać:

```
tcbck -t tree
```

Jeśli komenda **tcbck** zostanie użyta z wartością *tree*, wszystkie pliki w systemie zostaną sprawdzone pod kątem prawidłowej instalacji (może to chwilę potrwać). Jeśli komenda **tcbck** wykryje, że niektóre pliki mogą stanowić zagrożenie dla bezpieczeństwa systemu, można zmodyfikować podejrzany plik w celu usunięcia atrybutu, który to powoduje. Ponadto na wszystkich innych plikach w systemie plików są wykonywane poniższe sprawdzenia:

- jeśli właścicielem pliku jest użytkownik root i plik ma ustawiony bit SetUID, bit SetUID zostanie usunięty,
- jeśli grupa pliku jest grupą administracyjną, plik jest wykonywalny i ma ustawiony bit SetGID, bit SetGID zostanie usunięty,
- jeśli plik ma ustawiony atrybut **tcb**, ustawienie tego atrybutu zostanie usunięte,
- jeśli plik jest urządzeniem (znakowym lub blokowym plikiem specjalnym), zostanie usunięty,
- jeśli plik jest dodatkowym dowiązaniem do nazwy ścieżki opisanym w pliku `/etc/security/sysck.cfg`, dowiązanie zostanie usunięte,
- jeśli plik jest dodatkowym dowiązaniem symbolicznym do nazwy ścieżki opisanym w pliku `/etc/security/sysck.cfg`, dowiązanie symboliczne zostanie usunięte.

  Uwaga: Wszystkie wpisy urządzeń muszą zostać dodane do pliku `/etc/security/sysck.cfg` przed wykonaniem komendy **tcbck**, inaczej nie będzie można używać systemu. Aby dodać zaufane urządzenia do pliku `/etc/security/sysck.cfg`, należy użyć opcji **-l**.

Ostrzeżenie: *Nie należy* uruchamiać opcji **tcbck -y tree**. Opcja ta powoduje usunięcie i wyłączenie urządzeń, które nie mają prawidłowych wpisów w bazie TCB i może zablokować system.

Dodawanie zaufanego programu
Komenda **tcbck** umożliwia dodanie określonego programu do pliku `/etc/security/sysck.cfg`.

Aby dodać określony program do pliku `/etc/security/sysck.cfg`, należy wpisać:

```
tcbck -a NazwaŚcieżki [atrybut=wartość]
```

Jedynie atrybuty, których wartości nie są ustawiane na podstawie stanu bieżącego, muszą być określone w wierszu komend. Wszystkie nazwy atrybutów są zawarte w pliku `/etc/security/sysck.cfg`.

Na przykład następująca komenda rejestruje nowy program SetUID o nazwie /usr/bin/setgroups, który ma dowiązanie o nazwie /usr/bin/getgroups:

```
tcbck -a /usr/bin/setgroups links=/usr/bin/getgroups
```

Aby dodać użytkowników jfh i jsl jako użytkowników administracyjnych oraz dodać grupę developers jako grupę administracyjną, która ma zostać sprawdzona podczas kontroli bezpieczeństwa pliku /usr/bin/abc, należy wpisać:

```
tcbck -a /usr/bin/abc setuids=jfh,jsl setgids=developers
```

Po zainstalowaniu programu może nie być wiadomo, jakie nowe pliki są zarejestrowane w pliku /etc/security/sysck.cfg. Można je odszukać i dodać za pomocą następującej komendy:

```
tcbck -t tree
```

Ten łańcuch komendy powoduje wyświetlenie nazwy każdego pliku, który ma zostać zarejestrowany w pliku /etc/security/sysck.cfg.

Usuwanie zaufanego programu
Jeśli z systemu zostanie usunięty plik, który jest opisany w pliku /etc/security/sysck.cfg, należy usunąć jego opis również z pliku /etc/security/sysck.cfg.

Na przykład, jeśli usunięto program /etc/cvid, poniższa komenda spowoduje wyświetlenie komunikatu o błędzie:

```
tcbck -t ALL
```

Końcowy komunikat o błędzie brzmi następująco:

```
3001-020 Plik /etc/cvid nie został znaleziony.
```

Opis dla tego programu znajduje się w pliku /etc/security/sysck.cfg . Aby usunąć ten opis, należy wpisać następującą komendę:

```
tcbck -d /etc/cvid
```

Konfigurowanie dodatkowych zaufanych opcji
Istnieje możliwość skonfigurowania dodatkowych opcji Zaufanej Bazy Przetwarzania (TCB).

Ograniczanie dostępu do terminalu
System operacyjny można skonfigurować w taki sposób, aby ograniczał dostęp do terminali.

Komendy **getty** i **shell** powodują zmianę właściciela i trybu terminalu, co uniemożliwia niezaufanym programom dostęp do terminalu. System operacyjny daje możliwość skonfigurowania wyłącznego dostępu do terminalu.

Korzystanie z sekwencji przywołania bezpiecznej komunikacji
Zaufaną ścieżkę komunikacyjną można ustanowić przez naciśnięcie zastrzeżonej sekwencji przywołania bezpiecznej komunikacji (Secure Attention Key - SAK) (Ctrl-X, a następnie Ctrl-R).

Uwaga: Należy zachować ostrożność podczas używania sekwencji SAK, ponieważ powoduje ona zatrzymanie wszystkich procesów, które próbują uzyskać dostęp do terminalu, i wszystkich dowiązań do nich (na przykład /dev/console może być dowiązany do /dev/tty0).

Jest to możliwe po spełnieniu następujących warunków:

- Podczas logowania się do systemu.

  Po naciśnięciu sekwencji SAK:

  – Jeśli zostanie wyświetlony nowy ekran logowania, oznacza to, że zaufana ścieżka została ustanowiona.

  - Jeśli zostanie wyświetlona zachęta zaufanej powłoki, oznacza to, że ekran logowania był nieautoryzowanym programem, który mógł próbować dokonać kradzieży hasła. Należy określić, kto obecnie używa tego terminalu, za pomocą komendy **who**, a następnie wylogować się.
- W przypadku, gdy wprowadzona komenda ma uruchomić zaufany program. Niektóre przykłady takiego użycia są następujące:
  - Uruchamianie jako użytkownik root. Jako użytkownik root można uruchamiać programy tylko po ustanowieniu zaufanej ścieżki komunikacyjnej. Daje to pewność, że żadne niezaufane programy nie zostaną uruchomione z uprawnieniami użytkownika root.
  - Uruchamianie komend **su**, **passwd** i **newgrp**. Komendy te można uruchomić tylko po ustanowieniu zaufanej ścieżki komunikacyjnej.

Konfigurowanie sekwencji przywołania bezpiecznej komunikacji
Konfigurowanie sekwencji przywołania bezpiecznej komunikacji (Secure Attention Key - SAK) w celu utworzenia zaufanej ścieżki komunikacyjnej.

Każdy terminal może być skonfigurowany niezależnie, tak aby naciśnięcie sekwencji SAK (Secure Attention Key) w danym terminalu powodowało utworzenie zaufanej ścieżki komunikacyjnej. Można to określić za pomocą atrybutu **sak_enabled** w pliku `/etc/security/login.cfg`. Jeśli wartość atrybutu jest ustawiona na True, sekwencja SAK jest włączona.

Jeśli do komunikacji ma zostać użyty port (na przykład w przypadku komendy **uucp**), użytemu portowi odpowiada następujący wiersz w jego sekcji w pliku `/etc/security/login.cfg`:

```
sak_enabled = false
```

Ten wiersz (lub brak wpisu w tej sekcji) powoduje wyłączenie sekwencji SAK dla tego terminalu.

Aby włączyć sekwencję SAK w terminalu, należy dodać następujący wiersz do sekcji dla tego terminalu:

```
sak_enabled = true
```

Zaufane wykonywanie
Zaufane wykonywanie (Trusted Execution - TE) odnosi się do kolekcji opcji używanych do sprawdzania poprawności systemu i implementowania zaawansowanych strategii bezpieczeństwa, razem służących do zwiększenia poziomu zaufania całego systemu.

Standardową metodą naruszenia systemu przez złośliwego użytkownika jest uzyskanie dostępu do systemu i zainstalowanie plików programów typu koń trojański, pakietów plików użytkownika root lub sfałszowanie pewnych plików newralgicznych dla bezpieczeństwa. W wyniku tych działań system staje się wrażliwy na ataki i wykorzystanie. Kluczową ideą zebrania zestawu opcji w mechanizm TE jest zapobieganie takiej działalności, a w najgorszym razie zidentyfikowanie, że taki incydent zdarzył się w systemie. Korzystając z funkcjonalności zapewnianej przez TE, administrator systemu może podjąć decyzję, jaki ma być faktyczny zestaw programów wykonywalnych, których wykonywanie jest dozwolone lub które zestawy rozszerzeń jądra mogą zostać załadowane. Ponadto opcje TE mogą służyć do kontroli stanu bezpieczeństwa systemu oraz do identyfikowania plików, które zostały zmienione, tym samym zwiększając poziom zaufania systemu i utrudniają złośliwemu użytkownikowi naruszenie integralności systemu. Zestaw opcji zgromadzonych jako TE można pogrupować następująco:

- Zarządzanie bazą danych zaufanych podpisów
- Kontrola integralności bazy danych zaufanych podpisów
- Konfigurowanie strategii bezpieczeństwa
- Zaufane ścieżki wykonywania i Zaufane ścieżki bibliotek

Uwaga: Funkcjonalność TCB już istnieje w systemie operacyjnym AIX. Zaufane wykonywanie jest mocniejszym i bardziej rozbudowanym mechanizmem, pokrywającym się z niektórymi funkcjonalnościami bazy TCB i udostępniającym zaawansowane strategie bezpieczeństwa do lepszej kontroli integralności systemu. Baza TCB jest nadal dostępna, ale mechanizm TE wprowadza nowe i bardziej zaawansowane możliwości sprawdzania poprawności i ochrony integralności systemu.

Zarządzanie bazą danych zaufanych podpisów
Jest to baza danych podobna do Zaufanej Bazy Przetwarzania (TCB), służąca do przechowywania newralgicznych parametrów bezpieczeństwa zaufanych plików w systemie. Nazywa się ją bazą danych zaufanych podpisów, a znajduje się ona w pliku `/etc/security/tsd/tsd.dat`.

Plik zaufany to plik newralgiczny z punktu widzenia bezpieczeństwa systemu i naruszenie jego ochrony może zagrozić bezpieczeństwu całego systemu. Zwykle pliki pasujące do tego opisu są następujące:

- Jądro (system operacyjny).
- Wszystkie programy z bitem wykonania z uprawnieniami właściciela użytkownika root.
- Wszystkie programy z bitem wykonania z uprawnieniami właściciela grupowego użytkownika root.
- Wszystkie programy uruchamiane wyłącznie przez użytkownika root lub użytkownika należącego do grupy system.
- Wszystkie programy, które muszą być uruchomione przez administratora, znajdujące się w zaufanej ścieżce komunikacyjnej (na przykład komenda **ls**).
- Pliki konfiguracyjne sterujące działaniem systemu.
- Wszystkie programy uruchamiane z uprawnieniami lub prawami dostępu do zmiany jądra lub plików konfiguracyjnych systemu.

Najlepiej byłoby, gdyby każdy plik zaufany miał powiązaną sekcję lub definicję pliku przechowywaną w bazie danych zaufanych podpisów (TSD). Plik można oznaczyć jako zaufany przez dodanie jego definicji do bazy danych TSD przy użyciu komendy **trustchk**. Komenda **trustchk** umożliwia dodawanie, usuwanie i wyświetlanie wpisów bazy danych TSD.

Baza danych zaufanych podpisów
Baza danych zaufanych podpisów służy do przechowywania newralgicznych parametrów bezpieczeństwa zaufanych plików w systemie. Znajduje się ona w katalogu `/etc/security/tsd/tsd.dat`.

Najlepiej byłoby, gdyby każdy plik zaufany miał powiązaną sekcję lub definicję pliku przechowywaną w bazie danych zaufanych podpisów (TSD). Każdy plik zaufany jest powiązany z unikalną szyfrującą wartością mieszającą i podpisem cyfrowym. Szyfrująca wartość mieszająca domyślnego zestawu plików zaufanych jest generowana algorytmem SHA-256, a podpis cyfrowy jest generowany algorytmem RSA przez środowisko budowania systemu AIX; są one pakowane razem z zestawami plików instalacyjnych systemu AIX. Wartości mieszające i podpisy są dostarczane wraz z odpowiednimi obrazami instalacyjnymi systemu AIX i przechowywane w bazie danych zaufanego oprogramowania (`/etc/security/tsd/tsd.dat`) komputera docelowego, w postaci sekcji, podobnych do przedstawionych poniżej:

```
/usr/bin/ps:
           owner          = bin
           group          = system
           mode           = 555
           type           = FILE
           hardlinks      = /usr/sbin/ps
           symlinks       =
           size           = 1024
           cert_tag       = bbe21b795c550ab243
           signature      =
f7167eb9ba3b63478793c635fc991c7e9663365b2c238411d24c2a8a
           hash_value     = c550ab2436792256b4846a8d0dc448fc45
           minslabel      = SLSL
           maxslabel      = SLSL
           intlabel       = SHTL
           accessauths    = aix.mls.pdir, aix.mls.config
           innateprivs    = PV_LEF
           proxyprivs     = PV_DAC
           authprivs      =
aix.security.cmds:PV_DAC,aix.ras.audit:PV_AU_ADMIN
           secflags       = FSF_EPS
           t_accessauths  =
           t_innateprivs  =
           t_proxyprivs   =
           t_authprivs    =
           t_secflags     =
```

owner (właściciel)
Właściciel pliku. Wartość jest wyliczana przy użyciu komendy **trustchk** w momencie dodawania pliku do bazy TSD.

group (grupa)
Grupa pliku. Wartość jest wyliczana przy użyciu komendy **trustchk**.

mode (tryb)
Lista wartości rozdzielonych przecinkami. Dopuszczalne wartości: **SUID** (bit ustawienia SUID), **SGID** (bit ustawienia SGID), **SVTX** (bit ustawienia SVTX) i **TCB** (Zaufana Baza Przetwarzania). Uprawnienia do pliku muszą być ostatnią wartością i można je podać w postaci liczby ósemkowej. Na przykład dla pliku z ustawionym bitem **uid** i bitami uprawnień **rwxr-xr-x** wartość trybu wynosi **SUID,755**. Wartość jest wyliczana komendą **trustchk**.

type (typ)
Typ pliku. Wartość jest wyliczana przy użyciu komendy **trustchk**. Dopuszczalne wartości: **FILE**, **DIRECTORY**, **MPX_DEV**, **CHAR_DEV**, **BLK_DEV** i **FIFO**.

hardlinks (dowiązania stałe)
Lista dowiązań stałych do pliku. Ta wartość nie może być wyliczona przy użyciu komendy **trustchk**. Musi być dostarczona przez użytkownika w momencie dodawania pliku do bazy danych.

symlinks (dowiązania symboliczne)
Lista dowiązań symbolicznych do pliku. Ta wartość nie może być wyliczona przy użyciu komendy **trustchk**. Musi być dostarczona przez użytkownika w momencie dodawania pliku do bazy danych.

size (wielkość)
Definiuje wielkość pliku. Wpisanie wartości **VOLATILE** oznacza, że plik będzie się często zmieniał.

cert_tag (znacznik certyfikacji)
To pole odwzorowuje podpis cyfrowy pliku z powiązanym certyfikatem, który może służyć do sprawdzenia poprawności podpisów pliku. W tym polu jest przechowywany identyfikator certyfikatu, jest ono wyliczane przy użyciu komendy **trustchk** w momencie dodawania pliku do bazy TSD. Certyfikaty są przechowywane w katalogu `/etc/security/certificates`.

signature (podpis)
Podpis cyfrowy pliku. Wpisanie wartości **VOLATILE** oznacza, że plik będzie się często zmieniał. Pole jest wyliczane przy użyciu komendy **trustchk**.

hash_value (wartość mieszająca)
Szyfrująca wartość mieszająca pliku. Wpisanie wartości **VOLATILE** oznacza, że plik będzie się często zmieniał. Pole jest wyliczane przy użyciu komendy **trustchk**.

minslabel (etykieta minimum)
Definiuje etykietę czułości minimalnej obiektu.

maxslabel (etykieta maksimum)
Definiuje etykietę czułości maksymalnej obiektu (wartość poprawna w systemie Trusted AIX). Atrybut nie dotyczy zwykłych plików i kolejek FIFO.

intlabel (etykieta integralności)
Definiuje etykietę integralności obiektu (wartość poprawna w systemie Trusted AIX).

accessauths (uprawnienia dostępu)
Definiuje autoryzację dostępu dla obiektu (wartość poprawna w systemie Trusted AIX).

innateprivs (uprawnienia wrodzone)
Definiuje uprawnienia wrodzone pliku.

proxyprivs (uprawnienia proxy)
Definiuje uprawnienia proxy pliku.

authprivs (uprawnienia autoryzowane)
Definiuje uprawnienia przypisane użytkownikowi po nadaniu autoryzacji.

secflags (opcje bezpieczeństwa)
Definiuje opcje bezpieczeństwa pliku powiązane z obiektem.

t_accessauth (autoryzacje dostępu Trusted)
Definiuje dodatkowe autoryzacje dostępu dla modelu Trusted AIX z Multi-Level Security (MLS) (wartość poprawna w systemie Trusted AIX).

t_inateprivs (uprawnienia wrodzone Trusted)
Definiuje dodatkowe uprawnienia wrodzone pliku dla modelu Trusted AIX z MLS-specific (wartość poprawna w systemie Trusted AIX).

t_proxyprivs (uprawnienia proxy Trusted)
Definiuje dodatkowe uprawnienia proxy pliku dla modelu Trusted AIX z MLS-specific (wartość poprawna w systemie Trusted AIX).

t_authprivs (dodatkowe uprawnienia Trusted)
Definiuje dodatkowe uprawnienia dla modelu Trusted AIX z MLS-specific, które są przypisywane użytkownikowi po nadaniu autoryzacji (wartość poprawna w systemie Trusted AIX).

t_secflags (opcje bezpieczeństwa Trusted)
Definiuje dodatkowe opcje bezpieczeństwa powiązane z obiektem dla modelu Trusted AIX z MLS-specific (wartość poprawna w systemie Trusted AIX).

W momencie dopisywania pozycji w bazie TSD, jeśli do pliku zaufanego istnieją jakieś dowiązania symboliczne lub stałe, należy dodać je do bazy TSD, używając atrybutów **symlinks** i **hardlinks** w wierszu komend z komendą **trustchk**. Jeśli dodawany plik ma się często zmieniać, należy użyć w wierszu komend słowa kluczowego VOLATILE. Wtedy komenda **trustchk** nie obliczy wartości pól **hash_value** i **signature** w momencie generowania definicji pliku w celu dodania do bazy TSD. Podczas sprawdzania integralności pliku pola **hash_value** i **signature** są ignorowane.

Podczas dodawania definicji zwykłego pliku do bazy TSD konieczne jest podanie klucza prywatnego (w formacie ASN.1/DER). Należy użyć opcji **-s** i certyfikatu cyfrowego wraz z odpowiednim kluczem publicznym, używając opcji **-v**. Klucz prywatny posłuży do wygenerowania podpisu pliku i zostanie usunięty. Bezpieczne przechowanie tego klucza jest sprawą użytkownika. Certyfikat jest przechowywany w bazie certyfikatów w pliku `/etc/security/certificates` w celu weryfikowania podpisów po każdym żądaniu weryfikacji integralności. Obliczenie podpisu nie jest możliwe dla plików innych niż zwykłe (np. katalogów i plików urządzeń), dlatego podczas dodawania takich plików do bazy TSD podanie klucza prywatnego i certyfikatu nie jest obowiązkowe.

Do bazy TSD można również dopisać ustaloną wcześniej definicję pliku zawartą w pliku, w tym celu należy użyć opcji **-f**. W takim przypadku komenda **trustchk** nie wylicza żadnych wartości i zachowa definicje w bazie TSD bez ich weryfikacji. Za poprawność tych definicji plików jest odpowiedzialny użytkownik.

Obsługa weryfikacji bibliotek

Aby zapewnić obsługę weryfikacji bibliotek, w katalogu `/etc/security/tsd/lib/` dostępny jest plik `tsd.dat`. Nazwą bazy danych jest `/etc/security/tsd/lib/lib.tsd.dat`. Ta baza danych jest przeznaczona dla bibliotek i sekcji dla plików `.o` odpowiednich zaufanych bibliotek. Sekcja dla każdego pliku `.o` biblioteki jest w formacie podanym poniżej.

Dla biblioteki `libc.a`, jeśli jednym z plików `.o` jest plik `strcmp.o`, to sekcja dla pliku `strcmp.o` w pliku `/etc/security/tsd/lib/lib.tsd.dat` jest podobna do następującego przykładu:

```
/usr/lib/libc.a/strcmp.o:
            Type = OBJ
            Size = 2345
            Hash value
            Signature =
            Cert_tag =
```

Ta baza danych zawiera pozycje odpowiadające parametrom **type** (typ), **size hash** (wartość mieszająca wielkości), **cert tag** (znacznik certyfikacji) i **signature** (podpis) pliku `.o`. Ścieżka biblioteki jest aktualizowana w pliku `/etc/security/tsd/tsd.dat` w odpowiedniej sekcji. Wartości te są dynamicznie generowane podczas kompilacji i przenoszone do bazy danych `/etc/security/tsd/lib/lib.tsd.dat` podczas instalowania.

W pliku `/etc/security/tsd/tsd.dat` sekcje bibliotek są modyfikowane, tak aby atrybut **type** miał wartość `LIB`, a atrybuty **size** i **signature** były puste. Obecnie wartości atrybutów **dynamica**, **size**, **hash** i

signature są wartościami typu **VOLATILE**. Dlatego weryfikacja bibliotek jest pomijana podczas uruchamiania systemu. Od wersji 6.1.0 systemu AIX atrybuty **size**, **hash** i **signature** sekcji zaufanych bibliotek są obliczane dla plików `.o` biblioteki. Podczas instalowania baza danych `tsd.dat` jest zapełniana, odzwierciedlając wartości odpowiednich sekcji plików `.o` dla bibliotek zaufanych przechowywanych w bazie danych `/etc/security/tsd/lib/lib.tsd.dat`.

Dostęp do zdalnej bazy danych TE
Scentralizowane strategie bazy danych zaufanych podpisów (TSD) i Zaufanego wykonywania (TE) można zaimplementować w środowisku używanego systemu, zapisując je w LDAP.

Baza danych sterująca strategiami TSD i strategiami TE jest zapisana oddzielnie w każdym systemie. Scentralizowane strategie TSD i strategie TE systemu AIX są zapisane w LDAP, dzięki czemu można nimi zarządzać centralnie. Dzięki użyciu scentralizowanych strategii TSD i TE można sprawdzić, czy strategie zapisane w LDAP są główną kopią i czy strategie te mogą aktualizować klientów za każdym razem, gdy są oni reinstalowani, aktualizowani lub gdy wystąpi naruszenie zabezpieczeń. Scentralizowane strategie TE umożliwiają wymuszanie strategii TE z jednej lokalizacji bez konieczności oddzielnego aktualizowania każdego klienta. Scentralizowane strategie TSD są łatwiejsze w zarządzaniu niż strategie TSD, które nie są scentralizowane.

Za pomocą programów narzędziowych AIX można eksportować dane lokalnych strategii TSD i strategii TE do LDAP, konfigurować klientów, aby używali danych strategii TSD i strategii TE w LDAP, sterować wyszukiwaniem danych strategii TSD i strategii TE oraz zarządzać danymi LDAP z systemu klienta. W poniższych sekcjach przedstawiono więcej informacji na temat tych funkcji.

Eksportowanie strategii TSD i danych strategii TE do LDAP
Aby używać LDAP jako repozytorium centralnego dla strategii TSD i strategii TE, serwer LDAP musi być zapełniony danymi strategii.

Serwer LDAP musi mieć zainstalowany schemat strategii TSD i strategii TE dla LDAP zanim klienty LDAP będą mogły użyć tego serwera dla danych strategii. Schemat strategii TSD i strategii TE dla LDAP jest dostępny w systemie AIX w pliku **/etc/security/ldap/sec.ldif**. Schemat serwera LDAP należy zaktualizować danymi zawartymi w tym pliku, używając komendy **ldapmodify**.

Aby zidentyfikować wersję baz danych TE na serwerze LDAP i powiadomić klientów LDAP o tej konkretnej wersji, należy ustawić atrybut **databasename** w pliku **/etc/nscontrol.conf**. Atrybut **databasename** przyjmuje każdą nazwę jako wartość i jest on używany przez komendę **tetoldif** podczas generowania formatu ldif.

Użyj komendy **tetoldif**, aby odczytać dane w lokalnych plikach strategii TSD i strategii TE i uzyskać taki format strategii, który może być używany dla LDAP. Dane wyjściowe wygenerowane przez komendę **tetoldif** można zapisać do pliku w formacie ldif, a następnie wstawić do serwera LDAP komendą **ldapadd**. W systemie lokalnym komenda **tetoldif** używa następujących baz danych do generowania danych strategii TSD i strategii TE dla LDAP:

- /etc/security/tsd/tsd.dat
- /etc/security/tsd/tepolicies.dat

Konfiguracja klienta LDAP dla strategii TSD i strategii TE
Aby system mógł używać danych strategii TSD i strategii TE zapisanych na serwerze LDAP, musi być skonfigurowany jako klient LDAP.

Użyj komendy AIX **/usr/sbin/mksecldap**, aby skonfigurować system jako klienta LDAP. Komenda **mksecldap** dynamicznie przeszukuje podany serwer LDAP, aby określić położenie danych strategii TSD i strategii TE, a wyniki zapisuje w pliku **/etc/security/ldap/ldap.cfg**.

Po pomyślnym skonfigurowaniu systemu jako klienta LDAP za pomocą komendy **mksecldap**, należy następnie go skonfigurować, tak aby włączyć LDAP jako domenę wyszukiwania dla danych strategii TSD i strategii TE, konfigurując argument secorder pliku **/etc/nscontrol.conf**.

Po skonfigurowaniu systemu jako klienta LDAP jako domeny wyszukiwania dla danych strategii TSD i strategii TE demon klienta **/usr/sbin/secldapclntd** odtwarza dane strategii TSD i strategii TE z serwera LDAP podczas każdego wykonania dowolnych komend **trustchk** na kliencie LDAP.

Włączanie LDAP za pomocą komendy trustchk
Wszystkie komendy zarządzania bazą danych strategii TSD i strategii TE są włączone do użycia bazy danych strategii TSD i strategii TE LDAP.

Użyj komendy **trustchk** z opcją **–R**, aby wykonać początkowe konfigurowanie bazy danych LDAP. Początkowe konfigurowanie obejmuje dodanie strategii TSD, strategii TE i podstawowych nazw wyróżniających, a także utworzenie pliku **/etc/security/tsd/ldap/tsd.dat** lokalnej bazy danych i pliku **/etc/security/tsd/ldap/tepolicies.dat**.

Jeśli komenda **trustchk** zostanie uruchomiona z opcją **–R** z użyciem opcji LDAP, operacje będą oparte na danych serwera LDAP. Jeśli komenda **trustchk** zostanie uruchomiona z opcją **–R** z użyciem opcji files, operacje będą oparte na danych lokalnej bazy danych. Wartością domyślną dla opcji **–R** jest użycie opcji files.

Informacje pokrewne
Komenda mksecldap
Komenda trustchk

Kontrola integralności bazy danych zaufanych podpisów
Korzystając z komendy **trustchk** można sprawdzać stan integralności definicji plików w bazie danych zaufanych podpisów (TSD) z bieżącymi plikami.

Jeśli komenda **trustchk** wykryje jakąś anomalię, może skorygować ją automatycznie lub zapytać użytkownika przed próbą poprawienia. Nie jest możliwa naprawa takich anomalii, jak różnice wielkości, podpisu, wartości cert_tag lub hash_value. W takich przypadkach komenda **trustchk** spowoduje niedostępność pliku, wyświetlając go jako nieużyteczny i uszkodzony.

W przypadku innych niezgodnych atrybutów zostaną podjęte wymienione poniżej działania naprawcze:

owner (właściciel)
Właściciel pliku zostanie przywrócony na podstawie wpisu w bazie danych TSD.

group (grupa)
Grupa pliku zostanie przywrócona na podstawie wpisu w bazie danych TSD.

mode (tryb)
Bity trybu pliku zostaną zresetowane do wartości z bazy danych TSD.

hardlinks (dowiązania stałe)
Jeśli dowiązanie wskazuje inny plik, będzie zmienione, aby wskazywało ten plik. Jeśli dowiązanie nie istnieje, zostanie utworzone nowe dowiązanie do tego pliku.

symlinks (dowiązania symboliczne)
Tak samo jak dowiązania stałe.

type (typ)
Plik jest oznaczany jako niedostępny.

size (wielkość)
Plik jest oznaczany jako niedostępny, jeśli nie jest plikiem **ulotnym**.

cert_tag (znacznik certyfikacji)
Plik jest oznaczany jako niedostępny.

signature (podpis)
Plik jest oznaczany jako niedostępny, jeśli nie jest plikiem **ulotnym**.

hash_value (wartość mieszająca)
Plik jest oznaczany jako niedostępny, jeśli nie jest plikiem **ulotnym**.

minslabel (etykieta minimum)
W systemie Trusted AIX etykieta czułości minimalnej jest resetowana do wartości z bazy danych TSD.

maxslabel (etykieta maksimum)
W systemie Trusted AIX etykieta czułości maksymalnej jest resetowana do wartości z bazy danych TSD.

intlabel (etykieta integralności)
W systemie Trusted AIX etykieta integralności jest resetowana do wartości z bazy danych TSD.

accessauths (uprawnienia dostępu)
Autoryzacje dostępu są resetowane do wartości z bazy danych TSD. W systemie Trusted AIX wartości **t_accessauths** są częścią atrybutu **accessauths**.

innateprivs (uprawnienia wrodzone)
Uprawnienia wrodzone są resetowane do wartości z bazy danych TSD. W systemie Trusted AIX wartości **t_innateprivs** są częścią atrybutu **innateprivs**.

inheritprivs (uprawnienia dziedziczone)
Uprawnienia odziedziczone są resetowane do wartości z bazy danych TSD. W systemie Trusted AIX wartości **t_inheritprivs** są częścią atrybutu inherit.

authprivs (uprawnienia autoryzowane)
Uprawnienia autoryzowane są resetowane do wartości z bazy danych TSD. W systemie Trusted AIX wartości **t_authprivs** są częścią atrybutu **authprivs**.

aecflags (opcje bezpieczeństwa)
Opcje bezpieczeństwa są resetowane do wartości z bazy danych TSD. W systemie Trusted AIX wartości **t_secglags** są częścią atrybutu **secflags**.

Poprawność definicji plików można również sprawdzić z alternatywną bazą danych, używając opcji **-F**. Administrator systemu powinien unikać przechowywania bazy danych TSD w tym samym systemie i powinien tworzyć kopię zapasową tej bazy w położeniu alternatywnym. Sprawdzenie integralności plików można wykonać z kopią zapasową bazy danych TSD, używając opcji **-F**.

Konfigurowanie strategii bezpieczeństwa
Opcja Zaufane wykonywanie (Trusted Execution - TE) udostępnia mechanizm sprawdzania integralności wykonywanego pliku. Korzystając z tego mechanizmu można skonfigurować system, aby sprawdzał integralność plików zaufanych przed każdym żądaniem dostępu do tego pliku, umożliwiając systemowi dostęp tylko do zaufanych plików, które pomyślnie przejdą sprawdzenie integralności.

Gdy plik jest oznaczony jako zaufany (jego definicja jest dodana do bazy danych TSD), opcja TE może monitorować jego integralność przy każdym dostępie. Opcja ta stale monitoruje system i może wykrywać ingerencje w dowolny znajdujący się w systemie plik zaufany (próby ingerencji ze strony złośliwego użytkownika lub aplikacji) w czasie jego wykonywania. W przypadku wykrycia ingerencji w plik mechanizm TE podejmie działania naprawcze w oparciu o strategie konfigurowane fabrycznie: zatrzymanie wykonywania, zablokowanie dostępu do pliku lub zaprotokołowanie błędu. Podczas otwierania lub wykonywania pliku znajdującego się w bazie danych zaufanych podpisów, mechanizm TE wykona następujące czynności:

- Przed załadowaniem pliku binarnego komponent odpowiedzialny za ładowanie pliku (systemowy program ładujący) wywołuje podsystem zaufanego wykonywania i oblicza wartość mieszającą, używając algorytmu SHA-256 (który można skonfigurować).
- Wartość mieszająca obliczona w momencie wykonywania jest porównywana z przechowywaną w bazie danych TSD.
- Jeśli obie wartości są zgodne, otwarcie lub wykonanie pliku jest dozwolone.
- Jeśli wartości nie są zgodne, plik binarny został sfałszowany lub w jakiś sposób naruszono jego ochronę. Decyzja o tym, jakie działanie podjąć, należy do użytkownika. Mechanizm TE udostępnia użytkownikom opcje konfigurowania własnych strategii dla działań podejmowanych w momencie wykrycia niezgodności wartości mieszających.
- W oparciu o skonfigurowane strategie podejmowana jest stosowna akcja.

Można skonfigurować następujące strategie:

CHKEXEC
Sprawdza wartość mieszającą tylko zaufanych plików wykonywalnych przed załadowaniem ich do pamięci w celu wykonania.

CHKSHLIBS
Sprawdza wartość mieszającą tylko zaufanych bibliotek współużytkowanych przed załadowaniem ich do pamięci w celu wykonania.

CHKSCRIPTS
Sprawdza wartość mieszającą tylko zaufanych skryptów powłoki przed załadowaniem ich do pamięci.

CHKKERNEXT
Sprawdza wartość mieszającą tylko rozszerzeń jądra przed załadowaniem ich do pamięci.

STOP_UNTRUSTD
Zatrzymuje ładowanie niezaufanych plików. Ładowane są tylko pliki należące do bazy danych TSD. Strategia ta działa tylko w połączeniu z dowolną z wymienionych powyżej strategii CHK*. Na przykład, jeśli ustawiono **CHKEXEC=ON** i **STOP_UNTRUSTD=ON**, to blokowane jest wykonanie binarnego pliku wykonywalnego spoza wpisanych do bazy TSD.

STOP_ON_CHKFAIL
Zatrzymuje ładowanie zaufanych plików, dla których nie powiodło się sprawdzenie wartości mieszającej. Strategia ta działa również w połączeniu ze strategiami CHK*. Na przykład przy ustawieniach **CHKSHLIBS=ON** i **STOP_ON_CHKFAIL=ON** blokowane jest ładowanie do pamięci w celu użycia wszystkich bibliotek współużytkowanych, które nie należą do bazy danych TSD.

TSD_LOCK
Blokuje bazę danych TSD, aby nie była dostępna do edycji.

TSD_FILES_LOCK
Blokuje zaufane pliki. Nie zezwala na otwieranie plików zaufanych w trybie zapisu.

TE
Włącza/wyłącza funkcję Zaufane wykonywanie. Wyżej wymienione strategie mają zastosowanie, tylko jeśli włączono tę strategię.

W poniższej tabeli zebrano interakcje między różnymi włączonymi strategiami CHK* i STOP*:

Strategia	STOP_UNTRUSTD	STOP_ON_CHKFAIL
CHKEXEC	Zatrzymuje ładowanie plików wykonywalnych, które nie należą do bazy danych TSD.	Zatrzymuje ładowanie plików wykonywalnych, których wartość mieszająca jest niezgodna z wartością z bazy TSD.
CHKSHLIBS	Zatrzymuje ładowanie bibliotek współużytkowanych, które nie należą do bazy danych TSD.	Zatrzymuje ładowanie bibliotek współużytkowanych, których wartość mieszająca jest niezgodna z wartością z bazy TSD.
CHKSCRIPTS	Zatrzymuje ładowanie skryptów powłoki, które nie należą do bazy danych TSD.	Zatrzymuje ładowanie skryptów powłoki, których wartość mieszająca jest niezgodna z wartością z bazy TSD.
CHKKERNEXT	Zatrzymuje ładowanie rozszerzeń jądra, które nie należą do bazy danych TSD.	Zatrzymuje ładowanie rozszerzeń jądra, których wartość mieszająca jest niezgodna z wartością z bazy TSD.

Uwaga: Strategię można włączyć i wyłączyć w dowolnym momencie, dopóki włączona jest opcja TE wprowadzająca te strategie. Gdy strategia działa, jej wyłączenie obowiązuje dopiero po ponownym uruchomienia. Wszystkie komunikaty informacyjne są protokołowane w pliku **syslog**.

Informacje pokrewne
Usługa jądra TE_verify_reg
Usługa jądra TE_verify_unreg

Zaufane ścieżki wykonywania i Zaufane ścieżki bibliotek
Zaufane ścieżki wykonywania (Trusted Execution Path - TEP) to definicja listy katalogów zawierających zaufane pliki wykonywalne. Gdy weryfikacja TEP jest włączona, systemowy program ładujący pozwala na

wykonywanie tylko plików binarnych znajdujących się w podanych ścieżkach. Zaufana ścieżka bibliotek (Trusted Library Path - TLP) ma taką samą funkcjonalność, jednak służy do definiowania katalogów zawierających zaufane biblioteki systemu.

Gdy opcja TLP jest włączona, systemowy program ładujący pozwala na konsolidowanie z plikami binarnymi tylko bibliotek znajdujących się w podanej ścieżce. TEP lub TLP można włączyć za pomocą komendy **trustchk** z zestawem list ścieżek oddzielanych przecinkami. W tym celu należy użyć atrybutów wiersza komend TEP i TLP komendy **trustchk**.

Zaufana powłoka i sekwencja przywołania bezpiecznej komunikacji
Zaufana powłoka i sekwencja przywołania bezpiecznej komunikacji (Secure Attention Key - SAK) działają podobnie, jak Zaufana Baza Przetwarzania (Trusted Computing Base - TCB), jednak jeśli w systemie jest włączona opcja TE zamiast TCB, zaufana powłoka wykonuje pliki wpisane tylko do bazy danych zaufanych podpisów.

Więcej informacji o bazie TCB i sekwencji SAK zawierają sekcje Zaufana Baza Przetwarzania, Używanie sekwencji przywołania bezpiecznej komunikacji i Konfigurowanie sekwencji przywołania bezpiecznej komunikacji.

Baza danych strategii Zaufane wykonywanie (TE)
Strategie Zaufane wykonywanie (TE - Trusted Execution) są zapisane w pliku **/etc/security/tsd/tepolicies.dat**. Ścieżki dla strategii TE są podane z katalogami TLP i TEP.

Security Profile Evaluation Assurance Level 4+ i Labeled AIX Security oraz Evaluation Assurance Level 4+
Administrator systemu może zainstalować system następującymi opcjami Base AIX Security (BAS) i Evaluation Assurance Level 4+ (EAL4+) lub Labeled AIX Security (LAS) oraz Evaluation Assurance Level 4+ (EAL4+) podczas instalowania podstawowego systemu operacyjnego (BOS). System z tymi opcjami ma ograniczenia związane z oprogramowaniem instalowanym podczas instalacji BOS oraz dostępem sieciowym.

Uwaga: Trwa aktualizowanie systemu AIX wersja 7.1. Więcej informacji na ten temat można znaleźć w uwagach do wydania systemu AIX wersja 7.1.

Przegląd profilu bezpieczeństwa
Profil bezpieczeństwa jest produktem, który określa wymagania bezpieczeństwa dla systemów operacyjnych ogólnego przeznaczenia działających w sieci. Wymagania te pozwalają spełnić cele funkcji zabezpieczeń TOE (Target of Evaluation).

Profil bezpieczeństwa składa się z pakietu bazowego i kilku pakietów rozszerzonych. Produkty, które są powiązane z obsługą pakietu bazowego profilu bezpieczeństwa, to Identification and Authentication, Discretionary Access Control (DAC), Auditing, Cryptographic Services, Management of Security Mechanisms oraz Trusted Channel Communications. Profil bezpieczeństwa zawiera dodatkowe pakiety opcjonalne dla produktów: Labeled Security, Integrity Verification, Advanced Audit, General Purpose Cryptography, Advanced Management, Extended Identification and Authentication, Trusted Boot oraz Virtualization.

Założenia

- Środowisko przeznaczone do wykorzystania z TOE:

  Wszystkie założenia w tej sekcji odnoszą się do Base AIX Security (tryb BAS) i Labeled AIX Security (tryb LAS), chyba że stwierdzono inaczej. Wszystkie założenia dotyczące systemu VIOS są jawnie oznaczone, jako dotyczące wyłącznie systemu VIOS. System VIOS nie ma takich samych założeń, jak system operacyjny AIX ani Trusted AIX.

- Fizyczne:

  Środowisko IT udostępnia TOE z zachowaniem odpowiednich zabezpieczeń fizycznych proporcjonalnych do wartości zasobu IT chronionego przez TOE.

  Uwaga: Tylko VIOS: Środowisko operacyjne udostępnia TOE z zachowaniem odpowiednich zabezpieczeń fizycznych proporcjonalnych do wartości zasobu IT chronionego przez TOE.

- Administracyjne:
  - Funkcja zabezpieczeń TOE jest zarządzana przez przynajmniej jedną kompetentną osobę. Personel administrujący systemem nie jest beztroski, nie działa złośliwie lub wrogo i potrafi postępować zgodnie z instrukcjami zamieszczonymi w dokumentacji.
  - Upoważnieni użytkownicy mogą uzyskiwać dostęp do informacji zarządzanych przez TOE i oczekuje się, że będą oni współpracować.
  - Użytkownicy są wystarczająco przeszkoleni i można im ufać, że wykonają niektóre zadania lub grupy zadań w bezpiecznym środowisku IT. Muszą oni sprawować pełną kontrolę nad własnymi danymi.
  - Tylko VIOS: Funkcja zabezpieczeń TOE jest zarządzana przez przynajmniej jedną kompetentną osobę. Personel administrujący systemem nie jest beztroski, nie działa złośliwie lub wrogo i potrafi postępować zgodnie z instrukcjami zamieszczonymi w dokumentacji.
  - Tylko VIOS: Upoważnieni użytkownicy mają niezbędne uprawnienia pozwalające na dostęp przynajmniej do niektórych informacji zarządzanych przez TOE i oczekuje się, że będą oni współpracować.
  - Tylko VIOS: Użytkownicy są wystarczająco przeszkoleni i można im ufać, że wykonają niektóre zadania lub grupy zadań w bezpiecznym środowisku operacyjnym. Muszą oni sprawować pełną kontrolę nad własnymi danymi.
- Proceduralne:
  - Wszelkie modyfikacje lub uszkodzenia plików systemu TOE, dla których wymuszane są zabezpieczenia lub które dotyczą zabezpieczeń, które zostały spowodowane przez użytkownika lub platformę bazową, spowodowane przypadkowo lub celowo, muszą być wykrywane przez administratora.
  - Wszystkie zdalne systemy IT, które są określone jako zaufane przez TSF (Target Security Function) w celu dostarczania danych lub usług TSF do TOE lub w celu obsługi TSF w decyzjach wymuszania strategii bezpieczeństwa, działają pod kontrolą tych samych osób i w ramach ograniczeń strategii zabezpieczeń kompatybilnych ze strategią zabezpieczeń TOE.
  - Wszystkie zdalne systemy IT, które są określone jako zaufane przez TSF w celu dostarczania danych lub usług TSF do TOE lub w celu obsługi TSF w decyzjach wymuszania strategii bezpieczeństwa, poprawnie implementują funkcje używane przez TSF w sposób zgodny z założeniami zdefiniowanymi dla danej funkcji.
  - Zapewniana jest integralność następujących informacji:
    - Cały kod TSF (w tym również funkcja weryfikacji integralności, która jest ładowana i uruchamiana przed uruchomieniem mechanizmu weryfikacji integralności)
    - Wszystkie dane TSF (w tym dane TSF służące do sprawdzania integralności) wykorzystywane przez kod TSF ładowany i uruchamiany przed uruchomieniem mechanizmu weryfikacji integralności
  - Tylko VIOS: Wszelkie modyfikacje lub uszkodzenia plików systemu TOE, dla których wymuszane są zabezpieczenia lub które dotyczą zabezpieczeń, które zostały spowodowane przez użytkownika lub platformę bazową, spowodowane przypadkowo lub celowo, muszą być wykrywane przez administratora.
- Łączność: Wszystkie połączenia z i do zdalnych i zaufanych systemów IT oraz między fizycznie odrębnymi częściami TSF, które nie są chronione przez TSF, są fizycznie lub logicznie chronione w środowisku TOE w celu zapewnienia integralności i poufności przesyłanych danych wraz ze sprawdzaniem tożsamości komunikujących się punktów końcowych.

Uzyskiwanie oprogramowania

Aby uzyskać oprogramowanie, wykonaj następujące czynności:

1. Pobierz produkt.
2. Kliknij opcję Help w menu Entitled software support w menu po lewej stronie. Wymagane jest, aby produkt i jego aktualizacje były uzyskiwane na nośniku fizycznym lub z użyciem programu Download Director.

Informacje na temat instalowania produktu zawiera sekcja Instalowanie systemu BAS /EAL4+.

Instalowanie systemu BAS/EAL4+
Gdy opcja ta jest wybrana, automatycznie włączana jest kontrola RBAC.

Aby ustawić opcję BAS/EAL4+ podczas instalowania systemu BOS:

1. Na ekranie Instalacja i ustawienia wybierz pozycję **Więcej opcji**.
2. W sekcji Więcej opcji wybierz **Tak** dla BAS/EAL4+. Jeśli używana jest partycja WPAR, wybierz **Nie** dla TCB. Jeśli używany jest zmodyfikowany plik `bosinst.data` w celu wykonania instalacji nienadzorowanej, opcja TCB może mieć wartość **Tak**.

Wyłącz zdalne logowanie użytkownika root dla instalacji BAS. Aby wyłączyć zdalne logowanie, po instalacji wydaj następującą komendę:

```
/usr/bin/chuser rlogin=false subgroups=SUADMIN root
```

Dodaj użytkowników administracyjnych do grupy **SUADMIN**, aby mogli oni wydać komendę **su root**.

Opcja **Włącz technologie BAS oraz EAL4+** jest dostępna tylko po spełnieniu następujących warunków:

- metoda instalacji jest ustawiona na nową, pełną instalację nadpisującą,
- wybrany jest język angielski,
- włączone jest 64-bitowe jądro,
- włączony jest rozszerzony system plików JFS (JFS2).

Gdy wartość opcji **Włącz technologie BAS oraz EAL4+** jest ustawiona na Tak, wartość opcji **Zaufana Baza Przetwarzania** również jest ustawiona na Tak, a jedynymi prawidłowymi wartościami opcji **Pulpit** są BRAK lub CDE.

W przypadku instalacji nienadzorowanej z użyciem pliku `bosinst.data`, pole **INSTALL_TYPE** musi być ustawione na `CC_EVAL`, a następujące pola muszą być ustawione w sposób opisany poniżej:

```
control_flow:
    CONSOLE = ???
    PROMPT = yes
    INSTALL_TYPE = CC_EVAL
    INSTALL_METHOD = overwrite
    TCB = yes
    DESKTOP = NONE lub CDE
    ENABLE_64BIT_KERNEL = yes
    CREATE_JFS2_FS = yes
    ALL_DEVICES_KERNELS = no
    HTTP_SERVER_BUNDLE = no
    KERBEROS_5_BUNDLE = no
    SERVER_BUNDLE = no
    ALT_DISK_INSTALL_BUNDLE = no

locale:
    CULTURAL_CONVENTION = en_US lub C
    MESSAGES = en_US lub C
```

Więcej informacji na temat kontroli RBAC zawiera sekcja Role Based Access Control (RBAC).

Zarządzanie środowiskiem instalacji sieciowej dla BAS/EAL4+
Instalację klientów w technologii BAS/EAL4+ można przeprowadzić za pomocą środowiska Zarządzania Instalacją Sieciową (Network Installation Management - NIM).

System główny NIM jest skonfigurowany do udostępniania zasobów potrzebnych do zainstalowania odpowiedniego poziomu systemu BAS/EAL4+ w AIX 7.1. Klienty NIM można następnie instalować, korzystając z zasobów znajdujących się na systemie głównym NIM. Bezobsługową instalację NIM klienta można wykonać, ustawiając w zasobie **bosinst_data** następujące pola:

```
control_flow:
    CONSOLE = ???
    PROMPT = no
    INSTALL_TYPE = CC_EVAL
    INSTALL_METHOD = overwrite
```

```
    TCB = yes
    DESKTOP = NONE lub CDE
    ENABLE_64BIT_KERNEL = yes
    CREATE_JFS2_FS = yes
    ALL_DEVICES_KERNELS = no
    HTTP_SERVER_BUNDLE = no
    KERBEROS_5_BUNDLE = no
    SERVER_BUNDLE = no
    ALT_DISK_INSTALL_BUNDLE = no

locale:
    CULTURAL_CONVENTION = en_US lub C
    MESSAGES = en_US lub C
```

Systemu głównego NIM nie można konfigurować jako systemu BAS/EAL4+, a ponadto nie można go podłączyć do tej samej sieci, w której znajdują się inne systemy BAS/EAL4+. Podczas inicjowania instalacji z systemu głównego NIM, opcja menu **Pozostań klientem NIM po instalacji SMIT** musi być ustawiona na Nie. Po zainstalowaniu klienta NIM jako system BAS/EAL4+ klienta tego należy usunąć z sieci systemu głównego NIM i nie można wykonywać dodatkowych instalacji lub aktualizacji oprogramowania za pomocą tego systemu głównego NIM.

Rozpatrzmy przykładową sytuację, gdy mamy dwa środowiska sieciowe. Pierwsza sieć składa się z systemu głównego NIM i systemów innych niż BAS/EAL4+. Druga sieć składa się tylko z systemów BAS/EAL4+. Na kliencie NIM należy wykonać instalację NIM. Po jej zakończeniu należy odłączyć nowo zainstalowany system BAS/EAL4+ od sieci systemu głównego NIM i podłączyć go do zmienianej sieci.

Rozpatrzmy inny przykład, gdy mamy do dyspozycji jedną sieć. System główny NIM nie jest podłączony do sieci, gdy inne systemy pracują w zmienianej konfiguracji, a systemy BAS/EAL4+ nie są podłączone do sieci podczas instalacji NIM.

Pakunek oprogramowania BAS/EAL4+
Po wybraniu opcji **BAS/EAL4+** instalowana jest zawartość pakunku instalacyjnego `/usr/sys/inst.data/sys_bundles/CC_EVAL.BOS.autoi`.

Jeśli wybrana jest opcja **BAS/EAL4+**, opcjonalnie można wybrać instalację pakunku oprogramowania graficznego i pakunku oprogramowania usług dokumentacji. Jeśli razem z opcją **BAS/EAL4+** zostanie wybrana opcja **Oprogramowanie graficzne**, zostanie zainstalowana zawartość pakunku oprogramowania `/usr/sys/inst.data/sys_bundles/CC_EVAL.Graphics.bnd`. Jeśli razem z opcją **BAS/EAL4+** zostanie wybrana opcja Oprogramowanie usług dokumentacji, zainstalowana zostanie zawartość pakunku oprogramowania `/usr/sys/inst.data/sys_bundles/CC_EVAL.DocServices.bnd`.

Po zainstalowaniu programów licencjonowanych (Licensed Program Products - LPP) system zmieni konfigurację domyślną, tak aby była ona zgodna z wymaganiami BAS/EAL4+. Zostaną wprowadzone następujące zmiany:

- usunięcie wpisu `/dev/echo` z pliku `/etc/pse.conf`,
- utworzenie instancji urządzeń strumieniowych,
- umożliwienie dostępu do urządzeń wymiennych tylko użytkownikowi root,
- usunięcie z pliku `inetd.conf` wpisów nienależących do CC,
- zmiana innych uprawnień do pliku,
- zarejestrowanie dowiązania symbolicznego w pliku `sysck.cfg`,
- zarejestrowanie urządzenia w pliku `sysck.cfg`,
- ustawienie atrybutów domyślnego użytkownika i portu,
- skonfigurowanie aplikacji doc_search do używania przeglądarki,
- usunięcie wpisu httpdlite z pliku `inittab`,
- usunięcie wpisu writesrv z pliku `inittab`,
- usunięcie wpisu mkatmpvc z pliku `inittab`,
- usunięcie wpisu atmsvcd z pliku `inittab`,
- wyłączenie demona snmpd w pliku `/etc/rc.tcpip`,

- wyłączenie demona hostmibd w pliku `/etc/rc.tcpip`,
- wyłączenie demona snmpmibd w pliku `/etc/rc.tcpip`,
- wyłączenie demona aixmibd w pliku `/etc/rc.tcpip`,
- wyłączenie demona muxatmd w pliku `/etc/rc.tcpip`,
- port NFS (2049) jest portem uprawnionym,
- dodanie brakujących zdarzeń do pliku `/etc/security/audit/events`,
- zapewnienie, że interfejs pętli zwrotnej pracuje,
- utworzenie synonimów dla urządzenia `/dev/console`,
- wymuszenie domyślnych uprawnień połączenia serwera X,
- zmiana katalogu `/var/docsearch`, aby dla wszystkich możliwy był odczyt wszystkich plików,
- dodanie sekcji Menedżera Danych Obiektowych (Object Data Manager - ODM) w celu ustawienia uprawnień konsoli,
- ustawienie uprawnień terminali pty typu BSD na 000,
- wyłączenie plików `.netrc`,
- dodanie przetwarzania katalogu poprawek.

Graficzny interfejs użytkownika
System zgodny z BAS/EAL4+ wykorzystuje system X Windows w charakterze graficznego interfejsu użytkownika.

System X Window zapewnia mechanizm wyświetlania klientów graficznych, takich jak zegary, kalkulatory oraz inne aplikacje graficzne, a także wiele sesji terminalu wywoływanego za pomocą komendy **aixterm**. System X Window jest uruchamiany za pomocą komendy **xinit** wpisywanej w początkowym wierszu komend po zalogowaniu się użytkownika na konsoli hosta.

Aby uruchomić sesję X Window, wpisz:

```
xinit
```

Komenda ta uruchamia serwer X Window z lokalnymi mechanizmami dostępu możliwymi do wykorzystania tylko przez osobę wywołującą. Klienty X Window, które dysponują uprawnieniami użytkownika root, będą miały możliwość dostępu do serwera X Window za pośrednictwem gniazda domeny UNIX, korzystając z tego, że uprawnienia użytkownika root przesłaniają ograniczenia dostępu. Klienty X Window, które działają z uprawnieniami innych użytkowników lub zostały uruchomione przez innych użytkowników, nie będą miały dostępu do serwera X Window. To ograniczenie uniemożliwia uzyskanie przez użytkowników hosta dostępu bez uprawnień do serwera X Window.

Instalowanie systemu LAS/EAL4+
Gdy opcja ta jest wybrana, automatycznie włączana jest kontrola RBAC.

Aby ustawić opcję LAS/EAL4+ podczas instalowania systemu BOS:

Opcje instalacji są dostępne po wpisaniu wartości 3 w polu **Model zabezpieczeń** oraz wartości 4 w celu wyświetlenia pola **Więcej opcji** w oknie **Instalacja i konfiguracja**. Dostępne opcje zależą od typu instalacji (nadpisująca, zachowująca lub migracja) i opcji zabezpieczeń. Dla LAS metodą instalacji jest instalacja nowa lub z całkowitym nadpisaniem. Wybierz opcję **Instalowanie konfiguracji LAS/EAL4+**.

Więcej informacji na temat kontroli RBAC zawiera sekcja Role Based Access Control (RBAC).

Instalowanie konfiguracji LAS/EAL4+ (dostępne tylko dla środowiska Trusted AIX)
Opcja **Instalowanie konfiguracji LAS/EAL4+** powoduje zainstalowanie modelu Trusted AIX w trybie konfiguracji LAS/EAL4+. Skonfigurowany tryb LAS/EAL4+ wprowadza ostrzejsze rygory bezpieczeństwa w porównaniu z instalacją Trusted AIX.

W przypadku instalacji nienadzorowanej z użyciem pliku `bosinst.data`, pole **INSTALL_TYPE** należy pozostawić puste, pole **TRUSTED_AIX** powinno mieć wartość `yes`, a poniżej wymienione pola powinny być ustawione następująco:

```
control_flow:
    CONSOLE = ???
    PROMPT = yes
    INSTALL_TYPE =
    TRUSTED_AIX = yes
    INSTALL_METHOD = overwrite
    TCB = yes
    DESKTOP = NONE
    ENABLE_64BIT_KERNEL = yes
    CREATE_JFS2_FS = yes
    ALL_DEVICES_KERNELS = no
    HTTP_SERVER_BUNDLE = no
    KERBEROS_5_BUNDLE = no
    SERVER_BUNDLE = no
    ALT_DISK_INSTALL_BUNDLE = no

locale:
    CULTURAL_CONVENTION = en_US lub C
    MESSAGES = en_US lub C
```

Więcej informacji na temat środowiska Trusted AIX zawiera sekcja Trusted AIX.

Zarządzanie środowiskiem instalacji sieciowej dla LAS/EAL4+
Instalację klientów w technologii LAS/EAL4+ można przeprowadzić za pomocą środowiska Zarządzania Instalacją Sieciową (Network Installation Management - NIM).

System główny NIM jest skonfigurowany do udostępniania zasobów potrzebnych do zainstalowania odpowiedniego poziomu systemu LAS/EAL4+ w AIX 7.1. Klienty NIM można następnie instalować, korzystając z zasobów znajdujących się na systemie głównym NIM. Bezobsługową instalację NIM klienta można wykonać, ustawiając w zasobie bosinst_data następujące pola:

```
control_flow:
    CONSOLE = ???
    PROMPT = no
    INSTALL_TYPE =
    TRUSTED_AIX = yes
    INSTALL_METHOD = overwrite
    TCB = yes
    DESKTOP = NONE
    ENABLE_64BIT_KERNEL = yes
    CREATE_JFS2_FS = yes
    ALL_DEVICES_KERNELS = no
    HTTP_SERVER_BUNDLE = no
    KERBEROS_5_BUNDLE = no
    SERVER_BUNDLE = no
    ALT_DISK_INSTALL_BUNDLE = no

locale:
    CULTURAL_CONVENTION = en_US lub C
    MESSAGES = en_US lub C
```

Systemu głównego NIM nie można konfigurować jako systemu LAS/EAL4+, a ponadto nie można go podłączyć do tej samej sieci, w której znajdują się inne systemy LAS/EAL4+. Podczas inicjowania instalacji z systemu głównego NIM, opcja menu **Pozostań klientem NIM po instalacji SMIT** musi być ustawiona na Nie. Po zainstalowaniu klienta NIM jako system LAS/EAL4+ klienta tego należy usunąć z sieci systemu głównego NIM i nie można wykonywać dodatkowych instalacji lub aktualizacji oprogramowania za pomocą tego systemu głównego NIM.

Rozpatrzmy przykładową sytuację, gdy mamy dwa środowiska sieciowe. Pierwsza sieć składa się z systemu głównego NIM i systemów innych niż LAS/EAL4+. Druga sieć składa się tylko z systemów LAS/EAL4+. Na kliencie NIM należy wykonać instalację NIM. Po jej zakończeniu należy odłączyć nowo zainstalowany system LAS/EAL4+ od sieci systemu głównego NIM i podłączyć go do zmienianej sieci.

Rozpatrzmy inny przykład, gdy mamy do dyspozycji jedną sieć. System główny NIM nie jest podłączony do sieci, gdy inne systemy pracują w zmienianej konfiguracji, a systemy LAS/EAL4+ nie są podłączone do sieci podczas instalacji NIM.

Środowisko fizyczne systemów BAS/EAL4+ i LAS/EAL4+
Systemy BAS/EAL4+ i LAS/EAL4+ mają określone wymagania dotyczące środowiska, w którym mają działać.

Są one następujące:

- Fizyczny dostęp do systemów musi być tak ograniczony, aby jedynie autoryzowani administratorzy mogli korzystać z konsoli systemowych.
- Procesor serwisowy nie może być podłączony do modemu.
- Fizyczny dostęp do terminali musi być ograniczony tylko do użytkowników autoryzowanych.
- Sieć fizyczna musi być chroniona przed podsłuchami i podszywaniem się (końmi trojańskimi). W przypadku komunikowania się za pośrednictwem niezabezpieczonych linii, wymagane są dodatkowe zabezpieczenia, takie jak szyfrowanie.
- Komunikowanie z systemami innymi niż systemy AIX 7.1 BAS/EAL4+ i LAS/EAL4+ i systemami spoza tej samej kontroli zarządzania jest niedozwolone.
- Podczas komunikowania się z innymi systemami BAS/EAL4+ i LAS/EAL4+ używany jest tylko protokół IPv4. Protokół IPv6 znajduje się w konfiguracji wartościowanej, ale dostępne są tylko te funkcjonalne możliwości tego protokołu, które są obsługiwane także przez protokół IPv4.
- Użytkownicy nie mogą mieć możliwości zmiany godziny systemowej.
- Systemy w środowisku LPAR nie mogą współużytkować PHB.

Środowisko organizacyjne systemów BAS/EAL4+ i LAS/EAL4+
W przypadku systemów BAS/EAL4+ i LAS/EAL4+ muszą być spełnione pewne wymagania proceduralne i organizacyjne.

Muszą być spełnione następujące wymagania:

- Administratorzy muszą być godni zaufania i dobrze przygotowani.
- Jedynie użytkownicy autoryzowani do pracy z informacjami znajdującymi się w systemie mają przyznane identyfikatory użytkownika.
- Użytkownicy muszą korzystać z haseł o wysokiej jakości (maksymalnie losowych i niezwiązanych z użytkownikiem ani z organizacją). Więcej informacji na temat konfigurowania zasad dotyczących haseł można znaleźć w sekcji “Hasła” na stronie 65.
- Użytkownicy nie mogą ujawniać swoich haseł innym osobom.
- Administratorzy muszą mieć wystarczającą wiedzę, aby mogli zarządzać systemami, w których istotne jest bezpieczeństwo.
- Administratorzy muszą pracować zgodnie z instrukcjami zawartymi w dokumentacji systemu.
- Administratorzy muszą logować się za pomocą swojego identyfikatora osobistego i używać komendy **su** do przełączenia się w tryb administratora w celu wykonania zadań administracyjnych.
- Hasła wygenerowane przez administratorów dla użytkowników systemu muszą być do nich przesłane w sposób bezpieczny.
- Osoby odpowiedzialne za system muszą utworzyć i zaimplementować procedury niezbędne do bezpiecznego działania systemu.
- Administratorzy muszą zabezpieczyć dostęp do chronionych zasobów systemu za pomocą odpowiednich ustawień bitów uprawnień i list ACL.
- Organizacja musi wyrazić zgodę na przesyłanie przez fizyczną sieć przechowywanych w systemie danych objętych szczególnym zabezpieczeniem.
- Procedury konserwacji muszą obejmować normalną diagnostykę systemów.
- Administratorzy muszą mieć procedury, które zapewniają bezpieczną pracę systemu i jego odtwarzanie po awarii.
- Zmienna środowiskowa *LIBPATH* nie powinna być zmieniana, ponieważ może to spowodować, że zaufany proces załaduje niezaufaną bibliotekę.

- Oprogramowanie przechwytujące pakiety i śledzące (tcpdump, trace) nie może być używane w działającym systemie.
- Protokoły anonimowe, takie jak HTTP, mogą być używane tylko w przypadku informacji publicznych (takich jak dokumentacje elektroniczne).
- Można użyć jedynie systemu plików NFS bazującego na protokole TCP.
- Użytkownicy nie mają dostępu do nośników wymiennych. Pliki urządzeń muszą być chronione przez odpowiednie bity uprawnień lub listy ACL.
- Administratorom nie wolno używać dynamicznego partycjonowania do przydzielania i zwalniania zasobów. Konfigurowanie partycji można wykonać tylko wtedy, gdy żadna partycja nie jest uruchomiona.

Środowisko systemu operacyjnego BAS/EAL4+ i LAS/EAL4+
W przypadku systemów BAS/EAL4+ i LAS/EAL4+ muszą być spełnione pewne wymagania operacyjne i proceduralne.

Muszą być spełnione następujące wymagania i przestrzegane następujące procedury:

- Jeśli używana jest konsola Hardware Management Console (HMC), należy ją umieścić w środowisku będącym pod kontrolą fizyczną.
- Tylko autoryzowany personel ma dostęp do środowiska działania i konsoli HMC.
- Jeśli używana jest konsola HMC, można ją wykorzystywać tylko do następujących zadań:
  - Początkowe konfigurowanie partycji. Podczas procesu konfigurowania partycja nie może być aktywna.
  - Restartowanie "zawieszonych" partycji.
- Konsoli HMC nie można używać podczas pracy skonfigurowanego systemu.
- Funkcja "call home" systemu musi być wyłączona.
- Funkcja zdalnego dostępu za pomocą modemu musi być wyłączona.
- Jeśli system AIX działa w środowisku z obsługą partycji LPAR, administrator powinien sprawdzić w dokumentacji partycji LPAR wymagania dotyczące działania systemu EAL4+ na partycjach logicznych.
- Opcja uprawnień serwisowych musi być wyłączona na partycjach logicznych.

Konfigurowanie systemu BAS/EAL4+
Możliwe jest konfigurowanie systemu Base AIX Security (BAS) i Evaluation Assurance Level 4+ (EAL4+).

Grupy **system**, **sys**, **adm**, **uucp**, **mail**, **security**, **cron**, **printq**, **audit** i **shutdown** są traktowane jak grupy administracyjne. Do tych grup należy dodawać wyłącznie zaufanych użytkowników.

Administrowanie
Administratorzy muszą logować się przy użyciu konta osobistego i używać komendy **su**, aby stać się użytkownikiem root w celu administrowania systemem.

Aby efektywnie zapobiec próbom zgadywania hasła użytkownika root, jedynie autoryzowani administratorzy powinni mieć możliwość używania komendy **su** na koncie root. Aby tak było, wykonaj następujące czynności:

1. Dodaj następującą pozycję do sekcji **root** w pliku `/etc/security/user` :

```
root:
        admin = true
        .
        .
        .
        sugroups = SUADMIN
```

2. W pliku `/etc/group` zdefiniuj w następujący sposób grupę zawierającą jedynie identyfikatory użytkowników będących autoryzowanymi administratorami:

```
system:!:0:root,paul
staff:!:1:invscout,julie
```

```
bin:!:2:root,bin
.
.
.
SUADMIN:!:13:paul
```

Administratorzy muszą także postępować zgodnie z następującymi procedurami:

- tworzyć i implementować procedury w celu zapewnienia, że komponenty sprzętu, oprogramowania i oprogramowania wbudowanego składające się na system rozproszony są rozprowadzone, zainstalowane i skonfigurowane zgodnie z wymogami bezpieczeństwa,
- zapewnić, że system jest tak skonfigurowany, że jedynie administrator może instalować w nim nowe zaufane oprogramowanie,
- implementować procedury w celu zapewnienia, że użytkownicy czyszczą zawartość ekranu przed wylogowaniem się z szeregowych urządzeń logowania (na przykład terminali IBM® 3151).

Konfigurowanie użytkowników i portów
Opcje konfiguracji systemu AIX dotyczące użytkowników i portów muszą być ustawione, tak aby spełnić wymagania wartościowania. Rzeczywiste wymaganie jest takie, że TSF udostępnia mechanizm poprawnego zgadywania hasła, które spełnia zmierzoną jakość. Prawdopodobieństwo odgadnięcia hasła przez osobę atakującą musi być mniejsze od 2^-20 przez cały czas życia hasła.

Plik `/etc/security/user` przedstawiony w poniższym przykładzie korzysta z listy słowników `/usr/share/dict/words`. Plik `/usr/share/dict/words` znajduje się w zestawie plików `bos.data`. Zestaw plików `bos.data` należy zainstalować przed skonfigurowaniem pliku `/etc/security/user`. Zalecane wartości określone w pliku `/etc/security/user` są następujące:

```
default:
        admin = false
        login = true
        su = true
        daemon = true
        rlogin = true
        sugroups = ALL
        admgroups =
        ttys = ALL
        auth1 = SYSTEM
        auth2 = NONE
        tpath = nosak
        umask = 077
        expires = 0
        SYSTEM = "compat"
        logintimes =
        pwdwarntime = 5
        account_locked = false
        loginretries = 3
        histexpire = 52
        histsize = 20
        minage = 0
        maxage = 8
        maxexpired = 1
        minalpha = 2
        minother = 2
        minlen = 8
        mindiff = 4
        maxrepeats = 2
        dictionlist = /usr/share/dict/words
        pwdchecks =
        dce_export = false

root:
        rlogin = false
        login = false
```

Domyślne ustawienia w pliku `/etc/security/user` nie powinny być nadpisywane przez ustawienia charakterystyczne dla pojedynczego użytkownika.

Uwaga: Ustawienie `login = false` w sekcji root uniemożliwia bezpośrednie logowanie się użytkownika root. Jedynie użytkownicy, którzy mają uprawnienia do użycia komendy **su**, będą mogli logować się na koncie root. Jeśli dany system zostanie zaatakowany odmową usługi polegającą na wysyłaniu nieprawidłowych haseł użytkowników, może zablokować on wszystkie konta użytkowników. Taki atak

może uniemożliwić wszystkim użytkownikom (łącznie z administratorami) logowanie do systemu. Gdy konto użytkownika zostanie zablokowane, użytkownik nie będzie mógł się logować do czasu, gdy administrator systemu nie zresetuje atrybutu `unsuccessful_login_count` użytkownika w pliku `/etc/security/lastlog`, aby był mniejszy niż wartość atrybutu `loginretries` użytkownika. Jeśli wszystkie konta administracyjne zostaną zablokowane, należy uruchomić ponownie system w trybie konserwacji i uruchomić komendę **chsec**. Więcej informacji na temat korzystania z komendy **chsec** znajduje się w sekcji “Kontrola kont użytkowników” na stronie 52.

Proponuje się następujące wartości w pliku `/etc/security/login.cfg`:

```
default:
        sak_enabled = false
        logintimes =
        logindisable = 4
        logininterval = 60
        loginreenable = 30
        logindelay = 5
```

Lista programów setuid/setgid
Lista zaufanych aplikacji jest tworzona dla systemów AIX w włączoną obsługą BAS.

Bity **suid/sgid** są wyłączone w przypadku wszystkich niezaufanych programów należących do użytkownika root lub do zaufanej grupy. Po zainstalowaniu BAS jedynymi programami, które mają ustawiony bit **suid** i należą do użytkownika root albo mają ustawiony bit **sgid** i należą do jednej z zaufanych grup, są: **system**, **sys**, **adm**, **uucp**, **mail**, **security**, **cron**, **printq**, **audit** i **shutdown**. Do tych grup można dodawać wyłącznie zaufanych użytkowników.

Lista zaufanych aplikacji jest tworzona przy uwzględnieniu wszystkich aplikacji, które należą przynajmniej do jednej z następujących kategorii:

- włączony jest bit SUID użytkownika root odpowiedniej aplikacji,
- włączony jest bit SGID jednej z zaufanych grup,
- aplikacje uzyskujące dostęp do dowolnej z zaufanych baz danych zgodnie z dokumentem zawierającym zalecenia dla administratora,

Uwaga: Bit **setuid** dla komendy **ipcs** powinien zostać usunięty przez administratora systemu. Administrator systemu powinien uruchomić komendy **chmod u-s /usr/bin/ipcs** i **chmod u-s /usr/bin/ipcs64**.

Zmienianie systemu plików kontroli
Gdy opcja ta jest wybrana, automatycznie włączana jest kontrola RBAC.

System plików `/audit` jest systemem `jfs`. Musi on być zmieniony na system plików `jfs2`. Oprócz tego system BAS wymaga dodatkowych komend. Aby zmienić system plików, wykonaj następujące czynności:

1. Zmień system plików dla systemów BAS, używając komendy:

   ```
   audit shutdown
   lsvg -l rootvg
   ```

   Dla systemów LAS przejdź do kroku 3.
2. Jeśli pole TYP zawiera znak zapytania (?), wydaj komendę:

   ```
   synclvodm -v rootvg
   ```
3. Usuń system plików `jfs` i utwórz system plików `jfs2`, używając komendy:

   ```
   umount /audit
   rmfs /audit
   crfs -v jfs2 -m /audit -g rootvg -A yes -p rw -a size=100M
   ```

Aktualizowanie bazy danych zaufanych podpisów (trusted signature database - TSD)
W tej sekcji opisano procedurę aktualizowania bazy danych zaufanych podpisów (TSD).

Konfiguracja BAS/LAS zmienia bity trybu systemu, co powoduje występowanie błędów integralności TSD.

Podczas restartowania systemy wybierz opcję **Ignoruj wszystko**.

Aby zaktualizować TSD, wydaj komendę:

```
trustchk -u ALL mode
```

Używanie systemu LAS
W tej sekcji zamieszczono wskazówki na temat używania systemu LAS.

Ustaw wartość opcji automatycznego restartowania na **false** po zainstalowaniu systemu jako `isso`, wydając komendę:

```
chdev -l sys0 -a autorestart=false
```

Jeśli TSD nadal będzie generować błędy `intlabel`, usuń błędy, używając `isso` z uprawnieniem **PV_ROOT**:

```
cp /etc/security/tsd/tsd.dat /etc/security/tsd/tsd.dat.org
trustchk -q /usr/sbin/format /usr/sbin/fdformat /usr/sbin/mount /usr/sbin/unmount \
/usr/sbin/umount /usr/sbin/tsm /usr/sbin/getty /usr/sbin/login /usr/sbin/mkvg \
/usr/sbin/extendvg /usr/bin/w /usr/bin/uptime >/tmp/list.dat
grep -p SLTL /tmp/list.dat |sed 's/SLTL/SHTL/' >/tmp/new.dat
trustchk -w -a -f /tmp/new.dat
trustchk -y ALL
```

Jeśli na konsoli zostanie wyświetlony komunikat o błędzie dotyczący kontroli, używając uprawnień `isso` zrestartuj system kontroli komendami:

```
# audit shutdown
# audit start
```

Po trzech nieudanych próbach logowania przez sieć konta `isso/so` są blokowane. Administrator może jednak nadal uzyskać dostęp do tych kont, używając konsoli lokalnej.

Dane wyjściowe komend wykonywanych przez `cron/at` nie są przekazywane pocztą elektroniczną do użytkownika.

Katalogi dostępne do zapisu dla wszystkich, posiadające zakresy etykiet (na przykład: `/tmp`), nie są partycjonowane. Aby zapobiec przekazywaniu informacji między etykietami, administrator musi spartycjonować te katalogi natychmiast po wykonaniu początkowej konfiguracji.

Interfejs sieciowy
W tej sekcji opisano procedury używania interfejsu sieciowego.

W systemie Trusted AIX domyślny interfejs sieciowy ma zakres etykiet `minSL=impl_lo` i `maxSL=ts_all`. Dla systemów LAS/EAL4+ nie istnieje żaden zakres etykiet. Domyślna reguła jest automatycznie zmieniana na `impl_lo`, gdy wybrana zostanie opcja instalacji LAS/EAL4+. Aby zmienić domyślną regułę, jako użytkownik `isso` wydaj komendę **`netrule`**.

Na przykład:

```
/usr/sbin/netrule i+u default +impl_lo +impl_lo +impl_lo
```

Aktualizowanie partycji WPAR
W tej sekcji opisano procedurę aktualizowania partycji zarządzania obciążeniem (WPAR) w celu dostosowania do systemu AIX EAL4+.

Utwórz partycję WPAR w systemie BAS i wydaj następujące komendy w partycji WPAR, aby była ona zgodna z EAL4+:

```
/usr/lib/security/CC_EVALify.sh
```

Gdy komenda `clogin` jest uruchamiana w systemie LAS po raz pierwszy, uruchamiany jest skrypt firstboot (który wywołuje skrypt `CC_EVALify.sh`).

Skrypt firstboot powoduje, że komenda `clogin` działa dłużej niż zwykle, gdy komenda `clogin` wywołuje program TSM w celu zalogowania. Ponieważ partycja WPAR wciąż jest w trybie konfiguracji, logowanie nie powiedzie się. Przed kolejną próbą wydania komendy `clogin` należy odczekać około 10 minut, aby partycja WPAR zakończyła konfigurowanie. Dla nowo utworzonych partycji WPAR należy ustawić domyślne opcje użytkowników, aby spełnić wymagania:

- `root` w trybie BAS
- `isso/sa/so` w trybie LAS

Użytkownicy `root` i `isso` nie mają haseł lub wymagają słabych haseł. Hasła te muszą być zaktualizowane, zanim dopuści się dostęp niezaufanych użytkowników do środowiska globalnego lub danej partycji WPAR.

Wymagania dotyczące hasła są następujące: prawdopodobieństwo odgadnięcia hasła musi być mniejsze od 1 do 1000000, a prawdopodobieństwo odgadnięcia hasła w kolejnych próbach w ciągu jednej minuty musi być mniejsze od 1 do 100000. Aby spełnić to wymaganie, parametry użytkownika w pliku `/etc/security/user` muszą być zmienione w następujący sposób:

```
default:
 maxage = 8
 maxexpired = 1
 minother = 2
 minlen = 8
 maxrepeats = 2
 loginretries = 3
 histexpire = 52
 histsize = 20
```

Aktualizowanie EFS
W tej sekcji opisano procedurę ustawiania atrybutów bezpieczeństwa EFS, który został określony jako kryptograficzny system plików.

Określanie nie obejmuje trybu zabezpieczania przed pełnym dostępem użytkownika `root`. Podczas włączania EFS należy ustawić atrybuty zabezpieczeń dla komend **`efsmgr`** i **`egskeymgr`**:

```
setsecattr -c accessauths=ALLOW_ALL
innateprivs=PV_DEV_QUERY,PV_DEV_CONFIG,PV_AU_ADD,PV_DAC_R,PV_DAC_W,PV_DAC_X /usr/sbin/efsmgr

setsecattr -c accessauths=ALLOW_ALL
innateprivs=PV_DEV_QUERY,PV_DEV_CONFIG,PV_AU_ADD,PV_DAC_R,PV_DAC_W,PV_DAC_X /usr/sbin/efskeymgr

setkst -t cmd
```

Kasowanie dysku twardego
System AIX umożliwia kasowanie dysków twardych przy użyciu pomocy serwisowej **Formatuj nośnik** znajdującej się w pakiecie diagnostycznym systemu AIX. Pełną dokumentację pakietu diagnostycznego można znaleźć w książce *Diagnostic Information for Multiple Bus Systems*, a także w podręczniku użytkownika na temat sprzętu.

Aby skasować dysk twardy, należy wykonać następującą komendę:

```
diag -T "format"
```

Komenda ta powoduje uruchomienie opartej na interfejsie wielopoziomowego menu pomocy serwisowej **Formatuj nośnik**. Na prośbę programu należy wybrać używany terminal.

Zostanie wyświetlona lista zasobów do wyboru. Z listy należy wybrać urządzenia hdisk, które mają zostać skasowane, a następnie zatwierdzić dokonanie zmian zgodnie z instrukcjami pojawiającymi się na ekranie.

Po zatwierdzeniu zmian należy wybrać z menu opcję **Kasuj dysk**. Program prosi użytkownika o potwierdzenie wyboru. Należy wybrać opcję **Tak**.

Następnie program proponuje wybór jednej z opcji **Czytaj dane z dysku** lub **Zapisuj wzory na dysk**. Należy wybrać opcję **Zapisuj wzory na dysk**.

Na końcu użytkownik uzyskuje możliwość zmiany opcji kasowania dysku. Po określeniu preferowanych opcji należy wybrać polecenie **Commit Your Changes** (Zatwierdź zmiany). Rozpoczyna to kasowanie dysku.

Uwaga: Wykonywanie tego procesu może trwać bardzo długo.

Ograniczenia zasobów
Podczas ustawiania ograniczeń zasobów w pliku `/etc/security/limits` należy upewnić się, że odpowiadają one wymogom procesów w systemie.

W szczególności dla parametru `stack` nigdy nie należy ustawiać wartości `unlimited`. Nieograniczony stos może nadpisać inne segmenty uruchomionego procesu. Wielkość `stack_hard` także musi być ograniczona.

Podsystem kontrolujący
Istnieje kilka procedur ułatwiających zabezpieczenie podsystemu kontrolującego.

- Należy skonfigurować podsystem kontrolujący, tak aby zapisywał wszystkie czynności związane z bezpieczeństwem wykonywane przez użytkowników. Aby zapewnić, że przestrzeń plików wymagana do kontroli jest dostępna i nie mają na nią wpływu inne procesy korzystające z przestrzeni plików, należy skonfigurować dedykowany system plików dla danych kontroli.
- Należy chronić rekordy kontroli (takie jak zapisy kontrolne, pliki bin i inne dane przechowywane w katalogu `/audit`) przed użytkownikami nie będącymi użytkownikami root.
- W przypadku systemu BAS/EAL4+, jeśli jest wykorzystywany podsystem kontrolujący, musi być skonfigurowany tryb kontroli **bin**. Aby uzyskać informacje na temat konfigurowania podsystemu kontrolującego, należy zapoznać się z sekcją “Konfigurowanie kontroli” na stronie 151.
- Przynajmniej 20% dostępnej przestrzeni dyskowej musi być przeznaczone na zapisy kontrolne.
- Jeśli kontrola jest włączona, parametr *binmode* w sekcji start w pliku `/etc/security/audit/config` powinien być ustawiony na `panic`. Parametr *freespace* w sekcji bin powinien być ustawiony na wartość równą co najmniej 25% miejsca na dysku przeznaczonego na przechowywanie zapisów kontrolnych. Parametry *bytethreshold* i *binsize* należy ustawić na wartość 65536 bajtów.
- Należy skopiować rekordy kontroli z systemu do pamięci trwałej w celu archiwizacji.

Pliki niewspółużytkowane w systemie rozproszonym
Następujące pliki katalogu `/etc/security` nie są współużytkowane w systemie rozproszonym, ale są charakterystyczne dla każdego hosta:

/etc/security/failedlogin
Plik protokołu zawierający próby logowania, które się nie powiodły, dla każdego hosta

/etc/security/lastlog
Informacje dla każdego użytkownika o ostatniej pomyślnej i niepomyślnej próbie logowania do tego hosta

/etc/security/login.cfg
Charakterystyczne dla hosta parametry logowania dla zaufanych ścieżek, powłok logowania i inne informacje związane z logowaniem

/etc/security/portlog
Informacje dla każdego portu o portach zablokowanych na tym hoście

Automatycznie wygenerowane kopie zapasowe plików współużytkowanych także nie są współużytkowane. Pliki kopii zapasowych mają takie same nazwy, jak pliki oryginalne, ale na początku nazwy dołączona jest mała litera o.

Używanie funkcji DACinet w przypadku kontroli dostępu do sieci w oparciu o użytkowników i porty
Funkcja DACinet może być użyta w celu ograniczenia dostępu użytkowników do portów TCP.

Więcej informacji na temat DACinet znajduje się w sekcji “Oparta o użytkowników kontrola dostępu do portów TCP z indywidualną kontrolą dostępu do portów internetowych” na stronie 219. Na przykład, jeśli funkcja DACinet jest używana do ograniczania dostępu do portu TCP/25 dla połączeń przychodzących tylko do użytkownika root, jedynie użytkownicy root z systemów zgodnych z BAS/EAL4+ będą mieli do

niego dostęp. Ta sytuacja eliminuje ryzyko podszycia się pod adres e-mail normalnych użytkowników przez użycie komendy telnet w celu połączenia się z portem TCP/25 atakowanego komputera.

Aby aktywować ACL dla połączeń TCP w czasie uruchamiania, uruchamiany jest skrypt `/etc/rc.dacinet` z pliku `/etc/inittab`. Odczytuje on definicje z pliku `/etc/security/acl` i ładuje ACL do jądra. Porty, które nie powinny być chronione przez ACL, powinny być wymienione w pliku `/etc/security/services` (który ma ten sam format, co plik `/etc/services`).

Przyjmując, że podmaska 10.1.1.0/24 dotyczy wszystkich podłączonych systemów, pozycje listy ACL ograniczające dostęp tylko dla użytkowników root dla X (TCP/6000) w pliku `/etc/security/acl` będą miały postać:

```
      6000    10.1.1.0/24 u:root
```

Instalowanie dodatkowego oprogramowania w systemie zgodnym z BAS/EAL4+
Administrator może instalować dodatkowe oprogramowanie w systemie zgodnym z BAS/EAL4+. Jeśli oprogramowanie nie jest uruchamiane przez użytkownika root lub z uprawnieniami użytkownika root, nie spowoduje to naruszenia zgodności z systemem BAS/EAL4+. Typowym przykładem są aplikacje biurowe, które są uruchamiane przez normalnych użytkowników i nie mają komponentów SUID.

Zainstalowane oprogramowanie uruchomione z uprawnieniami użytkownika root narusza ponadto zgodność z systemem BAS/EAL4+. Oznacza to na przykład, że sterowniki starszych systemów plików JFS nie powinny być instalowane, ponieważ uruchamiane są w trybie jądra. Wszelkie aplikacje, którym nadano choć jedno uprawnienie z użyciem pliku `/etc/security/privcmds`, nie są akceptowane. Demony uruchomione jako użytkownicy root (na przykład demon SNMP) również naruszają zgodność z systemem BAS/EAL4+. System z włączoną opcją BAS/EAL4+ zwykle nie może być aktualizowany.

System zgodny z systemem BAS/EAL4+ jest rzadziej używany w konfiguracji wartościowanej, w szczególności w środowisku komercyjnym. Zwykle wymagane są dodatkowe usługi i system produkcyjny tworzony w oparciu o system wartościowany nie spełnia dokładnej specyfikacji systemu wartościowanego.

Listy kontroli dostępu i strategie dotyczące treści w systemie NSF v4
Lista kontroli dostępu (lista ACL) systemu plików NFS v4 zawiera pola **Type**, **Mask** i **Flags**.

Poniżej podano opis tych pól:

- Pole **Type** zawiera jedną spośród następujących wartości:
  - `ALLOW` - nadaje podmiotowi podanemu w polu **Who** uprawnienia podane w polu **Mask**.
  - `DENY` - odmawia podmiotowi podanemu w polu **Who** uprawnień podanych w polu **Mask**.
- Pole Mask zawiera jedną lub więcej spośród następujących rozczłonkowanych wartości uprawnień:
  - `READ_DATA / LIST_DIRECTORY` - odczytanie danych z obiektu niebędącego katalogiem lub wyświetlenie obiektów w katalogu.
  - `WRITE_DATA / ADD_FILE` - zapisanie danych w obiekcie niebędącym katalogiem lub dodanie obiektu niebędącego katalogiem do katalogu.
  - `APPEND_DATA / ADD_SUBDIRECTORY` - dołączenie danych do obiektu niebędącego katalogiem lub dodanie podkatalogu do katalogu.
  - `READ_NAMED_ATTRS` - odczytanie nazwanych atrybutów obiektu.
  - `WRITE_NAMED_ATTRS` - zapisanie nazwanych atrybutów obiektu.
  - `EXECUTE` - wykonanie pliku lub przejrzenie/wyszukanie katalogu.
  - `DELETE_CHILD` - usunięcie pliku lub katalogu w obrębie katalogu.
  - `READ_ATTRIBUTES` - odczytanie podstawowych (innych niż ACL) atrybutów pliku.
  - `WRITE_ATTRIBUTES` - zmiana czasów dotyczących pliku lub katalogu.
  - `DELETE` - usunięcie pliku lub katalogu.
  - `READ_ACL` - odczytanie listy ACL.

  - WRITE_ACL - zapisanie listy ACL.
  - WRITE_OWNER - zmiana właściciela i grupy.
  - SYNCHRONIZE - zsynchronizowanie dostępu (wartość dostępna ze względu na kompatybilność z innymi klientami NFS v4, ale nie ma zaimplementowanej funkcji).
- Pole **Flags** - to pole definiuje możliwości dziedziczenia list ACL katalogu i wskazuje, czy pole **Who** zawiera grupę. To pole nie zawiera żadnych opcji lub zawiera następujące opcje:
  - **FILE_INHERIT** - określa, że w tym katalogu nowo utworzone obiekty inne niż katalogi dziedziczą tę pozycję.
  - **DIRECTORY_INHERIT** - określa, że w tym katalogu nowo utworzone podkatalogi dziedziczą tę pozycję.
  - **NO_PROPAGATE_INHERIT** - określa, że w tym katalogu nowo utworzone podkatalogi dziedziczą tę pozycję, ale podkatalogi te nie przekazują tej pozycji do ich nowo utworzonych podkatalogów.
  - **INHERIT_ONLY** - określa, że ta pozycja nie ma zastosowania do tego katalogu, a tylko do nowo utworzonych obiektów dziedziczących tę pozycję.
  - **IDENTIFIER_GROUP** - określa, że pole **Who** reprezentuje grupę. W przeciwnym razie pole **Who** reprezentuje użytkownika lub specjalną wartość **Who**.
- Pole **Who** - to pole zawiera jedną spośród następujących wartości:
  - User - określa użytkownika, do którego ma zastosowanie ta pozycja.
  - Group - określa grupę, do której ma zastosowanie ta pozycja.
  - Special - ten atrybut może zawierać jedną spośród następujących wartości:
    - OWNER@ - określa, że ta pozycja ma zastosowanie do właściciela obiektu.
    - GROUP@ - określa, że ta pozycja ma zastosowanie do grupy będącej właścicielem obiektu.
    - EVERYONE@ - określa, że ta pozycja ma zastosowanie do wszystkich użytkowników systemu, w tym właściciela i grupy.

Jeśli lista ACL jest pusta, tylko podmiot z efektywnym UID o wartości 0 ma dostęp do obiektu. Właściciel obiektu niejawnie ma następujące wartości maski, bez względu na pozycje zawarte lub niezawarte na liście ACL:

- READ_ACL
- WRITE_ACL
- READ_ATTRIBUTES
- WRITE_ATTRIBUTES

Wartość APPEND_DATA jest implementowana jako WRITE_DATA. W rzeczywistości nie ma funkcjonalnej różnicy między wartościami WRITE_DATA i APPEND_DATA. Obie wartości muszą być ustawione jednomyślnie.

Prawo własności obiektu można zmodyfikować za pomocą wartości WRITE_OWNER. Zmiana właściciela lub grupy powoduje wyłączenie bitu **setuid**. Opcje dziedziczenia mają znaczenie tylko w odniesieniu do listy ACL katalogu i mają zastosowanie tylko do obiektów utworzonych w tym katalogu po ustawieniu opcji dziedziczenia (na przykład zmiany dziedziczenia na liście ACL katalogu macierzystego nie wpływają na istniejące obiekty). Kolejność pozycji na liście ACL systemu plików NFS v4 ma znaczenie. Aby określić, czy żądany dostęp jest dozwolony, każda pozycja jest przetwarzana po kolei. Uwzględniane są tylko te pozycje, które zawierają następujące wartości:

- pole **Who**, które jest zgodne z efektywnym UID;
- użytkownik określony w pozycji lub efektywny GID;
- grupa określona w pozycji podmiotu.

Każda pozycja jest przetwarzana, dopóki wszystkie bity dostępu requestera nie zostaną dozwolone (ALLOWED). Jeśli dla pozycji został ustawiony typ dostępu ALLOWED, pozycja ta nie jest już brana pod uwagę podczas przetwarzania kolejnych pozycji. Jeśli wystąpi pozycja odmawiająca (DENY), gdy dostęp

requestera dla danej wartości maski jest niezbędny i nieokreślony, następuje odmowa żądania. Jeśli wartościowanie osiągnie koniec listy ACL, następuje odmowa żądania.

Maksymalną obsługiwaną wielkością listy ACL jest 64 kB. Każda pozycja listy ACL ma zmienną długość, 64 kB jest dla niej jedynym ograniczeniem.

Wartość WRITE OWNER
Strategia systemu plików NFS v4 umożliwia sterowanie dostępem użytkowników do odczytu i zapisu atrybutów obiektów.

Podmiot o efektywnym UID 0 może zawsze przesłonić strategię systemu plików NFS v4. Właściciel obiektu może zezwolić innym użytkownikom na odczyt i zapis atrybutów obiektu, używając atrybutów `READ_ATTRIBUTES`, `WRITE_ATTRIBUTES`, `READ_NAMED_ATTRS` i `WRITE_NAME_ATTRS` maski ACL. Właściciel może sterować tym, kto może odczytywać i zapisywać listę ACL, używając wartości `READ_ACL` i `WRITE_ACL` maski ACL. Właściciel obiektu zawsze ma dostęp `READ_ATTRIBUTES`, `WRITE_ATTRIBUTES`, `READ_ACL` i `WRITE_ACL`. Właściciel obiektu może także zezwolić innym użytkownikom na zmianę właściciela i grupy obiektu, używając atrybutu `WRITE_OWNER`. Właściciel obiektu nie może domyślnie zmienić właściciela lub grupy, ale może on dodać do listy ACL pozycję `WRITE_OWNER` zawierającą takiego właściciela albo obiekt może dziedziczyć pozycję ACL określającą pozycję `WRITE_OWNER` z wartością **Who** parametru `OWNER@`. Zmiana właściciela lub grupy powoduje wyłączenie bitu **setuid**.

Poniżej podano kilka wyjątków od tych reguł:

- Jeśli właścicielem obiektu jest UID 0, tylko UID 0 może zmienić właściciela, ale grupa nadal może być zmieniana przez podmiot z atrybutem `WRITE_OWNER`.
- Przy założeniu, że obiekt ma atrybut `WRITE_OWNER` dla podmiotu, w wersjach systemu AIX 5.3 sprzed poziomu poprawek 5300-05, jeśli obiekt ma właściciela innego niż UID 0, takiego właściciela można zmienić wyłącznie na użytkownika innego niż UID 0. W systemie AIX z pakietem 5300-05 i w nowszych wersjach, jeśli obiekt ma właściciela innego niż UID 0, takiego właściciela można zmienić wyłącznie na EUID podmiotu próbującego zmienić właściciela.
- Grupę można zmienić na dowolną grupę z zestawu współbieżnych grup podmiotu. Istnieje jednak wyjątek: nigdy nie można jej zmienić na GID 0 lub GID 7 (system lub bezpieczeństwo), nawet jeśli te dwie grupy znajdują się w zestawie grup współbieżnych podmiotu.

Obsługiwana administracyjna baza danych: wykorzystująca LDAP i plikowa
Wartościowanie nie obsługuje administracyjnej bazy danych NFS. Metody uwierzytelniania, takie jak DCE i NIS, nie są obsługiwane.

Wartościowanie obsługuje tylko:

- uwierzytelnianie plikowe (wartość domyślna),
- uwierzytelnianie wykorzystujące LDAP (analogicznie do systemu UNIX) - należy użyć serwera LDAP IBM Tivoli Directory Server v 6.0.

Więcej informacji na temat uwierzytelniania plikowego zawiera sekcja Uwierzytelnianie użytkowników.

Uwierzytelnianie LDAP
Identyfikowanie i uwierzytelnianie wykorzystujące LDAP konfiguruje się w trybie uwierzytelniania "typu UNIX". W tym trybie dane administracyjne (w tym nazwy użytkowników, identyfikatory i hasła) są zapisane na serwerze LDAP, na którym dostęp do danych jest ograniczony do administratora LDAP.

Gdy użytkownik loguje się w systemie, system nawiązuje połączenie z serwerem LDAP za pomocą połączenia SSL, używając konta administratora LDAP, pobiera potrzebne dane dotyczące użytkownika (w tym hasło) z serwera LDAP, a następnie wykonuje uwierzytelnianie, korzystając z danych pobranych z tego serwera. System przechowuje administracyjną bazę danych na serwerze LDAP. Pozostałe hosty importują dane administracyjne z tego samego serwera LDAP, korzystając mechanizmu opisanego powyżej. System utrzymuje spójną administracyjną bazę danych, wprowadzając wszystkie zmiany administracyjne na wyznaczonym serwerze LDAP. ID użytkownika na dowolnym komputerze odnosi się do tej samej osoby na wszystkich pozostałych komputerach. Ponadto konfiguracja haseł, odwzorowania nazw na identyfikatory UID i inne dane są identyczne na wszystkich hostach w systemie rozproszonym.

Więcej informacji na temat konfigurowania uwierzytelniania LDAP zawiera sekcja Protokół LDAP (Light Directory Access Protocol). Więcej informacji na temat konfigurowania SSL w LDAP zawierają sekcje Konfigurowanie warstwy SSL na serwerze LDAP i Konfigurowanie warstwy SSL na kliencie LDAP.

Serwer LDAP
Komenda **mksecldap -s** umożliwia skonfigurowanie systemu AIX jako serwera LDAP na potrzeby uwierzytelniania bezpieczeństwa i zarządzania danymi.

Wykonaj następujące zadania:

- Użyj schematu RFC2307AIX z opcją **-S**.
- Skonfiguruj serwer, aby używał protokołu Secure Sockets Layer (SSL), używając opcji **-k**. Ta czynność wymaga zainstalowania zestawu plików **GSKit V8** i zestawu plików **idsldap.clt_max_crypto32bit63.rte** dla systemów 32-bitowych lub zestawu plików **idsldap.clt_max_crypto64bit63.rte** dla systemów 64-bitowych. Użyj programu narzędziowego ikeyman, aby wygenerować pary kluczy dla serwera katalogów.

Opcje użytkowników LDAP muszą być ustawione, tak aby spełniały wymagania wartościowania. Schemat RFC2370AIX definiuje atrybuty użytkowników. Użyj tych samych wartości, które opisano w sekcji Konfiguracja systemu BAS/EAL4+. Administratorzy Tivoli Directory Server nie muszą okresowo zmieniać haseł (np. nie ma wartości **MaxAge** dla haseł administratorów). Dlatego hasło administratora LDAP musi być zmieniane tak samo często, jak hasło użytkownika systemu AIX (**MaxAge** = 8 (tygodni)).

W produkcie Tivoli Directory Server 6.3 obsługa niepowodzenia uwierzytelniania nie ma zastosowania do administratora katalogu ani do członków grupy administratorów. Reguły tworzenia haseł także nie mają zastosowania do kont administratorów. Muszą one być wymuszane, jeśli używany jest produkt Tivoli Directory Server 6.3.

Jeśli administrator nie używa wspólnego zaplecza bazy danych LDAP do zarządzania użytkownikami, musi zapewnić, aby baza danych zawierająca referencje użytkowników pozostawała spójna między różnymi częściami systemów TOE (TCP Offload Engine) sieci. Przykłady:

- `/etc/group`
- `/etc/passwd`
- `/etc/security/.ids`
- `/etc/security/.profile`
- `/etc/security/environ`
- `/etc/security/group`
- `/etc/security/limits`
- `/etc/security/passwd`
- `/etc/security/user`

Informacje pokrewne
Informacje o pakietach, zestawach plików i wymaganiach wstępnych produktu IBM Tivoli Directory Server

Klient LDAP
Komenda **mksecldap -c** umożliwia skonfigurowanie systemu AIX jako klienta LDAP na potrzeby uwierzytelniania bezpieczeństwa i zarządzania danymi.

Wykonaj następujące zadania:

- Używając komendy **mksecldap -c**, podaj **unix_auth** dla **authType** z opcją **-A**.
- Skonfiguruj klienta, aby korzystał z protokołu SSL, używając opcji **-k** komendy **mksecldap -c**. Podanie klucza SSL klienta wymaga zainstalowania zestawów plików **GSKit** i **ldap.max_crypto_client**. Użyj programu narzędziowego **gsk7ikm**, aby wygenerować pary kluczy dla serwera katalogów.

Klient/serwer NFS v4 a protokół Kerberos
Środowisko Klient/serwer NFS v4 zawiera protokół LDAP do obsługi danych uwierzytelniania i protokół Kerberos do nawiązywania zaufanego kanału między klientami i serwerami systemu plików NFS v4.

Wartościowana konfiguracja obsługuje NAS v1.4 dla protokołu Kerberos i IBM Tivoli Directory Server v6.0 (serwer LDAP) jako bazę danych użytkowników.

Konieczne jest skonfigurowanie NAS v1.4 (Serwer Kerberos w wersji 5), aby można było używać LDAP jako bazy danych. Bilety Kerberos wcześniej nadawane przez serwer Kerberos są ważne do momentu utraty ważności.

Podczas korzystania z uwierzytelniania Kerberos referencje używane w zdalnych wywołaniach procedur inicjowanych przez użytkownika są powiązane z bieżącym biletem Kerberos należącym do użytkownika i nie wpływa na nie rzeczywisty lub efektywny identyfikator UID procesu. Podczas uzyskiwania dostępu do zdalnego systemu plików za pomocą uwierzytelniania Kerberos, gdy uruchomiony jest program **setuid**, identyfikator UID widziany na serwerze jest oparty na tożsamości Kerberos i nie jest to identyfikator UID będący właścicielem uruchomionego programu **setuid**.

Konfiguracja wartościowana obejmuje ustawienie systemu plików NFS pod kątem użycia zabezpieczeń RPCSEC-GSS. Więcej informacji na ten temat zawierają sekcje Network File System, Konfigurowanie serwera NFS i Konfigurowanie klienta NFS. Podczas konfigurowania serwera należy wybrać uwierzytelnianie Kerberos i włączyć rozszerzone bezpieczeństwo na serwerze. Można to zrobić za pomocą programu SMIT, używając komendy **chnfs**. Komenda **chnfs** udostępnia opcję włączania zabezpieczeń RPCSEC_GSS. Podczas konfigurowania klienta należy postępować zgodnie z instrukcjami dotyczącymi używania protokołu Kerberos podanymi w sekcji Konfigurowanie klienta NFS. Instrukcje dotyczące konfigurowania serwera danych Kerberos z szyfrowaniem DES3 na potrzeby bezpieczeństwa zawiera sekcja Konfigurowanie sieci dla RPCSEC-GSS. Konfiguracja wartościowana obsługuje tylko szyfrowanie DES3.

Reguły dotyczące haseł
Wartościowana konfiguracja powinna mieć podane tu wartości dla reguł dotyczących haseł, gdy używany jest serwer Kerberos z bazą danych LDAP.

Więcej informacji na temat reguł dotyczących haseł zawiera rozdział "Chapter 9. Managing Network Authentication Service passwords" dokumentacji *IBM Network Authentication Service Version 1.4 for AIX, Linux and Solaris Administrator's and User's Guide*.

Poniżej podano listę wartości:

mindiff
4

maxrepeats
2

minalpha
2

minother
2

minlen
8

minage
0

histsize
10

Aby klient NFS v4 AIX jawnie i bezpiecznie komunikował się z serwerem NFS v4 AIX NFS tylko za pomocą typów szyfrowania DES3, należy utworzyć nazwę użytkownika serwera "nfs/nazwa_hosta" z typem szyfrowania DES3 (np. des3-cbc-sha1) wraz z odpowiadającą jej pozycją w pliku `keytab` (za pomocą interfejsu **kadmin**) i ustawić typ DES3 (np. **des3-cbc-sha1**) jako pierwszą pozycję w sekcji **default_tgs_enctypes** pliku `/etc/krb5/krb5.conf` na kliencie NFS v4.

Wirtualny serwer we/wy
Wirtualny serwer we/wy (VIOS) znajduje się na oddzielnej partycji LPAR i udostępnia podstawową indywidualną kontrolę dostępu między sterownikami urządzeń SCSI serwera VIOS działającymi w imieniu partycji a opartymi na SCSI woluminami logicznymi i woluminami fizycznymi przez odwzorowania.

Partycję LPAR można (przez sterownik urządzenia SCSI serwera VIOS) odwzorować na 0 lub więcej woluminów logicznych i fizycznych, ale wolumin można odwzorować wyłącznie na jedną partycję LPAR. To odwzorowanie ogranicza partycję LPAR wyłącznie do przypisanych do niej woluminów. Serwer VIOS steruje także odwzorowaniem sterowników urządzeń adapterów Ethernet VIOS na sterowniki urządzeń Ethernet VIOS działające w imieniu grupy partycji LPAR, które współużytkują sieć wirtualną. W wartościowanej konfiguracji dozwolone jest wyłącznie odwzorowanie jeden-do-jednego sterownika urządzenia adaptera Ethernet na sterownik urządzenia Ethernet działający w imieniu grupy partycji LPAR. Odwzorowanie jeden-do-jednego jest konfigurowane przez administratora i wymuszane przez sterowniki urządzeń. Ponadto pakiety Ethernet nie mogą być oznaczane znacznikiem VLAN w wartościowanej konfiguracji. Tego mechanizmu można użyć do ograniczenia partycji LPAR, które mogą widzieć niektóre pakiety Ethernet.

Interfejs VIOS powinien być zabezpieczony przed dostępem przez nieuprzywilejowanych użytkowników. Opcje użytkowników VIOS muszą być ustawione, tak aby spełniały wymagania wartościowania. Rzeczywiste wymaganie jest następujące: TSF musi udostępniać mechanizm weryfikowania danych niejawnych w celu zweryfikowania, że spełniają one następujący warunek: prawdopodobieństwo odgadnięcia danych niejawnych przez osobę atakującą musi być mniejsze od 2^-20 przez cały czas ważności danych niejawnych. Poniżej podano parametry, które należy zmienić dla użytkownika w katalogu `/etc/security/user`:

maxage
8

maxexpired
1

minother
2

minlen
8

maxrepeats
2

loginretries
3

histexpire
52

histsize
20

Aby zmienić wartości domyślne, należy użyć następujących komend:

```
type oem_setup_env

chsec -f /etc/security/user -s default  -a maxage=8 -a maxexpired=1 -a minother=2
  -a minlen=8 -a maxrepeats=2 -a loginretries=3 -a histexpire=52 -a histsize=20
```

Gdy administrator podstawowy (**padmin**) tworzy nowego użytkownika, musi jawnie podać atrybuty tego użytkownika. Na przykład, aby utworzyć użytkownika *dawid*, administrator **padmin** musi użyć komendy:

```
mkuser  maxage=8 maxexpired=1 minother=2 minlen=8 maxrepeats=2 loginretries=3
  histexpire=52 histsize=20 dawid
```

Ponadto administrator **padmin** powinien zatrzymać następujące demony i wykonać restart:

- Aby usunąć **writesrv** i **ctrmc** z pliku `/etc/inittab`:

```
sshd:   stopsrc -s sshd
```

- Aby demon nie uruchamiał się przy starcie systemu, należy usunąć pliki `/etc/rc.d/rc2.d/Ksshd` i `/etc/rc.d/rc2.d/Ssshd`. Po restarcie należy zatrzymać demony RSCT:

```
stopsrc -g rsct_rm stopsrc -g rsct
```

Wszystkich użytkowników, bez względu na pełnione przez nich role, należy uważać za użytkowników administracyjnych.

Administrator systemu może uruchamiać wszystkie komendy, oprócz tych podanych poniżej, których może używać administrator podstawowy (**padmin**):

- **chdate**
- **chuser**
- **cleargcl**
- **de_access**
- **diagmenu**
- **invscout**
- **loginmsg**
- **lsfailedlogin**
- **lsgcl**
- **mirrorios**
- **mkuser**
- **motd**
- **oem_platform_level**
- **oem_setup_env**
- **redefvg**
- **rmuser**
- **shutdown**
- **unmirrorios**

Kontrola logowania
Parametry domyślne ekranu logowania można ze względów bezpieczeństwa zmienić po zainstalowaniu systemu.

Potencjalni hakerzy mogą uzyskać cenne informacje, takie jak nazwa hosta i wersja systemu operacyjnego, z domyślnego ekranu logowania systemu AIX. Te informacje mogą im umożliwić określenie, które metody ataku mogą zostać użyte. Ze względów bezpieczeństwa należy zmienić wartości domyślne ekranu logowania bezpośrednio po zainstalowaniu systemu.

Pulpity KDE i GNOME mają niektóre wspólne cechy dotyczące problemów z bezpieczeństwem. Więcej informacji na temat pulpitów KDE i GNOME znajduje się w podręczniku *Instalowanie i przeprowadzanie migracji*.

Więcej informacji na temat użytkowników, grup i haseł zawiera sekcja “Użytkownicy, grupy i hasła” na stronie 46.

Konfigurowanie kontroli logowania
Kontrolę logowania można konfigurować w pliku `/etc/security/login.cfg`.

Kontrolę logowania należy skonfigurować w pliku `/etc/security/login.cfg` w sposób opisany poniżej, aby utrudnić atak na system polegający na odgadywaniu haseł:

Tabela 1. Atrybuty oraz zalecane wartości dla kontroli logowania.				
Atrybut	**Dotyczy terminali PtY (sieć)**	**Dotyczy terminali TTY**	**Zalecana wartość**	**Uwagi**
sak_enabled	T	T	false	Sekwencja przywołania bezpiecznej komunikacji jest rzadko wymagana. Więcej informacji na ten temat zawiera sekcja “Korzystanie z sekwencji przywołania bezpiecznej komunikacji” na stronie 5.
logintimes	N	T		Określa dozwolone czasy trwania logowania.
logindisable	N	T	4	Uniemożliwia logowanie na tym terminalu po 4 kolejnych nieudanych próbach.
logininterval	N	T	60	Terminal zostanie wyłączony, gdy w ciągu 60 sekund zostanie wykonana określona liczba nieudanych prób.
loginreenable	N	T	30	Po 30 minutach włącza terminal, który został automatycznie wyłączony.
logindelay	T	T	5	Czas w sekundach między próbami logowania. Zostanie on przemnożony przez liczbę nieudanych prób; na przykład 5, 10, 15, 20 sekund; gdy wartością początkową jest 5.

Te ograniczenia portów działają głównie na podłączonych terminalach szeregowych, a nie na pseudoterminalach używanych przy logowaniu przez sieć. W tym pliku można określić jawne terminale, na przykład:

```
/dev/tty0:
        logintimes = 0600-2200
        logindisable = 5
        logininterval = 80
        loginreenable = 20
```

Zmiana komunikatu powitalnego na ekranie logowania

Aby uniemożliwić wyświetlanie określonych informacji na ekranach logowania, należy poddać edycji parametr *herald* w pliku /etc/security/login.cfg.

Domyślnie parametr *herald* zawiera komunikat powitalny, który jest wyświetlany podczas logowania. Aby zmienić ten parametr, można użyć komendy **chsec** lub bezpośrednio modyfikować plik.

W poniższym przykładzie komenda **chsec** została użyta do zmiany wartości domyślnej parametru *herald*:

```
# chsec -f /etc/security/login.cfg -s default
-a herald="Użycie tego systemu bez zezwolenia jest surowo wzbronione.\n\nlogin:"
```

Więcej informacji na temat komendy **chsec** znajduje się w publikacji *Commands Reference, Volume 1*.

Aby bezpośrednio modyfikować plik, należy otworzyć plik `/etc/security/login.cfg` i zaktualizować parametr *herald* w następujący sposób:

```
default:
herald ="Użycie tego systemu bez zezwolenia jest surowo wzbronione\n\nlogin:"
 sak_enable = false
 logintimes =
 logindisable = 0
```

```
 logininterval = 0
 loginreenable = 0
 logindelay = 0
```

Uwaga: Aby podnieść poziom zabezpieczenia systemu, należy ustawić zmienne *logindisable* i *logindelay* na wartości większe niż `0` (`# > 0`).

Zmiana ekranu logowania dla uniwersalnego środowiska graficznego (CDE)
Ten problem bezpieczeństwa dotyczy także użytkowników systemu Uniwersalne Środowisko Graficzne (CDE). Ekran logowania CDE również domyślnie wyświetla nazwę hosta i wersję systemu operacyjnego. Aby zapobiec wyświetlaniu tych informacji, należy poddać edycji plik `/usr/dt/config/$LANG/Xresources`, gdzie **$LANG** oznacza lokalny język zainstalowany na komputerze.

W tym przykładzie, zakładając że **$LANG** jest ustawione na **C**, należy skopiować ten plik do katalogu `/etc/dt/config/C/Xresources`. Następnie należy otworzyć plik `/usr/dt/config/C/Xresources` i poddać go edycji, usuwając komunikaty powitalne zawierające nazwę hosta i wersję systemu operacyjnego.

Więcej informacji na temat zagadnień bezpieczeństwa CDE znajduje się w sekcji “Uwagi dotyczące zarządzania środowiskami X11 i CDE” na stronie 39.

Wyłączanie wyświetlania nazwy użytkownika oraz zmiana pytania o hasło
W środowisku zabezpieczonym konieczne może się okazać ukrycie wyświetlania nazwy użytkownika lub udostępnienie niestandardowego pytania o hasło, które różni się od domyślnego.

Domyślny komunikat dla logowania i pytania o hasło przedstawiono poniżej:

```
login: foo
Hasło foo:
```

Aby wyłączyć wyświetlanie nazwy użytkownika z pytań i komunikatów o błędach systemowych, należy zmienić parametr *usernameecho* w pliku `/etc/security/login.cfg`. Wartością domyślną parametru *usernameecho* jest wartość true, która powoduje, że nazwa użytkownika zostanie wyświetlona. Aby zmienić ten parametr, można użyć komendy **chsec** lub bezpośrednio modyfikować plik.

W poniższym przykładzie komenda **chsec** została użyta do zmiany domyślnej wartości parametru *usernameecho* na wartość false:

```
# chsec -f /etc/security/login.cfg -s default -a usernameecho=false
```

Więcej informacji na temat komendy **chsec** znajduje się w publikacji *Commands Reference, Volume 1*.

Aby bezpośrednio edytować plik, należy otworzyć plik `/etc/security/login.cfg` i dodać lub zmodyfikować parametr *usernameecho* w następujący sposób:

```
default:
 usernamecho = false
```

Podanie wartości false dla parametru *usernameecho* spowoduje, że w pytaniu o logowanie nazwa użytkownika nie będzie wyświetlana. Zamiast tego, w podpowiedziach systemu oraz komunikatach o błędach nazwa użytkownika zostanie zamaskowana znakami '*', tak jak przedstawiono to poniżej:

```
login:
Hasło ***:
```

Pytanie o hasło można zmodyfikować oddzielnie, podając jako wartość parametru *pwdprompt* w pliku `/etc/security/login.cfg` niestandardowy łańcuch. Wartością domyślną jest łańcuch "Hasło *użytkownik*: ", gdzie *użytkownik* to nazwa uwierzytelniająca użytkownika.

Aby zmienić ten parametr, można użyć komendy **chsec** lub bezpośrednio modyfikować plik.

W poniższym przykładzie komenda **chsec** została użyta do zmiany domyślnej wartości parametru *pwdprompt* na wartość "Hasło: ":

```
# chsec -f /etc/security/login.cfg -s default -a pwdprompt="Hasło: "
```

Aby bezpośrednio edytować plik, należy otworzyć plik `/etc/security/login.cfg` i dodać lub zmodyfikować parametr *pwdprompt* w następujący sposób:

```
default:
 pwdprompt = "Hasło: "
```

Podanie wartości "Hasło: " dla parametru *pwdprompt* spowoduje, że określone pytanie będzie wyświetlane podczas logowania, a także przez inne aplikacje, które korzystają z systemowego pytania o hasło. Pytanie dla logowania po skonfigurowaniu niestandardowego pytania wygląda następująco:

```
login: foo
Hasło:
```

Konfigurowanie domyślnych systemowych parametrów logowania
W celu skonfigurowania domyślnych systemowych parametrów logowania należy zmodyfikować plik `/etc/security/login.cfg`.

Aby skonfigurować podstawowe wartości domyślne wielu parametrów logowania, które mogą zostać skonfigurowane dla nowego użytkownika (liczba prób logowania, odblokowanie możliwości logowania i logowanie wewnętrzne), należy zmodyfikować plik `/etc/security/login.cfg`.

Zabezpieczanie terminali nienadzorowanych
W celu zabezpieczenia terminalu należy użyć komendy **lock** i **xlock**.

Wszystkie systemy są podatne na atak, jeśli terminale są pozostawiane w stanie zalogowania bez nadzoru. Najpoważniejszy problem występuje wtedy, gdy menedżer systemu pozostawi bez nadzoru terminal, który ma uprawnienia użytkownika root. Użytkownicy powinni wylogować się więc za każdym razem, gdy oddalają się od terminali. Pozostawienie niechronionych terminali naraża system na potencjalne ryzyko. Aby zablokować terminal, należy użyć komendy **lock**. Jeśli interfejsem jest AIXwindows, należy użyć komendy **xlock**.

Włączanie automatycznego wylogowania
Należy aktywować automatyczne wylogowanie, aby zapobiec naruszeniu bezpieczeństwa systemu przez włamywaczy.

Inne istotne zagadnienia związane z bezpieczeństwem wynikają z tego, że użytkownicy pozostawiają swoje konta bez nadzoru przez długi okres. Taka sytuacja umożliwia włamywaczowi przejęcie kontroli nad terminalem użytkownika, co potencjalnie narusza bezpieczeństwo systemu.

Aby zapobiec tego typu potencjalnym zagrożeniom, można włączyć w systemie funkcję automatycznego wylogowywania. W tym celu należy ustawić wartości zmiennych środowiskowych TMOUT i TIMEOUT na liczbę sekund dozwolonej nieaktywności. Po upłynięciu tego czasu użytkownik jest wylogowywany automatycznie. Przykład definicji:

```
TMOUT=600; TIMEOUT=600; export TMOUT TIMEOUT
```

W powyższym przykładzie liczba 600 oznacza sekundy (600 sekund = 10 minut). Ta metoda działa tylko dla powłoki. Zmienne mogą być zabezpieczone przed przypadkowym nadpisaniem przez oznaczenie ich jako tylko do odczytu:

```
readonly TMOUT TIMEOUT
```

Zmienne środowiskowe TMOUT i TIMEOUT są ustawiane w pliku .profile użytkownika lub w pliku `/etc/security/.profile`. Pozwala to na dodawanie pliku do pliku .profile użytkownika w momencie zakładania użytkownika.

Zabezpieczenie przez wyłączenie wykonywania w stosie (Stack Execution Disable - SED)
Zapewnienie bezpieczeństwa systemów komputerowych stanowi ważny aspekt zwiększania mocy obliczeniowej na żądanie. W dzisiejszym świecie rozbudowanych środowisk sieciowych niezwykle ważne staje się odpieranie ataków z różnych źródeł.

Rośnie zagrożenie systemów komputerowych przez zaawansowane ataki prowadzące do zakłócenia codziennej działalności przedsiębiorstw i urzędów publicznych. Ponieważ żadne pojedyncze zabezpieczenie nie może zapewnić niezawodnej ochrony przed atakami, konieczne jest wdrożenie wielu mechanizmów zabezpieczeń, aby odeprzeć ataki na bezpieczeństwo systemu. Ta sekcja dotyczy mechanizmu zabezpieczeń używanego w systemie AIX w celu odparcia ataków polegających na wykonaniu kodu z wykorzystaniem przepełnienia buforu.

Naruszenia bezpieczeństwa występują w wielu formach, ale jedną z najpopularniejszych metod jest monitorowanie systemowych narzędzi administracyjnych w poszukiwaniu sytuacji przepełnienia buforu i wykorzystywanie ich. Ataki wykorzystujące przepełnienie buforu mogą nastąpić, kiedy wewnętrzny bufor programu zostanie nadpisany, ponieważ dane (pochodzące np. z wiersza komend, zmiennej środowiskowej, dysku lub terminalu we/wy) nie zostały odpowiednio sprawdzone. Przy użyciu przepełnienia buforu atakujący kod jest wstawiany do działającego procesu i zmienia jego ścieżkę wykonania. Adres zwrotny zostaje nadpisany i przekierowany do lokalizacji wstawionego kodu. Częste przyczyny naruszenia bezpieczeństwa to niewłaściwe sprawdzanie zakresu lub brak tego sprawdzenia oraz niepoprawne założenia dotyczące poprawności źródeł danych. Przepełnienie buforu może wystąpić, na przykład, kiedy obiekt danych może przechowywać 1 kB danych, ale program nie sprawdza zakresu danych wejściowych i dlatego możliwe jest skopiowanie do tego obiektu większej ilości danych niż 1 kB.

Celem włamywacza jest zaatakowanie komendy lub narzędzia, które udostępnia zwykłemu użytkownikowi uprawnienia użytkownika root. Można w ten sposób uzyskać kontrolę nad programem przy włączonych wszystkich uprawnieniach, co pozwala na przepełnianie buforów. Ataki są zwykle ukierunkowane na zestaw UID należący do użytkownika root lub na programy prowadzące do wykonania powłoki, aby w ten sposób uzyskać dostęp z powłoki do systemu z uprawnieniami użytkownika root.

Atakom tym można zapobiec, blokując wykonywanie kodu atakującego wprowadzonego przez przepełnienie buforu. Należy wyłączyć wykonywanie w obszarach pamięci procesu, w których wykonywanie zwykle nie następuje (obszary pamięci stosu i sterty).

Mechanizm SED chroniący przed przepełnieniem buforu
W systemie AIX włączony jest mechanizm SED (Stack Execution Disable), który wyłącza wykonywanie kodu w stosie i w wybranych obszarach danych procesu.

Wyłączenie wykonywania a następnie zakończenie programu naruszającego zabezpieczenia uniemożliwia włamywaczowi uzyskanie uprawnień użytkownika root za pomocą ataku wykorzystującego przepełnienie buforu. Opcja ta nie zapobiega wprawdzie przepełnieniu buforu, ale zapewnia bezpieczeństwo przez wyłączenie wykonywania kodu atakującego w buforach, które zostały przepełnione.

Począwszy od rodziny procesorów POWER4 można korzystać z opcji włączania i/lub wyłączania wykonywania dla pamięci na poziomie strony. Mechanizm SED systemu AIX wykorzystuje tę funkcję sprzętową do zaimplementowania opcji blokady wykonywania w wybranych obszarach pamięci. Po włączeniu tej opcji system operacyjny sprawdza i oznacza różne pliki w programach wykonywalnych. Następnie wysyła do menedżera pamięci systemu operacyjnego i menedżerów procesów informację, że mechanizm SED jest włączony dla tworzonego procesu. Wybrane obszary pamięci są zaznaczane do blokady wykonywania. Jeśli w zaznaczonych obszarach zostanie wykonany jakikolwiek kod, sprzęt wygeneruje flagę wyjątku i system operacyjny zatrzyma odpowiedni proces. Szczegóły dotyczące wyjątku i zakończenia aplikacji są przechwytywane przez zdarzenia protokołu błędów systemu AIX.

Mechanizm SED jest implementowany głównie za pomocą komendy **sedmgr**. Komenda **sedmgr** umożliwia sterowanie trybem działania SED w całym systemie oraz ustawianie flag SED dla plików wykonywalnych.

Tryby i monitorowanie SED
Mechanizm SED w systemie AIX jest implementowany za pomocą systemowych flag trybów oraz za pomocą indywidualnych flag w nagłówkach plików wykonywalnych.

Flagi systemowe sterują działaniem SED w całym systemie, natomiast flagi na poziomie pliku wskazują sposób traktowania poszczególnych plików przez mechanizm SED. Mechanizm ochrony przed przepełnieniem buforu udostępnia cztery systemowe tryby działania:

off (wyłączony)
Mechanizm SED jest wyłączony i nie ma procesów zaznaczonych do ochrony SED.

select (wybór)
Tylko wybrany zestaw plików jest aktywowany i monitorowany przez mechanizm SED. Przynależność pliku do wybranego zestawu jest określana przez sprawdzenie flag dotyczących SED w nagłówkach binarnych programów wykonywalnych. Jeśli w nagłówku programu wykonywalnego flagi te są włączone, oznacza to żądanie uwzględnienia pliku w trybie **select**.

setidfiles (pliki setid)
Umożliwia włączenie mechanizmu SED nie tylko dla plików z odpowiednim żądaniem, ale także dla wszystkich ważnych plików systemowych **setuid** i **setgid**. W tym trybie system operacyjny włącza mechanizm SED nie tylko dla plików z ustawioną flagą SED **request** (żądanie), ale także dla plików wykonywalnych z następującymi charakterystykami (oprócz plików zaznaczonych w nagłówkach jako *exempt* - wyłączone):

- pliki SETUID należące do użytkownika root,
- pliki SETGID z podstawową grupą **system** lub **security**.

all (wszystkie)
Wszystkie programy wykonywalne załadowane w systemie są chronione mechanizmem SED, z wyjątkiem plików zaznaczonych jako wykluczone z trybu SED. Flagi wykluczenia znajdują się w nagłówkach programów wykonywalnych.

Opcja SED w systemie AIX daje także możliwość monitorowania procesów w razie wystąpienia wyjątku, zamiast ich zatrzymywania. Ta systemowa opcja kontroli umożliwia administratorowi systemu sprawdzanie sytuacji awaryjnych i problemowych w środowisku systemowym przez ich monitorowanie, jeszcze przed wdrożeniem mechanizmu SED w systemach produkcyjnych.

Komenda **sedmgr** udostępnia opcję umożliwiającą włączenie mechanizmu SED w celu monitorowania plików zamiast zatrzymywania procesów w razie wystąpienia wyjątku. Administrator systemu może ocenić, czy dany przypadek wykonywania kodu programu wykonywalnego w stosie jest uzasadniony. Ustawienie to działa w połączeniu z trybem systemowym przy użyciu opcji `-c`. Kiedy włączony jest tryb **monitor**, system pozwala na kontynuowanie działania procesu, nawet jeśli wystąpił wyjątek dotyczący SED. Zamiast zatrzymywania procesu wyjątek jest rejestrowany w protokole błędów systemu AIX. Jeśli monitorowanie SED jest wyłączone, system operacyjny zatrzymuje każdy proces naruszający zasady i powodujący wyjątek narzędzia SED.

Każda zmiana systemowych flag trybu SED odniesie skutek dopiero po zrestartowaniu systemu. Kontrolowane są wszystkie typy zdarzeń.

Flagi SED dla plików wykonywalnych
W systemie AIX można użyć komendy **sedmgr** w celu oznaczenia plików wykonywalnych na potrzeby mechanizmu SED.

Konsolidator został rozszerzony o obsługę dwóch nowych flag dotyczących mechanizmu SED, aby umożliwić włączanie opcji `select` (wybór) i `exempt` (wykluczenie) w nagłówkach plików wykonywalnych. Opcja **select** oznacza, że plik wykonywalny może zostać uwzględniony w ochronie SED, kiedy funkcja SED działa w systemowym trybie `select`, natomiast opcja **exempt** oznacza, że plik wykonywalny może zostać wykluczony z mechanizmu SED. Pliki wykonywalne oznaczone tą flagą nie podlegają wyłączeniu wykonywania w żadnym obszarze pamięci procesu.

Flaga wykluczenia umożliwia administratorowi systemu monitorowanie mechanizmu SED i ocenę sytuacji. Administrator systemu może włączyć wykonywanie w stosie i w obszarach danych, które uzna za potrzebne dla aplikacji, oceniając samodzielnie związane z tym ryzyko.

W następującej tabeli przedstawiono, jak ustawienia systemowe i ustawienia pliku wpływają na tryb działania SED:

Tabela 2. Ustawienia systemowe i ustawienia pliku wpływające na tryb SED				
	Flagi SED w plikach wykonywalnych			
Systemowy tryb SED	**request**	**exempt**	**system**	**Pliki setuid-root lub setgid-system/security**
off (wyłączony)	–	–	–	–
select (wybór)	włączone	–	–	–
setgidfiles (pliki setgid)	włączone	–	–	włączone
all (wszystkie)	włączone	–	włączone	włączone

Problemy i uwagi dotyczące mechanizmu SED
Domyślnie mechanizm SED w systemie AIX jest dostarczany w trybie **select**. Wiele programów typu **setuid** i **setgid** jest w trybie **select** włączonych dla mechanizmu SED i domyślnie działa w trybie chronionym.

Włączenie mechanizmu SED może spowodować awarię starszych plików binarnych, które nie są w stanie obsługiwać opcji blokady wykonywania w obszarach stert stosów. Te aplikacje muszą działać w obszarach danych stosów. Administrator systemu może ocenić sytuację i zaznaczyć plik, jako wykluczony, za pomocą komendy **bopmgr**. Środowiska AIX Java™ 1.3.1 i AIX Java 1.4.2 dysponują kompilatorami JIT (Just-In-Time), które dynamicznie generują i uruchamiają rodzimy kod obiektu podczas działania aplikacji Java (wirtualna maszyna języka Java decyduje, który kod należy skompilować, na podstawie profilu wykonywania aplikacji). Ten kod obiektu jest przechowywany w buforach danych przydzielanych przez kompilator JIT. W związku z tym, jeśli system AIX jest skonfigurowany do działania w trybie SED **ALL**, administrator systemu musi ustawić w binarnym pliku Java flagę wykluczenia.

Zmiana flag dotyczących SED w pliku wykonywalnym będzie zastosowana dopiero przy następnym załadowaniu i wykonaniu pliku. Zmiana ta nie jest stosowana do procesów aktualnie działających na podstawie tego pliku. Narzędzie SED kontroluje i monitoruje programy wykonywalne 32- i 64-bitowe pod kątem użycia ustawień systemowych i ustawień na poziomie pliku. Narzędzie SED jest dostępne tylko wtedy, gdy system operacyjny AIX jest używany z jądrem 64-bitowym.

Informacje pokrewne

Komenda **sedmgr**

Narzędzie rejestrowania błędów systemu AIX

Uwagi dotyczące zarządzania środowiskami X11 i CDE
W przypadku używania serwera X-Window X11 i Uniwersalnego Środowiska Graficznego (Common Desktop Environment - CDE) występują pewne potencjalne zagrożenia bezpieczeństwa.

Usuwanie pliku /etc/rc.dt
W systemach wymagających wysokiego poziomu bezpieczeństwa należy usunąć plik `/etc/rc.dt`.

Mimo iż interfejs CDE jest wygodny dla użytkowników, są z nim związane problemy z bezpieczeństwem. Z tego powodu nie należy uruchamiać środowiska CDE na serwerach wymagających wysokiego poziomu bezpieczeństwa. Najlepszym rozwiązaniem jest unikanie instalowania zestawów plików CDE (dt). Jeśli te zestawy plików zostały zainstalowane w systemie, należy wziąć pod uwagę ich odinstalowanie, w szczególności skryptu `/etc/rc.dt`, który uruchamia środowisko CDE.

Więcej informacji na temat środowiska CDE znajduje się w publikacji *Zarządzanie systemami operacyjnymi i urządzeniami*.

Blokowanie nieautoryzowanego monitorowania zdalnego serwera X
Istotnym problemem bezpieczeństwa związanym z serwerem X11 jest nieautoryzowane ciche monitorowanie zdalnego serwera.

Komendy **xwd** i **xwud** mogą być użyte w celu monitorowania działania serwera X, ponieważ umożliwiają one przejmowanie naciśnięć klawiszy, co może doprowadzić do ujawnienia haseł i innych danych objętych szczególnym zabezpieczeniem. Aby rozwiązać ten problem, należy usunąć te pliki wykonywalne, jeśli nie są one niezbędne w danej konfiguracji, lub dać dostęp do tych komend tylko użytkownikom root.

Komendy **xwd** i **xwud** znajdują się w zestawie plików `X11.apps.clients`.

Jeśli konieczne jest pozostawienie komend **xwd** i **xwud**, należy rozważyć użycie programów OpenSSH lub MIT Magic Cookies. Są to aplikacje pochodzące od innych firm, eliminujące ryzyko powstające w przypadku uruchomienia komend **xwd** i **xwud**.

Więcej informacji na temat aplikacji OpenSSH i MIT Magic Cookies znajduje się w dokumentacji każdej z tych aplikacji.

Włączanie i wyłączanie kontroli dostępu
Serwer X umożliwia zdalnym hostom używanie komendy **xhost +** do łączenia się z systemem użytkownika.

Należy upewnić się, że w komendzie **xhost +** została określona nazwa hosta, ponieważ powoduje ona wyłączenie kontroli dostępu dla serwera X. Umożliwia to przyznanie dostępu określonym hostom, co ułatwia monitorowanie potencjalnych ataków na serwer X. Aby nadać prawo dostępu określonemu hostowi, należy uruchomić komendę **xhost** w następujący sposób:

```
# xhost + nazwa hosta
```

Jeśli nazwa hosta nie zostanie określona, dostęp będzie przyznany wszystkim hostom.

więcej informacji na temat komendy **xhost** znajduje się w publikacji *Commands Reference*

Blokowanie uprawnień do uruchamiania komendy xhost
Wykonywaniu komendy **xhost** bez uprawnień można zapobiec, używając komendy **chmod**.

Innym sposobem zapewnienia, że komenda **xhost** jest wykorzystywana właściwie, jest ograniczenie uprawnień do wykonywania tej komendy tylko do użytkowników o uprawnieniach użytkownika root. Aby to zrobić, należy użyć komendy **chmod** w celu zmiany uprawnień do pliku `/usr/bin/X11/xhost` na 744:

```
chmod 744/usr/bin/X11/xhost
```

Lista programów setuid/setgid
W systemie AIX dostępne są różne programy setuid/setgid. Dostępne uprawnienia można usuwać dla komend, które nie muszą być dostępne dla zwykłych użytkowników.

Normalna instalacja systemu AIX obejmuje podane poniżej programy. W systemie AIX skonfigurowanym z CC ta lista zawiera mniej programów.

- `/opt/IBMinvscout/bin/invscoutClient_VPD_Survey`
- `/opt/IBMinvscout/bin/invscoutClient_PartitionID`
- `/usr/lpp/diagnostics/bin/diagsetrto`
- `/usr/lpp/diagnostics/bin/Dctrl`
- `/usr/lpp/diagnostics/bin/diagela`
- `/usr/lpp/diagnostics/bin/diagela_exec`
- `/usr/lpp/diagnostics/bin/diagrpt`
- `/usr/lpp/diagnostics/bin/diagrto`
- `/usr/lpp/diagnostics/bin/diaggetrto`
- `/usr/lpp/diagnostics/bin/update_manage_flash`
- `/usr/lpp/diagnostics/bin/utape`
- `/usr/lpp/diagnostics/bin/uspchrp`
- `/usr/lpp/diagnostics/bin/update_flash`

- /usr/lpp/diagnostics/bin/uesensor
- /usr/lpp/diagnostics/bin/usysident
- /usr/lpp/diagnostics/bin/usysfault
- /usr/lpp/X11/bin/xlock
- /usr/lpp/X11/bin/aixterm
- /usr/lpp/X11/bin/xterm
- /usr/lpp/X11/bin/msmitpasswd
- /usr/lib/boot/tftp
- /usr/lib/lpd/digest
- /usr/lib/lpd/rembak
- /usr/lib/lpd/pio/etc/piodmgrsu
- /usr/lib/lpd/pio/etc/piomkpq
- /usr/lib/lpd/pio/etc/pioout
- /usr/lib/mh/slocal
- /usr/lib/perf/libperfstat_updt_dictionary
- /usr/lib/sa/sadc
- /usr/lib/semutil
- /usr/lib/trcload
- /usr/sbin/allocp
- /usr/sbin/audit
- /usr/sbin/auditbin
- /usr/sbin/auditcat
- /usr/sbin/auditconv
- /usr/sbin/auditmerge
- /usr/sbin/auditpr
- /usr/sbin/auditselect
- /usr/sbin/auditstream
- /usr/sbin/backbyinode
- /usr/sbin/cfgmgr
- /usr/sbin/chcod
- /usr/sbin/chcons
- /usr/sbin/chdev
- /usr/sbin/chpath
- /usr/sbin/chtcb
- /usr/sbin/cron
- /usr/sbin/acct/accton
- /usr/sbin/arp64
- /usr/sbin/arp
- /usr/sbin/devinstall
- /usr/sbin/diag_exec
- /usr/sbin/entstat
- /usr/sbin/entstat.ethchan
- /usr/sbin/entstat.scent

- /usr/sbin/diskusg
- /usr/sbin/exec_shutdown
- /usr/sbin/fdformat
- /usr/sbin/format
- /usr/sbin/fuser
- /usr/sbin/fuser64
- /usr/sbin/getlvcb
- /usr/sbin/getlvname
- /usr/sbin/getvgname
- /usr/sbin/grpck
- /usr/sbin/getty
- /usr/sbin/extendvg
- /usr/sbin/fastboot
- /usr/sbin/frcactrl64
- /usr/sbin/frcactrl
- /usr/sbin/inetd
- /usr/sbin/invscout
- /usr/sbin/invscoutd
- /usr/sbin/ipl_varyon
- /usr/sbin/keyenvoy
- /usr/sbin/krlogind
- /usr/sbin/krshd
- /usr/sbin/lchangelv
- /usr/sbin/lchangepv
- /usr/sbin/lchangevg
- /usr/sbin/lchlvcopy
- /usr/sbin/lcreatelv
- /usr/sbin/ldeletelv
- /usr/sbin/ldeletepv
- /usr/sbin/lextendlv
- /usr/sbin/lmigratelv
- /usr/sbin/lmigratepp
- /usr/sbin/lparsetres
- /usr/sbin/lpd
- /usr/sbin/lquerylv
- /usr/sbin/lquerypv
- /usr/sbin/lqueryvg
- /usr/sbin/lqueryvgs
- /usr/sbin/lreducelv
- /usr/sbin/lresynclp
- /usr/sbin/lresynclv
- /usr/sbin/lsaudit
- /usr/sbin/lscfg

- /usr/sbin/lscons
- /usr/sbin/lslv
- /usr/sbin/lspath
- /usr/sbin/lspv
- /usr/sbin/lsresource
- /usr/sbin/lsrset
- /usr/sbin/lsslot
- /usr/sbin/lsuser
- /usr/sbin/lsvg
- /usr/sbin/lsvgfs
- /usr/sbin/login
- /usr/sbin/lvaryoffvg
- /usr/sbin/lvaryonvg
- /usr/sbin/lvgenmajor
- /usr/sbin/lvgenminor
- /usr/sbin/lvrelmajor
- /usr/sbin/lvrelminor
- /usr/sbin/lsmcode
- /usr/sbin/mailq
- /usr/sbin/mkdev
- /usr/sbin/mklvcopy
- /usr/sbin/mknod
- /usr/sbin/mkpasswd
- /usr/sbin/mkpath
- /usr/sbin/mkvg
- /usr/sbin/mount
- /usr/sbin/netstat64
- /usr/sbin/mtrace
- /usr/sbin/ndp
- /usr/sbin/newaliases
- /usr/sbin/named9
- /usr/sbin/named8
- /usr/sbin/netstat
- /usr/sbin/nfsstat
- /usr/sbin/pdelay
- /usr/sbin/pdisable
- /usr/sbin/penable
- /usr/sbin/perf/diag_tool/getschedparms
- /usr/sbin/perf/diag_tool/getvmparms
- /usr/sbin/phold
- /usr/sbin/portmir
- /usr/sbin/pshare
- /usr/sbin/pstart

- /usr/sbin/putlvcb
- /usr/sbin/putlvodm
- /usr/sbin/qdaemon
- /usr/sbin/quota
- /usr/sbin/reboot
- /usr/sbin/redefinevg
- /usr/sbin/repquota
- /usr/sbin/restbyinode
- /usr/sbin/rmdev
- /usr/sbin/ping
- /usr/sbin/rmgroup
- /usr/sbin/rmpath
- /usr/sbin/rmrole
- /usr/sbin/rmuser
- /opt/rsct/bin/ctstrtcasd
- /usr/sbin/srcd
- /usr/sbin/srcmstr
- /usr/sbin/rmsock64
- /usr/sbin/sendmail_ssl
- /usr/sbin/sendmail_nonssl
- /usr/sbin/rmsock
- /usr/sbin/sliplogin
- /usr/sbin/sendmail
- /usr/sbin/rwhod
- /usr/sbin/route
- /usr/sbin/snappd
- /usr/sbin/swap
- /usr/sbin/swapoff
- /usr/sbin/swapon
- /usr/sbin/swcons
- /usr/sbin/switch.prt
- /usr/sbin/synclvodm
- /usr/sbin/tsm
- /usr/sbin/umount
- /usr/sbin/umountall
- /usr/sbin/unmount
- /usr/sbin/varyonvg
- /usr/sbin/watch
- /usr/sbin/talkd
- /usr/sbin/timedc
- /usr/sbin/uucpd
- /usr/bin/bellmail
- /usr/bin/at

- /usr/bin/capture
- /usr/bin/chcore
- /usr/bin/acctras
- /usr/bin/acctctl
- /usr/bin/chgroup
- /usr/bin/chkey
- /usr/bin/chque
- /usr/bin/chquedev
- /usr/bin/chrole
- /usr/bin/chsec
- /usr/bin/chuser
- /usr/bin/confsrc
- /usr/bin/crontab
- /usr/bin/enq
- /usr/bin/filemon
- /usr/bin/errpt
- /usr/bin/fileplace
- /usr/bin/fileplacej2
- /usr/bin/fileplacej2_64
- /usr/bin/ftp
- /usr/bin/getconf
- /usr/bin/ipcs
- /usr/bin/ipcs64
- /usr/bin/iostat
- /usr/bin/logout
- /usr/bin/lscore
- /usr/bin/lssec
- /usr/bin/mesg
- /usr/bin/mkgroup
- /usr/bin/mkque
- /usr/bin/mkquedev
- /usr/bin/mkrole
- /usr/bin/mkuser
- /usr/bin/netpmon
- /usr/bin/newgrp
- /usr/bin/pagdel
- /usr/bin/paginit
- /usr/bin/paglist
- /usr/bin/passwd
- /usr/bin/pwck
- /usr/bin/pwdadm
- /usr/bin/pwdck
- /usr/bin/rm_mlcache_file

- /usr/bin/rdist
- /usr/bin/remsh
- /usr/bin/rlogin
- /usr/bin/rexec
- /usr/bin/rcp
- /usr/bin/rmque
- /usr/bin/rmquedev
- /usr/bin/rsh
- /usr/bin/ruptime
- /usr/bin/rwho
- /usr/bin/script
- /usr/bin/setgroups
- /usr/bin/setsenv
- /usr/bin/shell
- /usr/bin/su
- /usr/bin/sysck
- /usr/bin/tcbck
- /usr/bin/sysck_r
- /usr/bin/telnet
- /usr/bin/tftp
- /usr/bin/traceroute
- /usr/bin/tn
- /usr/bin/tn3270
- /usr/bin/usrck
- /usr/bin/utftp
- /usr/bin/vmstat
- /usr/bin/vmstat64
- /usr/bin/yppasswd
- /sbin/helpers/jfs2/backbyinode
- /sbin/helpers/jfs2/diskusg
- /sbin/helpers/jfs2/restbyinode

Użytkownicy, grupy i hasła

Możliwe jest zarządzanie użytkownikami i grupami systemu AIX.

Automatyczne tworzenie katalogu osobistego podczas logowania
System operacyjny AIX może automatycznie tworzyć katalog osobisty podczas logowania użytkownika.

Ta opcja jest przydatna dla zdalnie definiowanych użytkowników (na przykład dla użytkowników zdefiniowanych na serwerze LDAP), którzy mogą nie mieć katalogu osobistego w systemie lokalnym. System operacyjny AIX udostępnia dwa mechanizmy umożliwiające automatyczne tworzenie katalogu osobistego podczas logowania użytkownika: standardowy mechanizm systemu AIX i mechanizm PAM. Mechanizmy te mogą być włączone jednocześnie.

Mechanizm systemu AIX
Mechanizm systemu AIX obsługuje logowanie za pomocą następujących komend: **getty**, **login**, **rlogin**, **rsh**, **telnet** i **tsm**. Mechanizm systemu AIX obsługuje uwierzytelnianie STD_AUTH i uwierzytelnianie PAM_AUTH za pomocą modułu pam_aix. Mechanizm systemu AIX włącza się w pliku **/etc/security/**

login.cfg, ustawiając wartość `true` dla atrybutu mkhomeatlogin w sekcji usw (dodatkowe informacje o tym pliku zawiera plik `/etc/security/login.cfg`). Aby włączyć lub wyłączyć opcję automatycznego tworzenia katalogu osobistego podczas logowania, należy użyć komendy **chsec**. Na przykład, aby włączyć tę opcję, uruchom komendę:

```
# chsec -f /etc/security/login.cfg -s usw -a mkhomeatlogin=true
```

Gdy opcja ta jest włączona, proces logowania po pomyślnym uwierzytelnieniu sprawdza, czy katalog osobisty użytkownika istnieje. Jeśli katalog osobisty użytkownika nie istnieje, zostanie utworzony.

Uwaga: Atrybut **mkhomeatlogin** jest obsługiwany tylko w systemie AIX wersja 6.1 z pakietem Technology Level 6100-02 lub nowszym.

Mechanizm PAM

System AIX udostępnia ponadto moduł pam_mkuserhome umożliwiający tworzenie katalogów osobistych przez mechanizmy PAM. Moduł pam_mkuserhome można układać w stos z innymi modułami sesji dla usług logowania. Aby włączyć ten moduł PAM dla usługi, do tej usługi należy dodać odpowiednią pozycję. Na przykład, aby włączyć tworzenie katalogu osobistego za pomocą komendy **telnet** z wykorzystaniem PAM, do pliku **/etc/pam.cfg** należy dodać następującą pozycję:

```
telnet session optional pam_mkuserhome
```

Identyfikator konta

Każde konto użytkownika ma liczbowy identyfikator, który jednoznacznie je identyfikuje. W systemie operacyjnym AIX autoryzacja jest nadawana na podstawie identyfikatora konta.

Ważne jest zrozumienie, że konta z takim samym identyfikatorem są wirtualnie jednym kontem. Podczas tworzenia użytkowników i grup komendy **mkuser** i **mkgroup** systemu AIX zawsze sprawdzają w rejestrze docelowym, czy identyfikator tworzonego konta nie będzie kolidować z istniejącymi kontami.

Przy użyciu atrybutu systemowego `dist_uniqid` można także tak skonfigurować system, aby podczas tworzenia konta były sprawdzane wszystkie rejestry użytkowników (grup). Atrybut `dist_uniqid` sekcji usw w pliku `/etc/security/login.cfg` może być zarządzany przy użyciu komendy **chsec**. W celu skonfigurowania systemu w taki sposób, aby zawsze sprawdzał wszystkie rejestry pod względem kolizji identyfikatorów, należy uruchomić komendę:

```
# chsec -f /etc/security/login.cfg -s usw -a dist_uniqid=always
```

Atrybut `dist_uniqid` może przyjmować trzy wartości:

never

W przypadku tej wartości kolizja identyfikatorów nie jest sprawdzana w rejestrach różnych od docelowego (ustawienie domyślne).

always

W przypadku tej wartości kolizja identyfikatorów jest sprawdzana we wszystkich innych rejestrach. Jeśli zostanie wykryta kolizja między rejestrem docelowym i dowolnym innym rejestrem, komenda **mkuser** (**mkgroup**) pobierze unikalny identyfikator, który nie jest używany w żadnym rejestrze. Komenda nie powiedzie się tylko wtedy, gdy wartość identyfikatora została podana w wierszu komend (na przykład `mkuser id=234 foo`, a identyfikator 234 jest już zajęty przez użytkownika w jednym z rejestrów).

uniqbyname

W przypadku tej wartości kolizja identyfikatorów jest sprawdzana we wszystkich innych rejestrach. Kolizja między rejestrami jest dozwolona tylko wtedy, gdy tworzone konto ma nazwę taką samą, jak istniejące konto, i użyto komendy typu `mkuser id=123 foo`. Jeśli identyfikator nie został podany w wierszu komend, nowe konto może nie mieć takiej samej wartości identyfikatora, jak konto o takiej samej nazwie istniejące w innym rejestrze. Na przykład konto *acct1* z identyfikatorem 234 jest kontem lokalnym. Podczas tworzenia konta LDAP *acct1* komenda `mkuser -R LDAP acct1` może pobrać dla konta LDAP unikalny identyfikator równy 235. W rezultacie otrzymamy lokalne konto *acct1* z identyfikatorem 234 i konto LDAP *acct1* z identyfikatorem 235.

Uwaga: Wykrywanie kolizji identyfikatorów w rejestrze docelowym jest wymuszane zawsze, niezależnie od wartości atrybutu `dist_uniqid`.

Wartość **uniqbyname** działa dobrze w przypadku dwóch rejestrów. Jeśli istnieją więcej niż dwa rejestry i istnieje już kolizja identyfikatorów między dwoma rejestrami, działanie komendy **mkuser** (**mkgroup**) podczas tworzenia nowego konta w trzecim rejestrze przy użyciu kolidujących wartości identyfikatorów będzie nieokreślone. Utworzenie nowego konta może się powieść lub nie, zależnie od kolejności sprawdzania rejestrów.

Na przykład: załóżmy, że w systemie skonfigurowane są trzy rejestry: lokalny, LDAP i DCE. W rejestrze LDAP istnieje konto *acct1*, a w rejestrze DCE istnieje konto *acct2* i oba te konta mają identyfikator 234. Kiedy administrator systemu tworzy konto lokalne, wykonując komendę `mkuser -R files id=234 acct1` (`mkgroup -R files id=234 acct1`), a atrybut ma wartość **uniqbyname**, komenda **mkuser** (**mkgroup**) sprawdza najpierw rejestr LDAP i znajduje tam identyfikator 234 użyty przez konto LDAP *acct1*. Ponieważ tworzone konto ma mieć taką samą nazwę, komenda **mkuser** (**mkgroup**) pomyślnie utworzy konto lokalne *acct1* z identyfikatorem 234. Jeśli najpierw zostanie sprawdzony rejestr DCE, komenda **mkuser** (**mkgroup**) znajdzie tam identyfikator 234 użyty przez konto DCE *acct2* i tworzenie konta lokalnego *acct1* nie powiedzie się. Sprawdzanie rejestrów pod względem kolizji identyfikatorów wymusza niepowtarzalność identyfikatorów między rejestrem lokalnym i rejestrami zdalnymi lub między rejestrami zdalnymi. Nie zapewnia niepowtarzalności identyfikatorów między nowo utworzonym kontem w rejestrze zdalnym i użytkownikami lokalnymi istniejącymi w innych systemach, korzystających z tego samego rejestru zdalnego. Komenda **mkuser** (**mkgroup**) pomija rejestr zdalny, jeśli nie jest on osiągalny podczas jej wykonywania.

Konto użytkownika root

Konto użytkownika root ma praktycznie nieograniczony dostęp do wszystkich programów, plików i zasobów w systemie.

Administrator to specjalny użytkownik w pliku `/etc/passwd` o identyfikatorze użytkownika (User ID - UID) równym `0`, którego nazwą najczęściej jest *root*. Tak więc to nie nazwa sprawia, że konto użytkownika root jest wyjątkowe, ale wartość UID równa `0`. Oznacza to, że każdy użytkownik, dla którego wartość UID jest równa `0`, ma takie same przywileje jak administrator. Ponadto konto użytkownika root zawsze jest uwierzytelniane przez lokalne pliki zabezpieczeń.

Konto użytkownika root zawsze powinno posiadać hasło, którego nigdy nie należy udostępniać. Konto to powinno mieć nadane hasło natychmiast po zainstalowaniu systemu. Tylko administrator systemu powinien je znać. Administratorzy systemu powinni wykonywać jako użytkownik root jedynie te czynności administracyjne, które wymagają uprawnień użytkownika root. Wszystkie inne czynności powinny być wykonywane za pomocą normalnych kont użytkowników.

Ostrzeżenie: Rutynowa praca w systemie z konta użytkownika root może doprowadzić do uszkodzenia systemu, ponieważ konto użytkownika root działa ponad wieloma zabezpieczeniami systemu.

Wyłączanie bezpośredniego logowania się jako użytkownik root

Popularny atak potencjalnych hakerów polega na uzyskaniu hasła użytkownika root.

Aby uniknąć tego typu ataku, można wyłączyć bezpośredni dostęp do identyfikatora użytkownika root, a następnie wymagać od administratorów systemu używania komendy **su -** w celu uzyskania uprawnień użytkownika root. Ograniczenie bezpośredniego dostępu do konta użytkownika root nie tylko sprawia, że przestaje ono być źródłem bezpośredniego ataku, ale także pozwala monitorować, którzy użytkownicy uzyskali uprawnienia użytkownika root i jak długo wykonywali czynności związane z tymi uprawnieniami. Można to zrobić, wyświetlając zawartość pliku `/var/adm/sulog`. Alternatywnie, można włączyć kontrolę systemu, która będzie raportować tego typu czynności.

Aby wyłączyć zdalne logowanie dla użytkownika root, należy poddać edycji plik `/etc/security/user`. Jako wartość parametru rlogin w sekcji dla użytkownika root należy podać False.

Przed wyłączeniem zdalnego logowania dla użytkownika root, należy sprawdzić, czy nie wystąpią sytuacje, które uniemożliwią administratorom systemu logowanie się przy użyciu konta nie będącego kontem użytkownika root. Na przykład, jeśli osobisty system plików użytkownika jest pełen, użytkownik nie będzie mógł się zalogować. Jeśli logowanie zdalne z użyciem konta użytkownika root zostanie wyłączone, a

użytkownik, który może użyć komendy **su -**, będzie miał zapełniony system plików, użytkownik root nigdy już nie będzie mógł przejąć kontroli nad systemem. Ten problem mogą obejść administratorzy systemu tworzący dla siebie osobiste systemy plików większe niż przeciętne systemy plików użytkowników.

Konta użytkowników
Istnieje kilka związanych z bezpieczeństwem zadań administracyjnych dotyczących kont użytkowników.

Zalecane atrybuty użytkownika
Administrowanie użytkownikami składa się z takich czynności, jak tworzenie użytkowników i grup oraz definiowanie ich atrybutów.

Głównym atrybutem użytkownika jest sposób jego uwierzytelniana. Użytkownicy są głównymi agentami w systemie. Ich atrybuty kontrolują ich prawa dostępu, środowisko, sposób uwierzytelniania i to jak, kiedy i gdzie mogą uzyskać dostęp do swoich kont.

Grupy to zbiory użytkowników, którzy mogą współużytkować te same uprawnienia dostępu do zabezpieczonych zasobów. Grupa posiada swój identyfikator i składają się na nią członkowie i administratorzy. Założyciel grupy jest zazwyczaj pierwszym administratorem.

Dla każdego konta użytkownika można ustawić wiele atrybutów, w tym atrybuty hasła i logowania. Listę konfigurowalnych atrybutów zawiera sekcja “Przegląd systemu limitowania pamięci dyskowej” na stronie 78. Zaleca się stosowanie następujących atrybutów:

- Każdy użytkownik powinien mieć identyfikator użytkownika, który nie jest współużytkowany z żadnym innym użytkownikiem. Wszystkie środki bezpieczeństwa i narzędzia obsługi kont działają tylko wtedy, gdy każdy z użytkowników ma unikalny identyfikator.
- Należy nadawać użytkownikom nazwy, które im odpowiadają. Najlepsze są nazwiska, ponieważ większość systemów poczty elektronicznej korzysta z identyfikatora użytkownika przy nadawaniu etykiet poczcie przychodzącej.
- Użytkowników należy dodawać, zmieniać i usuwać za pomocą interfejsu programu SMIT. Chociaż wszystkie zadania można wykonywać z wiersza komend, interfejs programu SMIT pomaga wyeliminować powstawanie mniej znaczących błędów.
- Nie należy przydzielać początkowego hasła do konta użytkownika, zanim użytkownik nie będzie gotowy do zalogowania się w systemie. Jeśli pole hasła jest zdefiniowane jako * (gwiazdka) w pliku `/etc/passwd`, informacje o koncie zostaną zachowane, ale nikt nie będzie mógł się zalogować do tego konta.
- Nie należy zmieniać zdefiniowanych przez system identyfikatorów użytkowników, które są wymagane do prawidłowej pracy systemu. Zdefiniowane przez system identyfikatory są wymienione w pliku `/etc/passwd`.
- Ogólnie, nie należy ustawiać parametru *admin* na wartość `true` dla żadnego z identyfikatorów użytkowników. Jedynie użytkownik root może zmieniać atrybuty użytkowników z ustawioną wartością `admin=true` w pliku `/etc/security/user`.

System operacyjny obsługuje standardowe atrybuty użytkowników znajdujące się zazwyczaj w pliku `/etc/passwd` i `/etc/system/group`, takie jak:

Informacje o uwierzytelnianiu
Hasło.

Wiarygodność
Identyfikator użytkownika, grupa główna i identyfikator grupy uzupełniającej.

Środowisko
Środowisko osobiste lub powłoki.

limit długości nazwy użytkownika i grupy
Istnieje możliwość skonfigurowania limitu długości nazwy użytkownika i grupy oraz pobierania go.

Domyślną wartością parametru określającego limit długości nazwy użytkownika i grupy jest 9 znaków. W systemie AIX 5.3 i w jego nowszych wersjach limit długości nazwy użytkownika i grupy można zwiększyć z

9 do 256 znaków. Ponieważ parametr określający limit długości nazwy użytkownika i grupy obejmuje kończący znak o kodzie zero, rzeczywiste poprawne długości nazw wynoszą od 8 do 255 znaków.

Limit długości nazwy użytkownika i grupy jest określony za pomocą parametru konfiguracyjnego systemu **v_max_logname** dla urządzenia `sys0`. Wartość parametru **v_max_logname** można zmieniać lub pobierać z jądra albo bazy danych ODM. Wartość tego parametru w jądrze jest wartością używaną podczas działania systemu. Wartość tego parametru w bazie danych ODM jest wartością używaną przez system po następnym restarcie.

Uwaga: Zmniejszenie limitu długości nazwy użytkownika i grupy po jego uprzednim zwiększeniu może spowodować nieprzewidywalne działanie. Nazwy użytkowników i grup utworzone przy większym limicie mogą nadal istnieć w systemie.

Pobieranie limitu długości nazwy grupy i użytkownika z bazy danych ODM
Aby pobrać parametr **v_max_logname**, można użyć komend lub procedur.

Aby pobrać parametr **v_max_logname** z bazy danych ODM, można użyć komendy **lsattr**. Komenda **lsattr** wyświetla parametr **v_max_logname** jako atrybut `max_logname`.

Więcej informacji na ten temat zawiera opis komendy **lsattr** w dokumentacji *Commands Reference, Volume 3*.

W poniższym przykładzie przedstawiono sposób użycia komendy **lsattr** do pobrania atrybutu `max_logname`:

```
$ lsattr -El sys0
SW_dist_intr    fałsz            Włącz programową dystrybucję
przerwań                           Prawda
autorestart     prawda           Automatycznie RESTARTUJ system po
awarii                         Prawda
boottype        dysk             Nie
dotyczy                                          Fałsz
capacity_inc    1.00             Przyrost mocy obliczeniowej
procesora                          Fałsz
capped          prawda           Partycja jest
limitowana                                 Fałsz
conslogin       włącz            Login na konsoli
systemowej                                 Fałsz
cpuguard        włącz            Ochrona
CPU                                              Prawda
dedicated       prawda           Partycja jest
dedykowana                                 Fałsz
ent_capacity    4.00             Uprawniona moc obliczeniowa
procesora                          Fałsz
frequency       93750000         Częstotliwość magistrali
systemowej                           Fałsz
fullcore        fałsz            Aktywowanie pełnego zrzutu
CORE                                 Prawda
fwversion       IBM,SPH01316     Wersja oprogramowania wbudowanego i poziomy
poprawek            Fałsz
iostat          fałsz            Stałe utrzymywanie historii DYSKOWYCH OPERACJI WE/
WY            Prawda
keylock         normalny         Położenie kluczyka w momencie ładowania
systemu                 Fałsz
max_capacity    4.00             Maksymalna potencjalna moc obliczeniowa
procesora               Fałsz
max_logname     20               Maksymalna długość nazwy użytkownika podczas
startu              Prawda
maxbuf          20               Maks. liczba stron PAMIĘCI PODRĘCZNEJ BUFORÓW blokowego WE/
WY    Prawda
maxmbuf         0                Maksymalna liczba kilobajtów pamięci rzeczywistej
                                 dozwolonej dla buforów
MBUF                                   Prawda
maxpout         0                GÓRNY znacznik oczekujących operacji we/wy dla
                                 pojedynczego
pliku                                        Prawda
maxuproc        128              Maksymalna liczba PROCESÓW dostępnych dla
                                 jednego
użytkownika                                      Prawda
min_capacity    1.00             Minimalna potencjalna moc obliczeniowa
procesora                Fałsz
minpout         0                DOLNY znacznik oczekujących operacji we/wy dla
                                 pojedynczego
pliku                                        Prawda
```

```
modelname       IBM,7044-270     Nazwa
maszyny                                              Fałsz
ncargs          6                Wielkość listy ARG/ENV w 4-kilobajtowych
blokach                 Prawda
pre430core      fałsz            Użyj zrzutu pamięci w stylu sprzed wersji
4.3.0                   Prawda
pre520tune      wyłącz           Tryb kompatybilności strojenia z wersjami wcześniejszymi od
520  Prawda
realmem         3145728          Ilość użytecznej pamięci fizycznej w
kilobajtach                Fałsz
rtasversion     1                Wersja Open Firmware
RTAS                                        Fałsz
sec_flags       0                Opcje
bezpieczeństwa                                       Prawda
sed_config      wybierz          Tryb wyłączenia wykonywania stosu
(SED)                          Prawda
systemid        IBM,0110B5F5F    Identyfikator sprzętu
systemowego                               Fałsz
variable_weight 0                Zmienna waga mocy obliczeniowej
procesora                        Fałsz
$
```

Pobieranie limitu długości nazwy grupy i użytkownika z jądra
Aby pobrać parametr **v_max_logname** z jądra, można użyć komend i procedur.

Użycie komendy `getconf`

Aby pobrać limit długości nazwy użytkownika i grupy z jądra, można użyć komendy **`getconf`** z parametrem **LOGIN_NAME_MAX**. Wyjście komendy **`getconf`** zawiera kończący znak o kodzie zero.

W poniższym przykładzie przedstawiono sposób użycia komendy **`getconf`** do pobrania bieżącego limitu nazwy użytkownika i grupy z jądra:

```
$ getconf LOGIN_NAME_MAX
20
$
```

Użycie procedury `sysconf`

Aby pobrać limit długości nazwy użytkownika i grupy z jądra, można użyć procedury `sysconf` z parametrem **_SC_LOGIN_NAME_MAX**.

W poniższym przykładzie przedstawiono sposób użycia procedury `sysconf` do pobrania limitu długości nazwy użytkownika i grupy z jądra:

```
#include <unistd.h>
main()
{
       long len;

       len = sysconf(_SC_LOGIN_NAME_MAX);

       printf("Limit długości nazwy wynosi %d\n", len);
}
```

Użycie procedury `sys_parm`

Aby pobrać bieżący limit długości nazwy użytkownika z jądra, można użyć procedury `sys_parm` z parametrem **SYSP_V_MAX_LOGNAME**.

W poniższym przykładzie przedstawiono sposób użycia procedury `sys_parm` do pobrania limitu długości nazwy użytkownika z jądra:

```
#include <sys/types.h>
#include <sys/var.h>
#include <errno.h>
main()
{
   int rc;
```

```
    struct vario myvar;

    rc = sys_parm (SYSP_GET, SYSP_V_MAX_LOGNAME, &myvar);

    if (!rc)
       printf("Max_login_name = %d\n", myvar.v.v_max_logname.value);
    else
       printf("sys_parm() nie powiodło się, rc = %d, errno = %d\n", rc, errno);
}
```

Zmiana limitu długości nazwy użytkownika i grupy w bazie danych ODM
Limit długości nazwy użytkownika i grupy można skonfigurować w jądrze tylko podczas fazy startu systemu. Wartość tę można zmienić w bazie danych ODM za pomocą komendy **chdev**. Zmiana jest uwzględniana po następnym restarcie systemu.

W poniższym przykładzie przedstawiono sposób użycia komendy **chdev** do zmiany parametru **v_max_logname** w bazie danych ODM:

```
$ chdev -l sys0 -a max_logname=30
sys0 changed
$
```

Kontrola kont użytkowników
Konta użytkowników mają atrybuty, które można zmieniać.

Każdy użytkownik ma przypisany zestaw atrybutów. Te atrybuty są tworzone z wartości domyślnych podczas tworzenia użytkownika za pomocą komendy **mkuser**. Można je zmienić, używając komendy **chuser**. Poniżej znajduje się lista atrybutów użytkownika, które kontrolują logowanie i nie są związane z jakością hasła:

account_locked
Jeśli konto musi zostać jawnie zablokowane, ten atrybut można ustawić na True; domyślną wartością jest False.

admin
Jeśli zostanie ustawiony na True, użytkownik nie będzie mógł zmienić swojego hasła. Może je zmienić tylko administrator.

admgroups
Wyświetla listę grup, w których użytkownik ma prawa administracyjne. Użytkownik może dodawać lub usuwać członków tych grup.

auth1
Metoda uwierzytelniania używana w celu przyznawania użytkownikowi dostępu. Zwykle jest ona ustawiona na SYSTEM, co spowoduje użycie nowszych metod.

Uwaga: Atrybut **auth1** jest nieaktualny. Nie należy go używać.

auth2
Metoda uruchamiana po uwierzytelnieniu użytkownika w sposób określony w atrybucie **auth1**. Nie może blokować dostępu do systemu. Zwykle jest on ustawiony na NONE.

Uwaga: Atrybut **auth2** jest nieaktualny. Nie należy go używać.

daemon
Ten parametr określa, czy użytkownik ma prawo uruchamiać demony lub podsystemy za pomocą komendy **startsrc**. Powoduje on również ograniczenie użycia narzędzi cron i at.

login
Określa, czy użytkownik ma prawo logowania się. Pomyślne logowanie resetuje atrybut **unsuccessful_login_count** do wartości 0 (z podprocedury **loginsuccess**).

logintimes
Ogranicza czas, w którym użytkownik może się logować. Na przykład dostęp użytkownika do systemu może zostać ograniczony tylko do godzin pracy.

registry
Określa rejestr użytkownika. Może on zostać użyty w celu poinformowania systemu o alternatywnych rejestrach informacji o użytkowniku, takich jak NIS, LDAP czy Kerberos.

rlogin
Określa, czy podany użytkownik może zalogować się za pomocą komendy **rlogin** lub **telnet**. Atrybut rlogin steruje tylko zdalnym logowaniem. Aby uzyskać informacje na temat sterowania możliwością uruchamiania poszczególnych komend zdalnych, patrz rcmds.

su
Określa, czy inni użytkownicy mogą przełączać się na ten identyfikator za pomocą komendy **su**.

sugroups
Określa, które grupy mogą przełączać się na ten identyfikator użytkownika.

ttys
Ogranicza niektóre konta do stref zabezpieczonych fizycznie.

expires
Zarządza kontami studentów lub gości; może być również użyty w celu tymczasowego wyłączenia kont.

loginretries
Określa maksymalną liczbę następujących po sobie nieudanych prób logowania, po przekroczeniu której identyfikator użytkownika zostanie zablokowany. Nieudane próby są rejestrowane w pliku `/etc/security/lastlog`.

umask
Określa początkową komendę **umask** dla użytkownika.

rcmds
Określa, czy podany użytkownik może uruchamiać poszczególne komendy za pomocą komendy **rsh** lub **rexec**. Wartość `allow` wskazuje, że można uruchamiać komendy zdalnie za pomocą komend **rsh** i **rexec**. Wartość `deny` wskazuje, że nie można uruchamiać komend zdalnie. Wartość `hostlogincontrol` wskazuje, że uruchamianiem komend zdalnych sterują atrybuty **hostallowedlogin** i **hostsdeniedlogin**. Informacje na temat sterowania zdalnym logowaniem zawiera opis atrybutu rlogin.

hostallowedlogin
Określa hosty, które zezwalają użytkownikowi na zalogowanie się. Ten atrybut przeznaczony jest dla środowiska sieciowego, w którym atrybuty użytkowników są współużytkowane przez wiele hostów.

hostsdeniedlogin
Określa hosty, które nie zezwalają użytkownikowi na zalogowanie się. Ten atrybut przeznaczony jest dla środowiska sieciowego, w którym atrybuty użytkowników są współużytkowane przez wiele hostów.

maxulogs
Określa maksymalną liczbę logowań użytkownika. Jeśli użytkownik osiągnie maksymalną liczbę dozwolonych logowań, logowanie nie powiedzie się.

Pełny zestaw atrybutów użytkownika jest zdefiniowany w plikach `/etc/security/user`, `/etc/security/limits`, `/etc/security/audit/config` i `/etc/security/lastlog`. Wartości domyślne używane przy tworzeniu użytkownika za pomocą komendy **mkuser** są określone w pliku `/usr/lib/security/mkuser.default`. W pliku `mkuser.default` trzeba określić jedynie opcje, które zastępują ogólne wartości domyślne podane w sekcjach default plików `/etc/security/user` i `/etc/security/limits`, a także klasy kontroli. Niektóre z tych atrybutów kontrolują sposób, w jaki użytkownik może się logować, i mogą zostać skonfigurowane w celu automatycznego zablokowania konta użytkownika (uniemożliwiając przyszłe próby logowania) po wystąpieniu określonych warunków.

Gdy konto użytkownika zostanie zablokowane przez system z powodu zbyt dużej liczby nieudanych prób logowania, użytkownik nie będzie mógł logować się do czasu, gdy administrator systemu zresetuje atrybut

użytkownika **unsuccessful_login_count** w pliku `/etc/security/lastlog` do wartości mniejszej niż liczba prób logowania. Można to zrobić, używając następującej komendy **chsec**:

```
chsec -f /etc/security/lastlog -s nazwa_użytkownika -a
unsuccessful_login_count=0
```

Wartości domyślne można zmienić, dokonując za pomocą komendy **chsec** edycji sekcji default w odpowiednim pliku zabezpieczeń, takim jak `/etc/security/user` lub `/etc/security/limits`. Wiele wartości domyślnych jest definiowanych na działanie standardowe. Aby jawnie określić atrybuty ustawiane przy tworzeniu nowego użytkownika, należy zmienić wpis *user* w pliku `/usr/lib/security/mkuser.default`.

W celu uzyskania informacji na temat rozszerzonych atrybutów hasła użytkownika, należy zapoznać się z sekcją “Hasła” na stronie 65.

Związane z logowaniem komendy, na które mają wpływ atrybuty użytkownika

Poniższa tabela zawiera listę atrybutów sterujących logowaniem i komend, na które atrybutu te mają wpływ.

Atrybut użytkownika	Komendy
account_locked	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
login	Ma wpływ wyłącznie na logowanie z konsoli. Wartość atrybutu **login** nie ma wpływu na komendy zdalnego logowania, komendy zdalnej powłoki ani komendy zdalnego kopiowania: **rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet** i **ftp**).
logintimes	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
rlogin	Ma wpływ wyłącznie na komendy zdalnego logowania, niektóre komendy zdalnej powłoki i niektóre komendy zdalnego kopiowania (**ssh**, **scp**, **rlogin** i **telnet**).
loginretries	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
/etc/nologin	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
rcmds=deny	**rexec**, **rsh**, **rcp**, **ssh**, **scp**
rcmds=hostlogincontrol i hostsdeniedlogin=<hosty_docelowe>	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
ttys = !REXEC, !RSH	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**
ttys = !REXEC, !RSH, /dev/pts	**rexec**, **rsh**
ttys = !REXEC, !RSH, ALL	**rexec**, **rsh**
expires	**rexec**, **rsh**, **rcp**, **ssh**, **scp**, **rlogin**, **telnet**, **ftp**, **login**

Uwaga: rsh uniemożliwia tylko wykonywanie zdalnych komend. Zdalne logowania pozostają dozwolone.

Informacje pokrewne

Procedura loginsuccess

Komenda **rexec**

Komenda **rsh**
Komenda **startsrc**
Komenda **su**

Identyfikatory logowania użytkowników
System operacyjny identyfikuje użytkowników na podstawie ich identyfikatorów logowania.

Identyfikator logowania użytkownika umożliwia systemowi śledzenie wszystkich czynności użytkownika. Po zalogowaniu się użytkownika do systemu, przed uruchomieniem początkowego programu użytkownika, system ustawia identyfikator logowania procesu na identyfikator użytkownika znaleziony w bazie danych użytkowników. Wszystkie kolejne procesy podczas sesji logowania są oznaczone tym identyfikatorem użytkownika. Te znaczniki umożliwiają śledzenie wszystkich czynności wykonywanych przez użytkownika o danym identyfikatorze logowania. Użytkownik może podczas sesji zresetować efektywny identyfikator użytkownika, rzeczywisty identyfikator użytkownika i identyfikator grupy uzupełniającej, ale nie może zmienić identyfikatora logowania użytkownika.

Zwiększanie bezpieczeństwa użytkowników za pomocą list kontroli dostępu (ACL)
Aby uzyskać odpowiedni poziom bezpieczeństwa w systemie, należy utworzyć spójną strategię bezpieczeństwa w celu zarządzania kontami użytkowników. Najczęściej używanym mechanizmem zabezpieczeń jest lista kontroli dostępu (ACL).

Aby uzyskać informacje na temat list ACL i tworzenia strategii bezpieczeństwa, należy zapoznać się z sekcją “Listy kontroli dostępu (ACL)” na stronie 123.

Zmienna środowiskowa PATH
Zmienna środowiskowa **PATH** jest istotnym elementem sterującym bezpieczeństwem. Określa ona katalogi, które są przeszukiwane w celu znalezienia komendy.

Domyślna systemowa wartość **PATH** jest określona w pliku `/etc/profile`, a każdy użytkownik ma określoną wartość **PATH** w pliku `$HOME/.profile` użytkownika. Wartość **PATH** określona w pliku `.profile` nadpisuje systemową wartość **PATH** lub dodaje do niej dodatkowe katalogi.

Nieautoryzowane zmiany zmiennej środowiskowej **PATH** mogą umożliwić użytkownikowi podszycie się pod innych użytkowników (w tym użytkowników root). Programy *podszywające się* (znane również jako *konie trojańskie*) zamieniają komendy systemowe, a następnie przechwytują informacje przeznaczone dla tych komend, takie jak hasła użytkowników.

Przypuśćmy, że użytkownik zmieni na przykład wartość **PATH** w taki sposób, aby system podczas uruchomienia komendy przeszukiwał najpierw katalog `/tmp`. Następnie umieści on w katalogu `/tmp` program o nazwie **su**, który prosi użytkownika o hasło użytkownika root, tak jak komenda **su**. Następnie program **/tmp/su** wysyła pocztą hasło użytkownika root do danego użytkownika, a potem wywołuje prawdziwą komendę **su** przed zakończeniem pracy. W tym scenariuszu dowolny użytkownik root używający komendy **su** ujawni hasło użytkownika root i nie będzie nawet tego świadomy.

Aby uniknąć problemów ze zmienną środowiskową **PATH**, należy wykonać poniższe czynności:

- W przypadku wątpliwości, należy określać pełne nazwy ścieżek. Jeśli zostanie określona pełna nazwa ścieżki, zmienna środowiskowa **PATH** zostanie zignorowana.
- Nigdy nie należy umieszczać katalogu bieżącego (określanego przez **.** - kropkę) w wartości **PATH** określonej dla użytkownika root. Nie należy nigdy umożliwiać określenia bieżącego katalogu w pliku `/etc/profile`.
- Użytkownik root powinien mieć zdefiniowaną własną zmienną PATH w prywatnym pliku `.profile`. Typowo specyfikacja na listach `/etc/profile` jest standardowym minimum dla wszystkich użytkowników, przy czym użytkownik root może wymagać większej lub mniejszej liczby katalogów, niż jest to określone domyślnie.
- Należy przestrzec użytkowników przed zmianą zawartości plików `.profile` bez konsultacji z administratorem systemu. W przeciwnym razie nieświadomy użytkownik może wprowadzić zmiany umożliwiające niezamierzony dostęp. Plik `.profile` użytkownika powinien mieć uprawnienia ustawione na 740.

- Administratorzy systemu nie powinni używać komendy **su** w celu uzyskania uprawnień użytkownika root z sesji użytkownika, ponieważ używana jest wartość **PATH** użytkownika określona w pliku `.profile`. Użytkownicy mogą tworzyć własne pliki `.profile`. Administratorzy systemu powinni logować się do komputera użytkownika jako użytkownicy root lub ze swoim własnym identyfikatorem i powinni użyć następującej komendy:

  ```
  /usr/bin/su - root
  ```

  Zapewnia ona, że podczas sesji zostanie użyte środowisko użytkownika root. Jeśli administrator systemu pracuje jako użytkownik root w sesji innego użytkownika, powinien określać pełne nazwy ścieżek podczas trwania sesji.
- Należy chronić zmienną środowiskową separatora pola wejściowego (**IFS**) przed zmianą w pliku `/etc/profile`. Zmienna środowiskowa **IFS** w pliku `.profile` może być użyta do zmiany wartości **PATH**.

Korzystanie z demona secldapclntd
Demon **secldapclntd** dynamicznie zarządza połączeniami z serwerem LDAP.

Podczas uruchamiania demon **secldapclntd** łączy się z serwerami zdefiniowanymi w pliku **/etc/security/ldap/ldap.cfg** (jedno połączenie dla jednego serwera LDAP). Później, jeśli demon **secldapclntd** stwierdzi, że połączenie LDAP ogranicza żądania przetwarzania LDAP, demon ten automatycznie ustanowi inne połączenie z bieżącym serwerem LDAP. Ten proces jest kontynuowany do momentu osiągnięcia predefiniowanej maksymalnej liczby połączeń. Po osiągnięciu maksymalnej liczby połączeń nie będą dodawane żadne nowe połączenia.

Demon **secldapclntd** okresowo sprawdza wszystkie połączenia z bieżącym serwerem LDAP. Jeśli jakiekolwiek połączenie, inne niż pierwsze połączenie, pozostaje bezczynne przez predefiniowany okres, demon zamknie to połączenie.

Maksymalną liczbę połączeń określa zmienna connectionsperserver w pliku **/etc/security/ldap/ldap.cfg**. Jeśli jednak zmienna connectionsperserver ma wartość większą niż wartość zmiennej numberofthread, demon **secldapclntd** ustawia wartość zmiennej connectionsperserver na wartość zmiennej numberofthread. Poprawne wartości zmiennej connectionsperserver należą do zakresu od 1 do 100. Wartością domyślną jest 10 (`connectionsperserver: 10`).

Zmienna connectionmissratio w pliku **/etc/security/ldap/ldap.cfg** określa kryteria nawiązywania nowych połączeń LDAP. Zmienna connectionmissratio określa wartość procentową operacji, które nie uzyskały połączeń LDAP (brak-obsługi) podczas pierwszych prób. Jeśli liczba nieudanych prób jest większa niż wartość zmiennej connectionmissratio, demon **secldapclntd** rozszerza zapytania LDAP, ustanawiając nowe połączenia LDAP (bez przekraczania liczby połączeń zdefiniowanych w zmiennej connectionsperserver). Poprawne wartości zmiennej connectionmissratio należą do zakresu od 10 do 90. Wartością domyślną jest 50 (`connectionmissratio: 50`).

Zmienna connectiontimeout w pliku **/etc/security/ldap/ldap.cfg** jest używana jako okres, przez jaki połączenia mogą pozostać bezczynne, zanim zostaną zamknięte przez demon **secldapclntd**. Poprawna wartość zmiennej connectiontimeout to 5 sekund lub więcej (nie ma limitu maksymalnego). Wartością domyślną jest 300 sekund (`connectiontimeout: 300`).

Konfigurowanie anonimowego ftp z bezpiecznym kontem użytkownika
Istnieje możliwość skonfigurowania anonimowego FTP z bezpiecznym kontem użytkownika.

W tym scenariuszu konfigurowany jest anonimowy dostęp do FTP przy użyciu bezpiecznego konta użytkownika, za pomocą interfejsu wiersza komend i skryptu.

1. Sprawdź, czy zestaw plików `bos.net.tcp.client` jest zainstalowany w systemie, wpisując następującą komendę:

   ```
   lslpp -L | grep bos.net.tcp.client
   ```

   Jeśli nic się nie wyświetli, oznacza to, że zestaw plików nie jest zainstalowany. W celu uzyskania instrukcji na temat instalowania zestawu plików zapoznaj się z publikacją *Instalowanie i przeprowadzanie migracji*.

2. Mając uprawnienia użytkownika root, przejdź do katalogu /usr/samples/tcpip. Na przykład:

```
cd /usr/samples/tcpip
```

3. Aby skonfigurować konto, uruchom następujący skrypt:

```
./anon.ftp
```

4. Po wyświetleniu komunikatu Czy na pewno chcesz zmodyfikować /home/ftp?, wpisz yes. Zostaną wyświetlone dane wyjściowe zbliżone do następujących:

```
Dodano użytkownika anonymous.
Utworzono katalog /home/ftp/bin.
Utworzono katalog /home/ftp/etc.
Utworzono katalog /home/ftp/pub.
Utworzono katalog /home/ftp/lib.
Utworzono wpis /home/ftp/dev/null.
Utworzono katalog /home/ftp/usr/lpp/msg/en_US directory.
```

5. Przejdź do katalogu /home/ftp. Na przykład:

```
cd /home/ftp
```

6. Utwórz podkatalog home, wpisując:

```
mkdir home
```

7. Zmień uprawnienia do katalogu /home/ftp/home na drwxr-xr-x, wpisując:

```
chmod 755 home
```

8. Przejdź do katalogu /home/ftp/etc, wpisując:

```
cd /home/ftp/etc
```

9. Utwórz podkatalog objrepos, wpisując:

```
mkdir objrepos
```

10. Zmień uprawnienia do katalogu /home/ftp/etc/objrepos na drwxrwxr-x, wpisując:

```
chmod 775 objrepos
```

11. Zmień właściciela i grupę dla katalogu /home/ftp/etc/objrepos na użytkownika root i grupę system, wpisując:

```
chown root:system objrepos
```

12. Utwórz podkatalog security, wpisując:

```
mkdir security
```

13. Zmień uprawnienia do katalogu /home/ftp/etc/security na drwxr-x--, wpisując:

```
chmod 750 security
```

14. Zmień właściciela i grupę dla katalogu /home/ftp/etc/security na użytkownika root i grupę security, wpisując:

```
chown root:security security
```

15. Przejdź do katalogu /home/ftp/etc/security, wpisując:

```
cd security
```

16. Dodaj użytkownika, wpisując następującą krótką ścieżkę SMIT:

```
smit mkuser
```

W tym scenariuszu dodawany jest użytkownik o nazwie `test`.

17. W polach SMIT wprowadź następujące wartości:

```
Nazwa UŻYTKOWNIKA                                   [test]
UŻYTKOWNIK ADMINISTRACYJNY?                                 true
GRUPA Podstawowa                                    [staff]
ZBIÓR Grup                                          [staff]
Inny użytkownik może wykonać SU na UŻYTKOWNIKA?                             true
Katalog OSOBISTY                                    [/home/test]
```

Po wprowadzeniu zmian naciśnij ENTER, aby utworzyć użytkownika. Po zakończeniu przetwarzania programu SMIT zamknij ten program.

18. Utwórz hasło dla tego użytkownika za pomocą następującej komendy:

```
passwd test
```

Po wyświetleniu komunikatu, wprowadź żądane hasło. W celu potwierdzenia, należy wprowadzić nowe hasło po raz drugi.

19. Przejdź do katalogu `/home/ftp/etc`, wpisując:

```
cd /home/ftp/etc
```

20. Skopiuj plik `/etc/passwd` do pliku `/home/ftp/etc/passwd` za pomocą następującej komendy:

```
cp /etc/passwd /home/ftp/etc/passwd
```

21. Korzystając z dowolnego edytora, dokonaj edycji pliku `/home/ftp/etc/passwd`. Na przykład:

```
vi passwd
```

22. Usuń wszystkie wiersze ze skopiowanej zawartości z wyjątkiem wierszy dotyczących użytkowników root, ftp i test. Po zakończeniu edycji zawartość pliku powinna być następująca:

```
root:!:0:0::/:/bin/ksh
ftp:*:226:1::/home/ftp:/usr/bin/ksh
test:!:228:1::/home/test:/usr/bin/ksh
```

23. Zapisz zmiany i zakończ edycję.
24. Zmień uprawnienia do pliku `/home/ftp/etc/passwd` na `-rw-r--r--`, wpisując:

```
chmod 644 passwd
```

25. Zmień właściciela i grupę dla pliku `/home/ftp/etc/passwd` na użytkownika root i grupę security, wpisując:

```
chown root:security passwd
```

26. Skopiuj zawartość pliku `/etc/security/passwd` do pliku `/home/ftp/etc/security/passwd`, korzystając z następującej komendy:

```
cp /etc/security/passwd /home/ftp/etc/security/passwd
```

27. Korzystając z dowolnego edytora, dokonaj edycji pliku `/home/ftp/etc/security/passwd`. Na przykład:

```
vi ./security/passwd
```

28. Usuń wszystkie sekcje ze skopiowanej zawartości z wyjątkiem sekcji należącej do użytkownika test.
29. Usuń wiersz `flags = ADMCHG` z sekcji użytkownika test. Po zakończeniu edycji zawartość pliku powinna być następująca:

```
test:
        password = 2HaAYgpDZX3Tw
        lastupdate = 990633278
```

30. Zapisz zmiany i zakończ edycję.

31. Zmień uprawnienia do pliku /home/ftp/etc/security/passwd na -rw-----, wpisując:

```
chmod 600 ./security/passwd
```

32. Zmień właściciela i grupę dla pliku /home/ftp/etc/security/passwd na użytkownika root i grupę security, wpisując:

```
chown root:security ./security/passwd
```

33. Korzystając z dowolnego edytora, utwórz i dokonaj edycji pliku /home/ftp/etc/group. Na przykład:

```
vi group
```

34. Dodaj do pliku następujące wiersze:

```
system:*:0:
staff:*:1:test
```

35. Zapisz zmiany i zakończ edycję.
36. Zmień uprawnienia dostępu do pliku /home/ftp/etc/group na -rw-r--r--, wpisując komendę:

```
chmod 644 group
```

37. Zmień właściciela i grupę dla pliku /home/ftp/etc/group na użytkownika root i grupę security, wpisując komendę:

```
chown root:security group
```

38. Korzystając z dowolnego edytora, utwórz i dokonaj edycji pliku /home/ftp/etc/security/group. Na przykład:

```
vi ./security/group
```

39. Dodaj do pliku następujące wiersze:

```
system:
    admin = true
staff
    admin = false
```

40. Zapisz zmiany i zakończ edycję.

    W tym celu wykonaj następujące kroki:

    a. Skopiuj plik /etc/security/user do katalogu /home/ftp/etc/security, wpisując:

    ```
    cp /etc/security/user /home/ftp/etc/security
    cd /home/ftp/etc/
    ```

    b. Za pomocą edytora usuń wszystkie sekcje ze skopiowanej zawartości z wyjątkiem sekcji dotyczącej użytkownika test, wpisując:

    ```
    vi ./security/user
    ```

    c. Zapisz plik i zakończ edycję.
41. Zmień uprawnienia do pliku /home/ftp/etc/security/group na -rw-r-----, wpisując komendę:

```
chmod 640 ./security/group
```

42. Zmień właściciela i grupę dla pliku /home/ftp/etc/group na użytkownika root i grupę security, wpisując komendę:

```
chown root:security ./security/group
```

43. Użyj następujących komend, aby skopiować odpowiednią zawartość do katalogu /home/ftp/etc/objrepos:

```
cp /etc/objrepos/CuAt ./objrepos
cp /etc/objrepos/CuAt.vc ./objrepos
cp /etc/objrepos/CuDep ./objrepos
cp /etc/objrepos/CuDv ./objrepos
cp /etc/objrepos/CuDvDr ./objrepos
cp /etc/objrepos/CuVPD ./objrepos
cp /etc/objrepos/Pd* ./objrepos
```

44. Przejdź do katalogu /home/ftp/home, wpisując:

```
cd ../home
```

45. Utwórz nowy katalog osobisty dla użytkownika, wpisując:

```
mkdir test
```

    Będzie to katalog osobisty dla nowego użytkownika ftp.

46. Zmień właściciela i grupę dla katalogu /home/ftp/home/test na użytkownika test i grupę personel, wpisując:

```
chown test:staff test
```

47. Zmień uprawnienia do pliku /home/ftp/home/test na -rwx------, wpisując:

```
chmod 700 test
```

48. Wyłącz zdalne logowanie i logowanie na konsoli dla użytkownika test, wpisując następującą komendę:

```
chuser login=false rlogin=false test
```

Na komputerze zostało skonfigurowane podkonto logowania ftp. Można je przetestować, wykonując następującą procedurę:

1. Użyj programu ftp do połączenia się z hostem, na którym zostało utworzone konto użytkownika test. Na przykład:

```
ftp MójHost
```

2. Zaloguj się jako użytkownik anonymous. Po wyświetleniu komunikatu z prośbą o podanie hasła naciśnij Enter.
3. Przełącz się na nowo utworzonego użytkownika test, korzystając z następującej komendy:

```
user test
```

    Po wyświetleniu komunikatu z prośbą o podanie hasła użyj hasła ustawionego w kroku “18” na stronie 58

4. Użyj komendy **pwd** do sprawdzenia, czy katalog osobisty użytkownika istnieje. Na przykład:

```
ftp> pwd
     /home/test
```

    Wyświetlone komunikaty wskazują, że katalog /home/test jest podkatalogiem katalogu ftp. W rzeczywistości pełna nazwa ścieżki na hoście to /home/ftp/home/test.

Uwagi:

- Użytkowników można przełączać tylko z użyciem podużytkowników ftp. Na przykład test jest podużytkownikiem ftp.
- Tworząc użytkowników ftp anonymous za pomocą skryptu anon.users.ftp, można nadać takim użytkownikom dowolną nazwę, zastępując *username* w skrypcie.

- W przypadku użytkowników anonymous wszystkie pliki związane z konfiguracją, takie jak *fileftpaccess.ctl*, powinny znajdować się w tym samym katalogu osobistym, np. ~/etc/, danego użytkownika anonymous, ponieważ serwer wykonuje komendę **chroot** w katalogu osobistym konta użytkownika. Ograniczenia 'tylko do zapisu', 'tylko do odczytu' i 'odczyt/zapis' w pliku /etc/ftpaccess.ctl muszą mieć ścieżkę względną w stosunku do ścieżki chrooted.

Więcej informacji:

- "Bezpieczeństwo TCP/IP" w podręczniku *Bezpieczeństwo*
- "**Komenda ftp**" w podręczniku *Commands Reference*

Systemowe specjalne konta użytkowników
System AIX posiada podstawowy zestaw systemowych specjalnych kont użytkownika, które sprawiają, że użytkownicy root i system nie mogą być właścicielami wszystkich plików i systemów plików systemu operacyjnego.

Ostrzeżenie: Należy zachować ostrożność podczas usuwania systemowych specjalnych kont użytkowników. Określone konto można wyłączyć, wstawiając gwiazdkę (*) na początku odpowiadającego mu wiersza w pliku /etc/security/passwd. Należy jednak uważać, aby nie wyłączyć konta użytkownika root. Jeśli zostaną usunięte systemowe specjalne konta użytkowników lub zostanie wyłączone konto użytkownika root, system operacyjny przestanie działać.

W systemie znajdują się następujące predefiniowane konta:

adm
Konto użytkownika adm jest właścicielem następujących podstawowych funkcji systemowych:

- Diagnostyki, której narzędzia znajdują się w katalogu /usr/sbin/perf/diag_tool .
- Rozliczania, którego narzędzia są przechowywane w następujących katalogach:
  - /usr/sbin/acct,
  - /usr/lib/acct,
  - /var/adm,
  - /var/adm/acct/fiscal,
  - /var/adm/acct/nite,
  - /var/adm/acct/sum.

bin
Konto użytkownika bin jest zwykle właścicielem plików wykonywalnych dla większości komend użytkownika. Głównym celem istnienia tego konta jest pomoc w dystrybucji praw własności ważnych systemowych katalogów i plików, aby wszystkie pliki nie musiały być własnością użytkownika root i sys.

daemon
Konto użytkownika daemon służy jedynie do przejmowania na własność i wykonywania procesów serwera systemowego i powiązanych z nimi plików. To konto gwarantuje, że procesy te zostaną uruchomione z odpowiednimi prawami dostępu do plików.

nobody
Konto użytkownika nobody jest używane przez Network File System (NFS) w celu umożliwienia zdalnego drukowania. To konto istnieje po to, aby program mógł zezwolić na tymczasowy dostęp z uprawnieniami użytkownika root do użytkowników root. Na przykład przed włączeniem Secure RPC lub Secure NFS należy sprawdzić w kluczu /etc/public na głównym serwerze NFS, czy użytkownik nie został przypisany do klucza publicznego i tajnego. Będąc użytkownikiem root, można tworzyć pozycje w bazie danych dla każdego nieprzypisanego użytkownika za pomocą następującej komendy:

```
newkey -u nazwa_użytkownika
```

Można również tworzyć pozycje w bazie dla użytkownika nobody, a następnie dowolny użytkownik może uruchomić program **chkey** celu utworzenia własnych pozycji w bazie danych bez potrzeby logowania się jako użytkownik root.

root
Konto użytkownika root, UID 0, za pomocą którego można wykonywać zadania związane z konserwacją systemu i rozwiązywaniem problemów.

sys
Użytkownik sys jest właścicielem domyślnego punktu podłączania pamięci podręcznej DFS (Distributed File Service), który musi istnieć, zanim obsługa DFS zostanie d zainstalowana lub skonfigurowana na kliencie. Katalog `/usr/sys` może również zawierać obrazy instalacyjne.

system
Grupa systemowa jest grupą zdefiniowaną systemowo dla administratorów systemu. Użytkownicy grupy systemowej mają uprawnienia do wykonywania niektórych zadań obsługi systemu, bez konieczności posiadania uprawnień użytkownika root.

Usuwanie niepotrzebnych kont użytkowników domyślnych
Podczas instalowania systemu operacyjnego tworzona jest określona liczba identyfikatorów użytkowników domyślnych i grup. W zależności od uruchomionych w systemie aplikacji i od tego, gdzie w sieci znajduje się system, niektóre z tych identyfikatorów użytkowników i grup mogą osłabić bezpieczeństwo systemu i narazić go na atak lub wykorzystanie.

Poniższa tabela zawiera listę najczęściej występujących domyślnych identyfikatorów użytkowników, które użytkownik może usunąć:

Tabela 3. Lista najczęściej występujących domyślnych identyfikatorów użytkowników, które użytkownik może usunąć.

Identyfikator użytkownika	**Opis**
uucp, nuucp	Właściciel ukrytych plików używanych przez protokół uucp. Konto użytkownika uucp jest używane przez grupę komend, programów i plików o wspólnej nazwie UNIX-to-UNIX Copy Program, obecnych w większości systemów AIX i umożliwiających użytkownikowi komunikowanie się z innym systemem AIX za pośrednictwem linii dedykowanej lub telefonicznej.
lpd	Właściciel ukrytych plików używanych przez podsystem drukowania.
guest	Umożliwia dostęp użytkownikom niemającym dostępu do kont.

Poniższa tabela zawiera listę najczęściej występujących identyfikatorów grup, które mogą nie być potrzebne:

Tabela 4. Najczęściej występujące identyfikatory grup, które mogą nie być potrzebne.

Identyfikator grupy	**Opis**
uucp	Grupa, do której należą użytkownicy uucp i nuucp
printq	Grupa, do której należy użytkownik lpd

Należy zanalizować system w celu określenia, które identyfikatory rzeczywiście nie są potrzebne. Mogą występować również dodatkowe identyfikatory użytkowników lub grup, które mogą nie być potrzebne. Przed uruchomieniem systemu należy szczegółowo ocenić, które identyfikatory są wymagane.

Uwaga: Zamiast usuwać grupę `printq` z powodu zależności od zestawów plików drukarek, należy wyłączyć identyfikator użytkownika `lp`, komendę **piobe** i program qdaemon we wpisach w pliku `/etc/inittab`, aby zminimalizować zagrożenie bezpieczeństwa. Uniemożliwia to temu użytkownikowi uruchamianie komend **print**.

Konta tworzone przez komponenty zabezpieczeń
W trakcie instalowania i konfigurowania komponentów zabezpieczeń, takich jak LDAP i OpenSSH, tworzone są konta użytkowników i grup.

Komponenty zabezpieczeń, takie jak LDAP i OpenSSH, tworzą następujące konta użytkowników i grup:

- IPSec (Internet Protocol Security)
  - Komponent IPSec dodaje podczas instalacji konto użytkownika *ipsec* oraz konto grupy *ipsec*. Identyfikatory te używane są przez usługę zarządzania kluczami.

  Uwaga: Identyfikator grupy w pliku /usr/lpp/group.id.keymgt nie może zostać dostosowany przed instalacją.
- Protokół Kerberos i infrastruktura klucza publicznego (PKI)
  - Komponenty te nie tworzą żadnych nowych kont użytkowników ani grup.
- LDAP
  - Gdy jest zainstalowany klient lub serwer LDAP, tworzone jest konto użytkownika *idsldap*. ID użytkownika *idsldap* jest stały i nie może zostać zmieniony na innego użytkownika. Ten identyfikator użytkownika jest właścicielem plików udostępnianych przez zestawy plików i pakiety *idsldap*. Baza danych Db2 musi zostać zainstalowana przed zainstalowaniem serwera LDAP. Podczas konfigurowania serwera LDAP komenda **mksecldap** tworzy konto użytkownika *ldapdb2* i używa tego konta jako właściciela instancji LDAP i Db2.
- OpenSSH
  - Podczas instalowania oprogramowania OpenSSH do systemu zostanie dodane konto użytkownika *sshd* i grupa *sshd*. Nie należy zmieniać odpowiednich identyfikatorów użytkowników ani grup. Opcja oddzielenia uprawnień w protokole SSH wymaga identyfikatorów.

Grupy bezdomenowe
Funkcja grup bezdomenowych umożliwia przypisywanie użytkowników zdefiniowanych w jednej domenie do grup zdefiniowanych w innej domenie. Ta funkcja obsługuje tylko LDAP (Lightweight Database Access Protocol) i domeny lokalne.

Na serwerze LDAP można utworzyć użytkowników i grupy, używając modułu ładowalnego uwierzytelniania LDAP (moduł LDAP). Użytkowników i grupy można także utworzyć w systemie lokalnym, używając lokalnego modułu ładowalnego uwierzytelniania (moduł lokalny). Gdy funkcja **domainlessgroups** nie jest włączona, użytkowników i grup utworzonych w module LDAP lub w systemie lokalnym nie można przypisywać do grup poza domeną lokalną, w której zostali utworzeni. Na przykład użytkownika utworzonego w domenie LDAP nie można przypisać do grupy powiązanej z domeną lokalną.

To ograniczenie można pokonać i przypisywać użytkowników do LDAP i grup lokalnych, włączając właściwość systemową **domainlessgroups**. Właściwość **domainlessgroups** jest zdefiniowana w pliku /etc/secvars.cfg. Jest ona obsługiwana tylko dla modułów LDAP i modułów lokalnych. Dostępne są następujące wartości tej właściwości:

false (wartość domyślna)
Atrybut grupy nie jest scalany z modułów LDAP i modułów lokalnych.

true
Atrybut grupy jest scalany z modułów LDAP i modułów lokalnych. Na przykład użytkowników LDAP można przypisywać do grup lokalnych.

Aby wyświetlić wartość właściwości **domainlessgroups**, uruchom następującą komendę:

```
lssec -f /etc/secvars.cfg -s groups -a domainlessgroups
```

Aby dla właściwości **domainlessgroups** ustawić wartość true, uruchom następującą komendę:

```
chsec -f /etc/secvars.cfg -s groups -a domainlessgroups=true
```

W poniższej tabeli przedstawiono wyniki działania komend dotyczących użytkowników i grup w zależności od ustawienia właściwości **domainlessgroups**.

*Tabela 5. Wyniki działania wybranych komend, na które wpływa właściwość **domainlessgroups***	
Komenda	**Wyniki, gdy dla właściwości domainlessgroups ustawiono wartość true**
`chgroup -R` **ldap**|**files**	Aktualizuje grupę w podanej domenie. Można dodać użytkownika do LDAP lub grupy lokalnej.
`chuser -R` **ldap**|**files**	Zmienia ustawienia dla użytkownika w podanej domenie. Jeśli zostaną podane grupy zdefiniowane w innej domenie, grupy te także zostaną zaktualizowane z użyciem informacji o użytkowniku.
`login` *nazwa_użytkownika* lub su	Pobiera atrybuty użytkownika z rejestru użytkowników oprócz atrybutu identyfikatora grupy. Atrybuty użytkownika dla identyfikatora grupy są scalane zarówno z LDAP, jak i domen lokalnych.
`lsgroup -R` **ldap**|**files**	Wyświetla wszystkie atrybuty grupy dla podanej domeny. Jeśli nie znajdzie podanej grupy w podanej domenie, wykonanie komendy nie powiedzie się.
`lsuser -R` **ldap**|**files**	Wyświetla atrybuty użytkownika po scaleniu informacji z wszystkich grup w domenie, w której zdefiniowano użytkownika i w drugiej domenie. Jeśli podstawowa grupa użytkownika nie jest zdefiniowana w domenie, w której zdefiniowano użytkownika, jest ona ustalana z drugiej domeny.
`mkgroup -R` **ldap**|**files**	Tworzy grupę w podanej domenie. Po utworzeniu grupy przypisuje się użytkownika (LDAP lub lokalnego) do tej grupy w bazie danych grup dla tej domeny. Można dodać użytkownika do grup LDAP albo grup lokalnych.
`mkuser -R` **ldap**|**files**	Tworzy użytkownika w podanej domenie. Jeśli zostaną podane grupy zdefiniowane w innej domenie, grupy te także zostaną zaktualizowane z użyciem informacji o użytkowniku.
`rmgroup -R` **ldap**|**files**	Usuwa podaną grupę z podanej domeny. Jeśli grupa jest przypisana jako grupa podstawowa dla dowolnego użytkownika zdefiniowanego w dowolnej domenie, wykonanie tej komendy nie powiedzie się.
`rmuser -R` **ldap**|**files**	Usuwa podanego użytkownika z podanej domeny. Ponadto usuwa tego użytkownika z grup zdefiniowanych w drugiej domenie, w których ten użytkownik jest członkiem.

Pojęcia pokrewne

Moduł ładowalny uwierzytelniania LDAP

Wykorzystanie podsystemu zabezpieczeń przez protokół LDAP zostało zaimplementowane jako moduł ładowalny uwierzytelniania LDAP. Jest on koncepcyjnie podobny do innych modułów ładowalnych, takich jak NIS, DCE i KRB5. Moduły ładowalne są zdefiniowane w pliku `/usr/lib/security/methods.cfg`.

Informacje pokrewne

Komenda chgroup

Komenda chuser
Komenda login
Komenda lsgroup
Komenda lsuser
Komenda mkgroup
Komenda mkuser
Komenda rmgroup
Komenda rmuser
Komenda su

Hasła
Odgadywanie haseł jest jedną z najczęstszych metod ataku na system. Z tego względu istotne jest kontrolowanie i monitorowanie strategii ograniczania haseł.

System AIX zawiera mechanizmy, które pomagają stosować lepsze strategie haseł, takie jak ustawianie następujących wartości:

- minimalna i maksymalna liczba tygodni, które mogą upłynąć, zanim hasło będzie mogło zostać zmienione i po jego zmianie,
- minimalna długość hasła,
- minimalna liczba liter, które mogą być użyte podczas tworzenia hasła.

Definiowanie dobrych haseł
Dobre hasła stanowią pierwszą linię obrony przed nieautoryzowanym dostępem do systemu.

Hasła są skuteczne, jeśli:

- Zawierają zarówno wielkie, jak i małe litery.
- Zawierają litery, cyfry i znaki przestankowe. Ponadto mogą zawierać następujące znaki specjalne: ~ ! @ # $ % ^ & * ( ) - _ = + [ ] { } | \ ; : ' " , . < > ? / <spacja>
- Nie są nigdzie zapisane.
- Ich długość wynosi od siedmiu do maksymalnie PW_PASSLEN znaków, jeśli używany jest plik `/etc/security/passwd` (implementacje uwierzytelniania stosujące rejestry, takie jak LDAP, mogą używać haseł przekraczających tę długość maksymalną).
- Nie są słowami, które można znaleźć w dostępnych słownikach.
- Nie tworzą wzorów z liter na klawiaturze, jak na przykład *qwerty*.
- Nie są słowami lub wzorami pisanymi od tyłu.
- Nie zawierają żadnych danych osobowych użytkownika, rodziny lub przyjaciół.
- Nie są w nich stosowane te same wzory co w poprzednim haśle.
- Można je wpisać szybko, tak aby osoba znajdująca się obok nie mogła go rozpoznać.

Oprócz tych mechanizmów można dalej zaostrzyć reguły, umożliwiając umieszczanie w hasłach standardowych słów związanych z systemem UNIX, które można odgadnąć. Ta funkcja używa atrybutu dictionlist, który wymaga zainstalowania zestawów plików `bos.data` i `bos.txt`.

Aby zaimplementować wcześniej zdefiniowaną listę dictionlist, należy poddać edycji następujący wiersz w pliku `/etc/security/users`:

```
dictionlist = /usr/share/dict/words
```

Atrybut dictionlist w pliku `/usr/share/dict/words` zapobiega używaniu standardowych słów związanych z systemem UNIX jako haseł.

Używanie pliku /etc/passwd
Tradycyjnie plik `/etc/passwd` jest używany do śledzenia każdego zarejestrowanego użytkownika, który uzyskał dostęp do systemu.

Plik /etc/passwd jest plikiem z wartościami rozdzielonymi dwukropkami i zawiera następujące informacje:

- nazwa użytkownika,
- zaszyfrowane hasło,
- identyfikator użytkownika (UID),
- identyfikator grupy użytkownika (GID),
- pełna nazwa użytkownika (GECOS),
- katalog osobisty użytkownika,
- powłoka logowania.

Oto przykładowy plik /etc/passwd:

```
root:!:0:0::/:/usr/bin/ksh
daemon:!:1:1::/etc:
bin:!:2:2::/bin:
sys:!:3:3::/usr/sys:
adm:!:4:4::/var/adm:
uucp:!:5:5::/usr/lib/uucp:
guest:!:100:100::/home/guest:
nobody:!:4294967294:4294967294::/:
lpd:!:9:4294967294::/:
lp:*:11:11::/var/spool/lp:/bin/false
invscout:*:200:1::/var/adm/invscout:/usr/bin/ksh
nuucp:*:6:5:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
paul:!:201:1::/home/paul:/usr/bin/ksh
jdoe:*:202:1:John Doe:/home/jdoe:/usr/bin/ksh
```

System AIX nie przechowuje haseł zaszyfrowanych w pliku /etc/passwd, tak jak systemy UNIX, ale domyślnie w pliku /etc/security/passwd [1], którego zawartość może odczytać tylko użytkownik root. Pole hasła w pliku /etc/passwd jest używane przez system AIX do określenia, czy ustalone jest jakieś hasło lub czy konto jest zablokowane.

Uwaga: >|Gdy powłoka logowania ma wartość null, logowanie powiodło się, a otrzymaną powłoką logowania będzie powłoką Bourne'a dla ssh. W przypadku dostępu za pomocą su powłoką logowania jest powłoka sh, która jest dowiązaniem stałym do powłoki ksh.|<

Właścicielem pliku /etc/passwd jest użytkownik root i plik ten musi być dostępny do odczytu dla wszystkich użytkowników, ale jedynie użytkownik root może mieć prawa zapisu do niego, co jest oznaczane przez uprawnienia -rw-r--r--. Jeśli identyfikator użytkownika ma przypisane hasło, pole hasła ma wartość ! (wykrzyknik). Jeśli identyfikator użytkownika nie ma przypisanego hasła, pole hasła ma wartość * (gwiazdka). Zaszyfrowane hasła są przechowywane w pliku /etc/security/passwd . Poniższy przykład zawiera cztery ostatnie pozycje pliku /etc/security/passwd utworzone w oparciu o pokazany wcześniej plik /etc/passwd .

```
guest:
        password = *

nobody:
        password = *

lpd:
        password = *

paul:
        password = eacVScDKri4s6
        lastupdate = 1026394230
        flags = ADMCHG
```

Identyfikator użytkownika jdoe nie ma wpisu w pliku /etc/security/passwd ponieważ nie ma ustawionego hasła w pliku /etc/passwd.

[1] /etc/security/passwd

Spójność pliku /etc/passwd można sprawdzić za pomocą komendy **pwdck**. Komenda **pwdck** sprawdza poprawność informacji o haśle w plikach bazy danych użytkowników, sprawdzając definicje wszystkich lub tylko wybranych użytkowników.

Używanie pliku /etc/passwd a środowiska sieciowe
Tradycyjnie w środowisku sieciowym użytkownik musi mieć konto w każdym systemie, do którego chce uzyskać dostęp.

Oznacza to zazwyczaj, że użytkownik ma wpis w każdym pliku /etc/passwd na każdym systemie. W środowisku rozproszonym nie ma jednak prostego sposobu na zapewnienie, że każdy system ma taki sam plik /etc/passwd. Aby rozwiązać ten problem, opracowano kilka metod udostępniania informacji zawartych w pliku /etc/passwd, w tym System informacji o sieci (NIS) i NIS+:

Ukrywanie haseł i nazw użytkowników
Aby uzyskać wyższy poziom bezpieczeństwa, należy upewnić się, że identyfikatory i hasła użytkowników nie są w systemie widoczne.

Pliki .netrc zawierają identyfikatory i hasła użytkowników. Ten plik nie jest szyfrowany ani kodowany, dlatego jego zawartość można wyświetlić jako zwykły tekst. Aby odnaleźć te pliki, należy uruchomić następującą komendę:

```
# find `awk -F: '{print $6}' /etc/passwd` -name .netrc -ls
```

Po zlokalizowaniu plików, usuń je. Bardziej efektywnym sposobem przechowywania haseł jest skonfigurowanie protokołu Kerberos. Więcej informacji na temat Kerberos zawiera sekcja “Kerberos” na stronie 296.

Ustawianie zalecanych opcji haseł
Prawidłowe zarządzanie hasłami nie jest możliwe bez edukacji użytkowników. Aby jednak zapewnić dodatkowe zabezpieczenie, system operacyjny oferuje konfigurowalne ograniczenia haseł. Umożliwia to administratorom ograniczanie wybierania niewłaściwych haseł przez użytkowników i wymusza regularną ich zmianę.

Opcje haseł i rozszerzone atrybuty użytkowników są umieszczone w pliku /etc/security/user, pliku w formacie ASCII, który zawiera sekcje atrybutów dla użytkowników. Te ograniczenia są stosowane podczas definiowania nowego hasła dla użytkownika. Wszystkie ograniczenia haseł są definiowane dla każdego użytkownika z osobna. W przypadku zachowania ograniczeń w domyślnej sekcji w pliku /etc/security/user, te same ograniczenia są stosowane dla wszystkich użytkowników. Aby utrzymać bezpieczeństwo haseł, wszystkie hasła muszą być chronione w podobny sposób.

Administratorzy mogą również rozszerzać ograniczenia dotyczące haseł. Za pomocą atrybutu **pwdchecks** z pliku /etc/security/user administrator może dodać nowe podprogramy (zwane również *metodami*) do programu ograniczenia wyboru haseł. Dzięki temu istnieje możliwość dodawania i stosowania przez system operacyjny lokalnych strategii. Więcej informacji na ten temat zawiera sekcja “Rozszerzanie ograniczeń haseł” na stronie 72.

Ograniczenia haseł należy stosować z wyczuciem. Próby stosowania zbyt dużych ograniczeń, takich jak ograniczanie długości hasła, co ułatwia jego odgadnięcie, lub zmuszanie użytkownika do wybierania haseł, które są trudne do zapamiętania, co może skłonić użytkownika do ich zapisania, mogą narazić bezpieczeństwo haseł. Bezpieczeństwo hasła jest w rękach użytkownika. Proste ograniczenia haseł, powiązane z rozsądnymi wskazówkami i okazjonalnymi kontrolami mającymi na celu zbadanie unikalności haseł, to najlepsze rozwiązanie.

Poniższa tabela przedstawia listę zalecanych wartości niektórych atrybutów bezpieczeństwa związanych z hasłami użytkowników z pliku /etc/security/user.

Tabela 6. Zalecane wartości atrybutów bezpieczeństwa dla haseł użytkownika.

Atrybut	Opis	Zalecana wartość	Wartość domyślna	Wartość maksymalna
dictionlist	Sprawdza, czy hasła nie zawierają słów związanych z systemem UNIX.	**/usr/share/dict/words**	nie dotyczy	nie dotyczy
histexpire	Liczba tygodni, które muszą upłynąć, zanim będzie można ponownie użyć hasła.	26	0	260*
histsize	Liczba dozwolonych powtórzeń hasła.	20	0	50
maxage	Maksymalna liczba tygodni, po upływie których hasło musi zostać zmienione.	8	0	52
maxexpired	Maksymalna liczba tygodni po okresie *maxage* , po upływie których hasło, które utraciło ważność, może zostać zmienione przez użytkownika. (Użytkownik root jest wyjątkiem).	2	-1	52
maxrepeats	Maksymalna liczba znaków, które mogą się w haśle powtórzyć.	2	8	8

Tabela 6. Zalecane wartości atrybutów bezpieczeństwa dla haseł użytkownika. (kontynuacja)

Atrybut	Opis	Zalecana wartość	Wartość domyślna	Wartość maksymalna
minage	Minimalna liczba tygodni, przed upływem których hasło nie może zostać zmienione. Nie należy ustawiać wartości niezerowej, chyba że administratorzy zawsze z łatwością mogą zresetować hasło, które zostało przypadkowo ujawnione, a które zostało ostatnio zmienione.	0	0	52
minalpha	Minimalna liczba liter wymagana w hasłach.	2	0	PW_PASSLEN**
mindiff	Minimalna liczba unikalnych znaków, które muszą znajdować się w haśle.	4	0	PW_PASSLEN**
minlen	Minimalna długość hasła	6 (8 dla użytkownika root)	0	PW_PASSLEN**
minother	Minimalna liczba znaków nie będących literami wymagana w hasłach	2	0	PW_PASSLEN**
pwdwarntime	Liczba dni, po upływie których system wysyła ostrzeżenie o tym, że hasło powinno zostać zmienione.	5	nie dotyczy	nie dotyczy

Tabela 6. Zalecane wartości atrybutów bezpieczeństwa dla haseł użytkownika. (kontynuacja)				
Atrybut	**Opis**	**Zalecana wartość**	**Wartość domyślna**	**Wartość maksymalna**
pwdchecks	Ta pozycja może być użyta do wzbogacenia komendy **passwd** o niestandardowy kod, który sprawdza jakość hasła.	Więcej informacji na ten temat zawiera sekcja "Rozszerzanie ograniczeń haseł" na stronie 72.	nie dotyczy	nie dotyczy

* Zachowywanych jest maksymalnie 50 haseł.

** PW_PASSLEN jest zdefiniowany w pliku `userpw.h`.

Jeśli w systemie jest zainstalowane oprogramowanie do przetwarzania tekstu, administrator może użyć pliku `/usr/share/dict/words` jako pliku słownika **dictionlist**. W takim przypadku może on ustawić atrybut **minother** na `0`. Ponieważ większość słów w pliku słownika nie zawiera znaków należących do kategorii atrybutu **minother**, ustawienie atrybutu **minother** na wartość 1 lub większą powoduje wyeliminowanie większości słów z tego pliku słownika.

Minimalna długość hasła w systemie określona jest przez wartość atrybutu **minlen** lub wartość atrybutu **minalpha** plus wartość atrybutu **minother**, w zależności od tego, która wartość jest większa.

Maksymalna długość hasła odpowiada wartości atrybutu **PW_PASSLEN**. Liczba znaków używanych podczas generowania przechowywanej wartości hasła zależy od algorytmu haseł używanego w systemie. Algorytmy haseł są definiowane w pliku `/etc/security/pwdalg.cfg`, a domyślnie używany algorytm hasła można skonfigurować w atrybucie **pwd_algorithm** w pliku `/etc/security/login.cfg`. Suma wartości atrybutów **minalpha** i **minother** nie może przekraczać wartości atrybutu **PW_PASSLEN**. Jeśli suma wartości atrybutów **minalpha** i **minother** jest większa od wartości atrybutu **PW_PASSLEN**, wartość atrybutu **minother** zostanie zmniejszona do wartości atrybutu **PW_PASSLEN** pomniejszonej o wartość atrybutu **minalpha**.

Jeśli wartości obu atrybutów **histexpire** i **histsize** są ustawione, system zachowa liczbę haseł wymaganą do spełnienia obu warunków, do wartości 50 haseł na użytkownika. Puste hasła nie zostaną zachowane.

Plik `/etc/security/user` można poddać edycji, aby dodać wszelkie wartości domyślne wymagane do zarządzania hasłami użytkownika. Alternatywnie, można zmienić wartości atrybutów za pomocą komendy **chuser**.

Inne komendy, które mogą być użyte z tym plikiem to **mkuser**, **lsuser** i **rmuser**. Komenda **mkuser** tworzy wpis dla każdego nowego użytkownika w pliku `/etc/security/user` i inicjuje jego atrybuty za pomocą atrybutów zdefiniowanych w pliku `/usr/lib/security/mkuser.default` . Aby wyświetlić atrybuty i ich wartości, należy użyć komendy **lsuser**. Aby usunąć użytkownika, należy użyć komendy **rmuser**.

Obsługa haseł dłuższych niż 8 znaków oraz algorytm LPA

Postęp, który dokonał się w dziedzinie sprzętu komputerowego, spowodował, że tradycyjne szyfrowanie haseł w systemie UNIX jest wrażliwe na ataki z odgadywaniem hasła metodą brute-force. Kryptograficznie słaby algorytm prowadzi do odtworzenia nawet bardzo mocnych haseł. W systemie AIX obsługiwany jest algorytm LPA udostępniający bezpieczne mechanizmy mieszające hasła.

Tradycyjna funkcja szyfrowania haseł crypt

Standardowy mechanizm uwierzytelniania systemu AIX używa do uwierzytelniania użytkowników jednokierunkowej funkcji mieszającej o nazwie **crypt**. Funkcja **crypt** to zmodyfikowany algorytm DES. Wykonuje ona jednokierunkowe szyfrowanie tablicy danych o stałej długości z dostarczonym hasłem i kluczem dodatkowym.

Funkcja **crypt** używa tylko pierwszych ośmiu znaków łańcucha hasła, więc hasło użytkownika jest obcinane do ośmiu znaków. Jeśli hasło zawiera mniej niż osiem znaków, jest uzupełniane z prawej strony bitami zerowymi. 56-bitowy klucz DES jest otrzymywany z 7 bitów z każdego znaku.

Klucz dodatkowy jest dwuznakowym łańcuchem (12 bitów klucza dodatkowego służy do zróżnicowania algorytmu DES) wybranym z zestawu znaków "**A**-**Z**", "**a**-**z**","**0**-**9**","**.**"(kropka) i "**/**". Klucz dodatkowy służy do zróżnicowania algorytmu mieszającego, aby z takiego samego hasła w tekście jawnym można było utworzyć 4096 możliwych zaszyfrowanych tekstów hasła. Osiąga to modyfikacja algorytmu DES zamieniająca bity i oraz i+24 w danych wyjściowych E-Box DES, kiedy bit i jest ustawiany w kluczu dodatkowym. Jednocześnie doprowadza do sytuacji, w której urządzenia do sprzętowego deszyfrowania DES stają się bezużyteczne do odgadywania haseł.

64-bitowy blok wszystkich bitów zerowych jest szyfrowany 25 razy kluczem DES. W wyniku tych działań otrzymywana jest konkatenacja 12-bitowego klucza dodatkowego z zaszyfrowaną 64-bitową wartością. Otrzymana wartość 76-bitowa zostaje zakodowana w 13 drukowalnych znaków ASCII w formacie base64.

Algorytmy kodowania mieszającego haseł
Algorytmy kodowania mieszającego, takie jak MD5, są trudniejsze do złamania od funkcji **crypt**. Stanowią silny mechanizm zabezpieczający przed atakami przez odgadywanie hasła metodą brute-force. Z uwagi na to, że do generowania wartości mieszającej jest używane całe hasło, jeśli do szyfrowania hasła są używane algorytmy kodowania mieszającego, nie trzeba ograniczać jego długości.

Algorytm LPA (Loadable Password Algorithm)
W systemie AIX 6.1 i w nowszych jego wersjach zaimplementowano mechanizm LPA służący do prostego wdrażania nowych algorytmów szyfrowania haseł.

Każdy obsługiwany algorytm szyfrowania haseł jest implementowany jako moduł ładowania LPA, ładowany w czasie wykonywania, gdy dany algorytm jest potrzebny. Obsługiwane algorytmy LPA wraz z atrybutami są zdefiniowane w pliku konfiguracyjnym systemu `/etc/security/pwdalg.cfg`.

Administrator może skonfigurować obowiązujący w całym systemie mechanizm szyfrowania haseł, używający konkretnego algorytmu LPA do szyfrowania haseł. Po zmianie tego mechanizmu system będzie nadal obsługiwał hasła szyfrowane wcześniej wybranym mechanizmem szyfrowania haseł (na przykład za pomocą funkcji **crypt**).

Obsługa haseł dłuższych niż osiem znaków
Wszystkie algorytmy LPA zaimplementowane w systemie AIX 6.1 i w nowszych jego wersjach obsługują hasła dłuższe niż osiem znaków. Ograniczenie długości hasła zależy od wybranego algorytmu LPA. Maksymalna obsługiwana długość hasła to 255 znaków.

Plik konfiguracyjny LPA
Plikiem konfiguracyjnym LPA jest plik `/etc/security/pwdalg.cfg`. Jest to plik podzielony na sekcje, w których zdefiniowane są atrybuty obsługiwanych algorytmów LPA.

W pliku konfiguracyjnym są zdefiniowane następujące atrybuty algorytmu LPA:

- Ścieżka do modułu LPA.
- Opcje przekazywane do modułu LPA w czasie wykonywania.

Dostęp do atrybutów LPA zdefiniowanych w pliku konfiguracyjnym jest możliwy z interfejsów **getconfattr** i **setconfattr**.

Poniższe przykładowe sekcje pliku `/etc/security/pwdalg.cfg` definiują algorytm LPA o nazwie **ssha256**:

```
ssha256:
                lpa_module = /usr/lib/security/ssha
                lpa_options = algorithm=sha256
```

Algorytm haseł w systemie
Administrator systemu może ustawić algorytm haseł obowiązujący w całym systemie, wybierając algorytm LPA jako algorytm kodowania mieszającego haseł. Jednocześnie w systemie może być tylko

jeden aktywny algorytm haseł. Algorytm haseł w systemie jest zdefiniowany atrybutem systemowym **pwd_algorithm** w sekcji **usw** pliku `/etc/security/login.cfg`.

Poprawnymi wartościami atrybutu **pwd_algorithm** w pliku `/etc/security/login.cfg` są nazwy sekcji LPA zdefiniowane w pliku `/etc/security/pwdalg.cfg`. Inną poprawną wartością atrybutu **pwd_algorithm** jest **crypt**. Wartość ta odnosi się do tradycyjnego szyfrowania programem **crypt**. Jeśli w pliku konfiguracyjnym atrybut **pwd_algorithm** zostanie pominięty, będzie używana wartość domyślna **crypt**.

W poniższym przykładzie pliku `/etc/security/login.cfg` jako algorytmu szyfrowania haseł w całym systemie użyto algorytmu LPA **ssha256**.

```
    ... ...
usw:
            shells = /bin/sh,/bin/bsh,/bin/csh,/bin/ksh,/bin/tsh,/bin/ksh93
            maxlogins = 32767
            logintimeout = 60
            maxroles = 8
            auth_type = STD_AUTH
            pwd_algorithm = ssha256
    ... ...
```

Algorytm haseł w systemie dotyczy tylko nowo tworzonych i zmienionych haseł. Po migracji przy tworzeniu wszystkich nowych haseł lub zmianie dotychczasowych używany jest algorytm haseł w systemie. Hasła istniejące przed wprowadzeniem tej zmiany, niezależnie od tego, czy zostały wygenerowane przy użyciu standardowej funkcji **crypt**, czy innymi obsługiwanymi modułami LPA, nadal będą działać w systemie. Dlatego w systemie mogą współistnieć różne hasła wygenerowane przez różne algorytmy LPA.

Konfigurowanie algorytmu haseł w systemie
Administrator systemu może komendą **chsec** skonfigurować algorytm haseł w systemie. Może również za pomocą edytora, na przykład **vi**, samodzielnie zmienić atrybut **pwd_algorithm** w pliku `/etc/security/login.cfg`.

Zaleca się, aby do ustawiania algorytmu haseł w systemie używać komendy **chsec**, ponieważ sprawdza ona automatycznie definicję podanego algorytmu LPA.

Korzystanie z komendy chsec

Uruchom następującą komendę, aby ustawić algorytm LPA **smd5** jako moduł szyfrowania haseł w całym systemie:

```
chsec -f /etc/security/login.cfg -s usw -a pwd_algorithm=smd5
```

Jeśli do zmiany atrybutu **pwd_algorithm** używana jest komenda **chsec**, sprawdza ona w pliku `/etc/security/pwdalg.cfg` podany algorytm LPA. Jeśli to sprawdzenie się nie powiedzie, wykonanie komendy **chsec** zakończy się niepowodzeniem.

Za pomocą edytora

Jeśli używasz edytora do samodzielnej zmiany wartości atrybutu **pwd_algorithm** w pliku `/etc/security/login.cfg`, upewnij się, że podana wartość jest nazwą sekcji zdefiniowanej w pliku `/etc/security/pwdalg.cfg`.

Rozszerzanie ograniczeń haseł
Reguły używane przez program obsługi haseł do akceptowania lub odrzucania haseł (ograniczenia budowy haseł) mogą zostać rozszerzone przez administratora systemu w celu dodawania ograniczeń charakterystycznych dla danego serwera.

Ograniczenia są rozszerzane przez dodawanie metod, które są wywoływane przy zmianie hasła. Atrybut **pwdchecks** w pliku `/etc/security/user` określa wywoływane metody.

Książka *AIX Version 6.1 Technical Reference* (i nowsze jej wydania) zawiera opis metody **pwdrestrict_method**, interfejsu podprogramu, z którym muszą być zgodne określone metody

ograniczenia haseł. Podczas pisania metody ograniczania haseł administrator systemu musi zaprogramować ten interfejs, aby poprawnie rozszerzyć ograniczenia budowy haseł. Podczas rozszerzania ograniczeń budowy haseł należy zachować ostrożność. Rozszerzenia te mają bezpośredni wpływ na komendy **login**, **passwd**, **su** i inne programy. Bezpieczeństwo systemu może zostać naruszone przez złośliwy lub uszkodzony kod.

Uwierzytelnianie użytkowników
Identyfikacja i uwierzytelnianie służą do określenia tożsamości użytkownika.

Każdy użytkownik musi zalogować się w systemie. Podaje on nazwę użytkownika i hasło, jeśli zostało ono przypisane (w chronionym systemie wszystkie konta muszą mieć hasła lub muszą zostać unieważnione). Jeśli hasło jest prawidłowe, użytkownik jest logowany do tego konta; uzyskuje on również prawa dostępu i uprawnienia tego konta. Pliki /etc/passwd i /etc/security/passwd zawierają hasła użytkowników.

Domyślnie użytkownicy są zdefiniowani w rejestrze plików. Oznacza to, że konto użytkownika oraz informacje o grupie przechowywane są w plikach tekstowych (ASCII). W miarę wprowadzania dodatkowych modułów ładowalnych użytkownicy mogą być definiowani także w innych rejestrach. Na przykład, gdy do administrowania użytkowników używany jest moduł wtyczki LDAP, definicje użytkowników przechowywane są w repozytorium LDAP. W takim przypadku w pliku /etc/security/user nie będą zapisywane pozycje dotyczące użytkowników (wyjątek stanowią atrybuty użytkowników **SYSTEM** i **registry**). Gdy do administrowania użytkownikami wykorzystywany jest mieszany moduł ładowalny (np. moduły ładowalne z częścią uwierzytelniającą i bazą danych), część dotycząca bazy danych określa, w jaki sposób odbywa się administrowanie informacjami konta użytkownika AIX, a część dotycząca administrowania opisuje czynności administracyjne związane z uwierzytelnianiem i hasłem. Część dotycząca administrowania może także opisywać atrybuty administracyjne konta użytkownika związane z uwierzytelnianiem, przez zaimplementowanie pewnych interfejsów modułu ładowalnego (newuser, getentry, putentry itp.).

Metoda uwierzytelniania jest kontrolowana przez atrybut **SYSTEM** i atrybuty rejestru zdefiniowane w pliku /etc/security/user. Administrator systemu może zdefiniować atrybut authcontroldomain w pliku /etc/security/login.cfg, aby wymusić pobranie atrybutu **SYSTEM** i atrybutów rejestru z authcontroldomain. Na przykład ustawienie authcontroldomain=LDAP wymusza wyszukiwanie atrybutów **SYSTEM** i rejestru użytkownika w serwerze LDAP, aby określić metodę uwierzytelniania dla danego użytkownika. Istnieje jeden wyjątek dla użytkowników zdefiniowanych lokalnie, dla których ustawienie authcontroldomain jest ignorowane i atrybut **SYSTEM** oraz atrybuty rejestru są zawsze pobierane z pliku /etc/security/user.

Akceptowalnym tokenem dla atrybutu authcontroldomain są pliki lub nazwa sekcji w pliku /usr/lib/security/methods.cfg.

Wartość atrybutu **SYSTEM** definiowana jest za pomocą gramatyki. Korzystając z tej gramatyki, administratorzy systemów mogą łączyć jedną lub więcej metod w celu uwierzytelnienia poszczególnych użytkowników w systemie. Dobrze znanymi znacznikami metod są compat, DCE, files i NONE.

Wartością domyślną w systemie jest compat. Wartość domyślna SYSTEM=compat informuje system, że w celu uwierzytelniania ma być użyta lokalna baza danych, a jeśli to się nie powiedzie, należy użyć bazy danych NIS (Network Information Services). Znacznik files określa, że podczas uwierzytelniania mają być używane tylko lokalne pliki, natomiast SYSTEM=DCE określa przepływ uwierzytelniania DCE.

Znacznik NONE powoduje wyłączenie metod uwierzytelniania. Aby całkowicie wyłączyć uwierzytelnianie, element NONE musi znajdować się w wierszach SYSTEM i auth1 sekcji użytkownika.

Użytkownik może określić dwie lub więcej metod i połączyć je za pomocą konstruktorów logicznych AND i OR. Na przykład SYSTEM=DCE OR compat wskazuje, że użytkownik może się zalogować, jeśli powiedzie się uwierzytelnianie DCE lub lokalne (crypt()).

W podobny sposób administrator systemu może użyć nazw modułów ładowalnych uwierzytelniania dla atrybutu **SYSTEM**. Na przykład, gdy atrybut SYSTEM ma wartość SYSTEM=KRB5files OR compat, host AIX najpierw spróbuje przepływu Kerberos w celu uwierzytelnienia, a jeśli się to nie powiedzie, spróbuje standardowego uwierzytelniania AIX.

Atrybuty **SYSTEM** i **registry** zawsze przechowywane są w lokalnym systemie plików w pliku /etc/security/user. Jeśli użytkownik AIX został zdefiniowany w katalogu LDAP, a atrybuty **SYSTEM** i

registry są ustawione odpowiednio, wtedy pozycja dla użytkownika będzie znajdowała się w pliku `/etc/security/user`.

Atrybuty **SYSTEM** i **registry** dla użytkownika można zmienić za pomocą komendy **chuser**.

Dopuszczalne tokeny dla atrybutu **SYSTEM** mogą zostać zdefiniowane w pliku `/usr/lib/security/methods.cfg`.

Uwaga: Użytkownik root jest zawsze uwierzytelniany za pomocą pliku zabezpieczeń lokalnego systemu. Pozycja atrybutu **SYSTEM** dla użytkownika root jest ustawiana na SYSTEM=`compat` w pliku `/etc/security/user`.

Alternatywne metody uwierzytelniania są zintegrowane w systemie za pomocą atrybutu **SYSTEM**, który znajduje się w pliku `/etc/security/user`. Na przykład Rozproszone środowisko przetwarzania danych (Distributed Computing Environment - DCE) wymaga uwierzytelniania hasłem, ale potwierdza to hasło w sposób różny od modelu szyfrowania użytego w plikach `/etc/passwd` i `/etc/security/passwd`. Użytkownik uwierzytelniający się za pomocą środowiska DCE może mieć swoją sekcję w pliku `/etc/security/user` ustawioną na SYSTEM=`DCE.`

Inne wartości atrybutu **SYSTEM** to **compat**, **files** i **NONE**. Element `compat` jest używany w przypadku, gdy tłumaczenie nazw (i kolejne uwierzytelnianie) następuje przy użyciu lokalnej bazy danych, a jeśli tłumaczenie nie zakończy się sukcesem, użyta zostanie baza systemu informacji sieciowej (NIS). Element `files` określa, że podczas uwierzytelniania mają być używane tylko lokalne pliki. Na koniec element `NONE` wyłącza metodę uwierzytelniania. Aby całkowicie wyłączyć uwierzytelnianie, element `NONE` musi znajdować się w wierszach **SYSTEM** i **auth1** sekcji użytkownika.

Inne dopuszczalne tokeny dla atrybutu **SYSTEM** mogą zostać zdefiniowane w pliku `/usr/lib/security/methods.cfg`.

Uwaga: Użytkownik root jest zawsze uwierzytelniany za pomocą pliku zabezpieczeń lokalnego systemu. Pozycja atrybutu **SYSTEM** dla użytkownika root jest ustawiana na SYSTEM `= "compat"` w pliku `/etc/security/user`.

Więcej informacji na temat zabezpieczania haseł można znaleźć w książce *Zarządzanie systemami operacyjnymi i urządzeniami*.

Identyfikatory logowania użytkowników

Wszystkie zdarzenia kontroli zapisane dla tego użytkownika są oznaczone tym identyfikatorem i mogą być zbadane po wygenerowaniu rekordów kontroli. Więcej informacji na temat identyfikatorów użytkowników można znaleźć w książce *Zarządzanie systemami operacyjnymi i urządzeniami*.

Atrybuty użytkowników i grup obsługiwane przez moduły ładowalne uwierzytelniania

W celu zapewnienia identyfikacji i uwierzytelniania w systemie AIX wykorzystywany jest zbiór atrybutów związanych z użytkownikami i grupami.

Poniższe tabele zawierają większość z tych atrybutów użytkowników i grup oraz informacje o modułach ładowalnych, które zapewniają obsługę tych atrybutów. Każdy wiersz tabeli odpowiada atrybutowi, a każda kolumna reprezentuje moduł ładowalny. Atrybuty obsługiwane przez moduł ładowalny zawierają w kolumnie moduły ładowalnego słowo Tak.

Uwaga: PKI i Kerberos są modułami używanymi wyłącznie do uwierzytelniania i trzeba je łączyć z modelem bazy danych (takim jak LOCAL lub LDAP). Obsługują one pewne dodatkowe (rozszerzone) atrybuty, inne od udostępnianych przez LOCAL lub LDAP. W przypadku tych modułów zaznaczona jest obsługa wyłącznie atrybutów rozszerzonych, mimo że funkcje innych atrybutów można zapewnić przy użyciu modeli LOCAL lub LDAP.

Tabela 7. Obsługa atrybutów użytkowników przez moduły ładowalne uwierzytelniania

Atrybut użytkownika	Lokalna	NIS/NIS+	LDAP	PKI	Kerberos
account_locked	Tak	Nie	Tak	Nie	Nie
admgroups	Tak	Nie	Tak	Nie	Nie

Tabela 7. Obsługa atrybutów użytkowników przez moduły ładowalne uwierzytelniania (kontynuacja)

Atrybut użytkownika	Lokalna	NIS/NIS+	LDAP	PKI	Kerberos
admin	Tak	Nie	Tak	Nie	Nie
auditclasses	Tak	Nie	Tak	Nie	Nie
auth_cert	Nie	Nie	Nie	Tak	Nie
auth_domain	Tak	Nie	Tak	Nie	Nie
auth_name	Tak	Nie	Tak	Nie	Nie
auth1 **Uwaga:** Atrybut **auth1** jest nieaktualny. Nie należy go używać.	Tak	Nie	Tak	Nie	Nie
auth2 **Uwaga:** Atrybut **auth2** jest nieaktualny. Nie należy go używać.	Tak	Nie	Tak	Nie	Nie
capabilities	Tak	Nie	Tak	Nie	Nie
core	Tak	Nie	Tak	Nie	Nie
core_compress	Tak	Nie	Nie	Nie	Nie
core_hard	Tak	Nie	Tak	Nie	Nie
core_naming	Tak	Nie	Nie	Nie	Nie
core_path	Tak	Nie	Nie	Nie	Nie
core_pathname	Tak	Nie	Nie	Nie	Nie
cpu	Tak	Nie	Tak	Nie	Nie
daemon	Tak	Nie	Tak	Nie	Nie
data	Tak	Nie	Tak	Nie	Nie
data_hard	Tak	Nie	Tak	Nie	Nie
dce_export	Tak	Nie	Tak	Nie	Nie
dictionlist	Tak	Nie	Tak	Nie	Nie
expires	Tak	Nie	Tak	Nie	Tak
flags	Tak	Nie	Tak	Nie	Tak
fsize	Tak	Nie	Tak	Nie	Nie
fsize_hard	Tak	Nie	Tak	Nie	Nie
funcmode	Tak	Nie	Tak	Nie	Nie
gecos	Tak	Tak	Tak	Nie	Nie
groups	Tak	Tak	Tak	Nie	Nie
groupsids	Tak	Tak	Tak	Nie	Nie
histexpire	Tak	Nie	Tak	Nie	Nie
home	Tak	Tak	Tak	Nie	Nie
host_last_login	Tak	Nie	Tak	Nie	Nie

Tabela 7. Obsługa atrybutów użytkowników przez moduły ładowalne uwierzytelniania (kontynuacja)					
Atrybut użytkownika	**Lokalna**	**NIS/NIS+**	**LDAP**	**PKI**	**Kerberos**
host_last_unsuccessful_login	Tak	Tak	Tak	Nie	Nie
hostsallowedlogin	Tak	Nie	Tak	Nie	Nie
hostsdeniedlogin	Tak	Nie	Tak	Nie	Nie
id	Tak	Tak	Tak	Nie	Nie
krb5_attributes	Nie	Nie	Nie	Nie	Tak
krb5_kvno	Nie	Nie	Nie	Nie	Tak
krb5_last_pwd_change	Nie	Nie	Nie	Nie	Tak
krb5_max_renewable_life	Nie	Nie	Nie	Nie	Tak
krb5_mknvo	Nie	Nie	Nie	Nie	Tak
krb5_mod_date	Nie	Nie	Nie	Nie	Tak
krb5_mod_name	Nie	Nie	Nie	Nie	Tak
krb5_names	Nie	Nie	Nie	Nie	Tak
krb5_principal	Nie	Nie	Nie	Nie	Tak
krb5_principal_name	Nie	Nie	Nie	Nie	Tak
krb5_realm	Nie	Nie	Nie	Nie	Tak
lastupdate	Tak	Tak	Tak	Nie	Nie
login	Tak	Nie	Tak	Nie	Nie
loginretries	Tak	Nie	Tak	Nie	Nie
logintimes	Tak	Nie	Tak	Nie	Nie
maxage	Tak	Tak	Tak	Nie	Tak
maxexpired	Tak	Tak	Tak	Nie	Nie
maxrepeats	Tak	Nie	Tak	Nie	Nie
maxulogs	Tak	Nie	Tak	Nie	Nie
minage	Tak	Tak	Tak	Nie	Nie
minalpha	Tak	Nie	Tak	Nie	Nie
mindiff	Tak	Nie	Tak	Nie	Nie
mindigit	Tak	Nie	Tak	Nie	Nie
minlen	Tak	Nie	Tak	Nie	Nie
minloweralpha	Tak	Nie	Tak	Nie	Nie
minother	Tak	Nie	Tak	Nie	Nie
minspecialchar	Tak	Nie	Tak	Nie	Nie
minupperalpha	Tak	Nie	Tak	Nie	Nie
nofiles	Tak	Nie	Tak	Nie	Nie
nofiles_hard	Tak	Nie	Tak	Nie	Nie

Tabela 7. Obsługa atrybutów użytkowników przez moduły ładowalne uwierzytelniania (kontynuacja)

Atrybut użytkownika	Lokalna	NIS/NIS+	LDAP	PKI	Kerberos
password	Tak	Tak	Tak	Nie	Nie
pgid	Tak	Tak	Nie	Nie	Nie
pgrp	Tak	Tak	Tak	Nie	Nie
projects	Tak	Nie	Tak	Nie	Nie
pwdchecks	Tak	Nie	Tak	Nie	Nie
pwdwarntime	Tak	Nie	Tak	Nie	Nie
rcmds	Tak	Nie	Tak	Nie	Nie
registry	Tak	Nie	Nie	Nie	Nie
rlogin	Tak	Nie	Tak	Nie	Nie
roles	Tak	Nie	Tak	Nie	Nie
rss	Tak	Nie	Tak	Nie	Nie
rss_hard	Tak	Nie	Tak	Nie	Nie
screens	Tak	Nie	Tak	Nie	Nie
shell	Tak	Tak	Tak	Nie	Nie
spassword	Tak	Tak	Tak	Nie	Nie
stack	Tak	Nie	Tak	Nie	Nie
stack_hard	Tak	Nie	Tak	Nie	Nie
su	Tak	Nie	Tak	Nie	Nie
sugroups	Tak	Nie	Tak	Nie	Nie
sysenv	Tak	Nie	Tak	Nie	Nie
SYSTEM	Tak	Nie	Nie	Nie	Nie
time_last_login	Tak	Nie	Tak	Nie	Nie
time_last_unsuccessful_login	Tak	Nie	Tak	Nie	Nie
tpath	Tak	Nie	Tak	Nie	Nie
tty_last_login	Tak	Nie	Tak	Nie	Nie
tty_last_unsuccessful_login	Tak	Nie	Tak	Nie	Nie
ttys	Tak	Nie	Tak	Nie	Nie
umask	Tak	Nie	Tak	Nie	Nie
unsuccessful_login_count	Tak	Nie	Tak	Nie	Nie
unsuccessful_login_times	Tak	Nie	Tak	Nie	Nie
usrenv	Tak	Nie	Tak	Nie	Nie

Tabela 8. Obsługa atrybutów grup przez moduły ładowalne uwierzytelniania

Atrybut użytkownika	Lokalna	NIS/NIS+	LDAP	PKI	Kerberos
admin	Tak	Nie	Tak	Nie	Nie

Tabela 8. Obsługa atrybutów grup przez moduły ładowalne uwierzytelniania (kontynuacja)					
Atrybut użytkownika	**Lokalna**	**NIS/NIS+**	**LDAP**	**PKI**	**Kerberos**
adms	Tak	Nie	Tak	Nie	Nie
dce_export	Tak	Nie	Tak	Nie	Nie
id	Tak	Tak	Tak	Nie	Nie
primary	Tak	Nie	Tak	Nie	Nie
projects	Tak	Nie	Tak	Nie	Nie
screens	Tak	Nie	Tak	Nie	Nie
users	Tak	Tak	Tak	Nie	Nie

Przegląd systemu limitowania pamięci dyskowej
Limit pamięci dyskowej umożliwia administratorom systemu kontrolowanie liczby plików i bloków danych, które mogą być przydzielone użytkownikom lub grupom.

Założenia systemu limitowania pamięci dyskowej
System limitowania pamięci dyskowej, który bazuje na systemie limitowania pamięci dyskowej Berkeley Disk Quota System, zapewnia efektywny sposób kontrolowania użycia przestrzeni dyskowej. System limitowania może być zdefiniowany dla indywidualnych użytkowników lub dla grup i jest obsługiwany przez każdy system plików (JFS i JFS2).

System limitowania pamięci dyskowej tworzy limity w oparciu o następujące parametry, które można zmieniać przy użyciu komendy dla systemu plików JFS **edquota** oraz komendy dla systemu plików JFS2 **j2edlimit**:

- miękkie limity użytkownika lub grupy,
- twarde limity użytkownika lub grupy,
- okres karencji limitu.

Miękki limit definiuje liczbę bloków dyskowych o rozmiarze 1 kB lub plików, których użytkownik lub grupa może używać podczas normalnego działania. *Twardy limit* definiuje maksymalną liczbę bloków dyskowych lub plików, które użytkownik może zgromadzić w obrębie utworzonego limitu pamięci dyskowej. *Okres karencji limitu* umożliwia użytkownikowi przekroczenie limitu miękkiego na krótki okres (wartość domyślna to tydzień). Jeśli użytkownik przez określony czas nie zmniejszy użytego miejsca dyskowego na niższe niż miękki limit, system zinterpretuje miękki limit jako maksymalną dozwoloną przestrzeń i użytkownik nie będzie mógł przechowywać dodatkowych plików. Użytkownik może zresetować ten warunek, usuwając odpowiednią liczbę plików w celu zmniejszenia użytej przestrzeni dyskowej poniżej miękkiego limitu.

System limitowania pamięci dyskowej śledzi limity użytkowników i grup w plikach `quota.user` i `quota.group` znajdujących się w katalogach głównych systemów plików, które mają włączone limity. Te pliki są tworzone za pomocą komend **quotacheck** i **edquota** i można je odczytać, używając komendy quota.

Usuwanie skutków wystąpienia warunku przekroczenia limitu
Istnieje możliwość usunięcia skutków wystąpienia warunku przekroczenia limitu poprzez ograniczenie wykorzystania systemu plików.

Aby zmniejszyć użycie systemu plików po przekroczeniu limitu przestrzeni dyskowej, użyj następujących metod:

- Zatrzymaj bieżący proces, który spowodował osiągnięcie limitu w systemie plików, usuń nadmiarowe pliki, aby zmniejszyć zajmowaną przestrzeń dyskową poniżej limitu, a następnie spróbuj ponownie uruchomić program, którego wykonanie nie powiodło się.

- Jeśli uruchomiony jest edytor, taki jak vi, użyj sekwencji o zmienionym znaczeniu dla powłoki, aby sprawdzić ilość wolnego miejsca na dysku, usuń nadmiarowe pliki i wróć do pliku bez tracenia modyfikowanych danych. Ewentualnie, jeśli używana jest powłoka C lub Korn, możesz zawiesić proces edytora za pomocą sekwencji klawiszy Ctrl-Z, wywołać komendy systemu plików i powrócić za pomocą komendy **fg** (pierwszy plan).
- Tymczasowo zapisz plik do systemu plików, w którym limit przestrzeni dyskowej nie został osiągnięty, usuń nadmiarowe pliki i wczytaj plik ponownie do poprawionego systemu plików.

Konfigurowanie systemu limitowania pamięci dyskowej
Zwykle tylko systemy plików, które zawierają katalogi osobiste i pliki użytkowników, wymagają limitu pamięci dyskowej.

Należy rozważyć implementację systemu limitowania pamięci dyskowej w następującej sytuacji:

- w systemie jest ograniczona ilość miejsca na dysku,
- wymagane jest lepsze zabezpieczenie systemu plików,
- poziom użycia dysku jest wysoki, jak w przypadku wielu uniwersytetów.

Jeśli te warunki nie mają zastosowania w danym środowisku, nie jest konieczne tworzenie limitów użycia dysku przez implementację systemu limitowania pamięci dyskowej.

Systemu limitowania pamięci dyskowej można używać tylko w systemie plików JFS (Journaled File System).

Uwaga: Nie należy tworzyć limitów pamięci dyskowej dla systemu plików `/tmp`.

Aby skonfigurować system limitowania pamięci dyskowej, użyj następującej procedury:

1. Zaloguj się jako użytkownik root.
2. Określ, które systemy plików wymagają limitów.

   Uwaga: Ponieważ wiele edytorów i systemowych programów narzędziowych tworzy tymczasowe pliki w systemie plików `/tmp`, nie można na niego nakładać żadnych limitów.
3. Użyj komendy **chfs** w celu uwzględnienia atrybutów konfiguracyjnych limitów **userquota** i **groupquota** w pliku `/etc/filesystems`. W poniższym przykładzie komenda **chfs** została użyta do włączenia limitowania pamięci dyskowej w systemie plików `/home`:

   ```
   chfs -a "quota = userquota" /home
   ```

   Aby włączyć limity dla użytkowników i grup, w systemie plików `/home` należy wpisać:

   ```
   chfs -a "quota = userquota,groupquota" /home
   ```

   Odpowiedni wpis w pliku `/etc/filesystems` wygląda następująco:

   ```
   /home:
   dev        = /dev/hd1
   vfs        = jfs
   log        = /dev/hd8
   mount      = true
   check      = true
   quota      = userquota,groupquota
   options    = rw
   ```
4. Opcjonalnie określ alternatywne nazwy plików zawierające limity pamięci dyskowej. Nazwy plików `quota.user` i `quota.group` są nazwami domyślnymi umieszczonymi w katalogach głównych systemów plików z włączonym limitowaniem pamięci dyskowej. Za pomocą atrybutów **userquota** i **groupquota** w pliku `/etc/filesystems` można określić alternatywne nazwy lub katalogi dla plików zawierających limity pamięci dyskowej.

W poniższym przykładzie komenda **chfs** została użyta do utworzenia limitów użytkownika i grupy dla systemu plików /home i określenia nazw plików limitów myquota.user i myquota.group:

```
chfs -a "userquota = /home/myquota.user" -a "groupquota = /home
                /myquota.group" /home
```

Odpowiedni wpis w pliku /etc/filesystems wygląda następująco:

```
/home:
dev         = /dev/hd1
vfs         = jfs
log         = /dev/hd8
mount       = true
check       = true
quota       = userquota,groupquota
userquota   = /home/myquota.user
groupquota  = /home/myquota.group
options     = rw
```

5. Jeśli określone systemy plików nie zostały wcześniej podłączone, podłącz je teraz.
6. Ustaw żądane limity pamięci dyskowej dla każdego użytkownika lub grupy. Użyj komendy **edquota** do utworzenia limitów miękkich i twardych dla użytkownika i grupy, dotyczących dozwolonej przestrzeni dyskowej i maksymalnej liczby plików.

   Przykładowy poniższy wpis przedstawia limity przestrzeni dyskowej dla użytkownika *davec*:

   ```
   Limity dla użytkownika davec:
   /home: blocks in use: 30, limits (soft = 100, hard = 150)
                   inodes in use: 73, limits (soft = 200, hard = 250)
   ```

   Ten użytkownik użył 30 KB z maksymalnej dostępnej przestrzeni dyskowej równej 100 KB. Z maksymalnej liczby 200 plików użytkownik *davec* utworzył 73. Ma on przydzielone bufory o wielkości 50 KB przestrzeni dyskowej i 50 plików, które mogą być użyte na pliki tymczasowe.

   Po utworzeniu limitów pamięci dyskowej dla wielu użytkowników należy użyć opcji **-p** w komendzie **edquota** w celu powielenia limitów jednego użytkownika dla innego użytkownika.

   Aby powielić limity utworzone dla użytkownika *davec* dla użytkownika *nanc*, należy wpisać:

   ```
   edquota -p davec nanc
   ```

7. Włącz system limitowania za pomocą komendy **quotaon**. Komenda **quotaon** włącza limity dla określonego systemu plików lub dla wszystkich systemów plików z utworzonymi limitami (jak to określono w pliku /etc/filesystems), jeśli zostanie użyta opcja **-a**.
8. Użyj komendy **quotacheck** w celu sprawdzenia spójności plików limitowanych z obecnym użyciem dysku.

   Uwaga: Czynność tę należy wykonać po pierwszym włączeniu limitów w systemie plików i po restarcie systemu. Komenda **quotacheck** trwa dłużej w systemie plików JFS niż w systemie plików JFS2 o tej samej wielkości. Jeśli limitowanie jest włączone przez cały czas przed restartem, nie jest konieczne uruchamianie komendy **quotacheck** dla systemu plików podczas restartu.

   Aby aktywować to sprawdzanie i włączać limitowanie podczas uruchamiania systemu, należy dodać następujące wiersze na końcu pliku /etc/rc:

   ```
   echo " Włączanie limitowania systemu plików "
   /usr/sbin/quotacheck -a
   /usr/sbin/quotaon -a
   ```

Dozwolona liczba grup

Istnieje możliwość skonfigurowania i pobierania wartości dozwolonej liczby grup dla systemu AIX 7.1. Wartość ta definiuje, do ilu grup mogą należeć użytkownicy.

Domyślna wartość dozwolonej liczby grup wynosi 128. Można ją dostroić w zakresie od 128 do 2048. Wartość Dozwolona liczba grup jest określona w parametrze konfiguracji systemu v_ngroups_allowed

dla urządzenia sys0. Wartość parametru v_ngroups_allowed można zmieniać lub pobierać z jądra albo bazy danych ODM. Wartość tego parametru w jądrze jest używana podczas działania systemu. Wartość parametru w bazie danych ODM jest efektywna po restarcie systemu.

Pobieranie z bazy danych ODM wartości Dozwolona liczba grup

Aby pobrać parametr v_ngroups_allowed, należy użyć komend lub procedur. Aby pobrać parametr v_ngroups_allowed z bazy danych ODM, należy użyć komendy **lsattr**.

Komenda **lsattr** wyświetla parametr v_ngroups_allowed jako atrybut ngroups_allowed. W poniższym przykładzie przedstawiono sposób użycia komendy **lsattr** do pobrania atrybutu ngroups_allowed:

```
$ lsattr -El sys0
SW_dist_intr    fałsz            Włącz programową dystrybucję
przerwań                           Prawda
autorestart     prawda           Automatycznie RESTARTUJ system po
awarii                         Prawda
boottype        dysk             Nie
dotyczy                                          Fałsz
capacity_inc    1.00             Przyrost mocy obliczeniowej
procesora                          Fałsz
capped          prawda           Partycja jest
limitowana                                   Fałsz
conslogin       włącz            Login na konsoli
systemowej                                 Fałsz
cpuguard        włącz            Ochrona
CPU                                                Prawda
dedicated       prawda           Partycja jest
dedykowana                                   Fałsz
ent_capacity    4.00             Uprawniona moc obliczeniowa
procesora                          Fałsz
frequency       93750000         Częstotliwość magistrali
systemowej                             Fałsz
fullcore        fałsz            Aktywowanie pełnego zrzutu
CORE                                Prawda
fwversion       IBM,SPH01316     Wersja oprogramowania wbudowanego i poziomy
poprawek             Fałsz
iostat          fałsz            Stałe utrzymywanie historii DYSKOWYCH OPERACJI WE/
WY            Prawda
keylock         normalny         Położenie kluczyka w momencie ładowania
systemu                 Fałsz
max_capacity    4.00             Maksymalna potencjalna moc obliczeniowa
procesora               Fałsz
max_logname     20               Maksymalna długość nazwy użytkownika podczas
startu              Prawda
maxbuf          20               Maks. liczba stron PAMIĘCI PODRĘCZNEJ BUFORÓW blokowego WE/
WY    Prawda
maxmbuf         0                Maksymalna liczba kilobajtów pamięci rzeczywistej
                                 dozwolonej dla buforów
MBUF                                      Prawda
maxpout         0                GÓRNY znacznik oczekujących operacji we/wy dla
                                 pojedynczego
pliku                                              Prawda
maxuproc        128              Maksymalna liczba PROCESÓW dostępnych dla
                                 jednego
użytkownika                                        Prawda
min_capacity    1.00             Minimalna potencjalna moc obliczeniowa
procesora                Fałsz
minpout         0                DOLNY znacznik oczekujących operacji we/wy dla
                                 pojedynczego
pliku                                              Prawda
modelname       IBM,7044-270     Nazwa
maszyny                                                Fałsz
ncargs          6                Wielkość listy ARG/ENV w 4-kilobajtowych
blokach               Prawda
pre430core      fałsz            Użyj zrzutu pamięci w stylu sprzed wersji
4.3.0                 Prawda
pre520tune      wyłącz           Tryb kompatybilności strojenia z wersjami wcześniejszymi od
520  Prawda
realmem         3145728          Ilość użytecznej pamięci fizycznej w
kilobajtach               Fałsz
rtasversion     1                Wersja Open Firmware
RTAS                                     Fałsz
sec_flags       0                Opcje
bezpieczeństwa                                     Prawda
sed_config      wybierz          Tryb wyłączenia wykonywania stosu
(SED)                          Prawda
```

```
systemid        IBM,0110B5F5F    Identyfikator sprzętu
systemowego                                Fałsz
variable_weight 0                Zmienna waga mocy obliczeniowej
procesora                        Fałsz
ngroups_allowed 128              Dozwolona liczba grup podczas
startu                             Prawda
$
```

Pobieranie z jądra dozwolonej liczby grup

W celu pobrania z jądra parametru `v_ngroups_allowed` należy użyć procedury `sys_param`.

```
#include<sys/types.h>
#include<sys/var.h>
#include<errno.h>
main()
{
 int rc;
 struct vario myvar;

 rc = sys_parm (SYSP_GET, SYSP_V_NGROUPS_ALLOWED, &myvar);

 if (!rc)
 printf("Dozwolona liczba grup = %d\n",
 myvar.v.v_ngroups_allowed.value);
 else
 printf("sys_parm() nie powiodło się, rc = %d, errno = %d\n", rc, errno);
 }
```

Zmiana wartości Dozwolona liczba grup w bazie danych ODM

Podczas fazy startu systemu należy skonfigurować w jądrze wartość Dozwolona liczba grup. Za pomocą komendy **chdev** można zmienić tę wartość w bazie danych ODM. Zmiana ta odniesie skutek po restarcie systemu.

Aby zmienić parametr **v_ngroups_allowed** w bazie danych ODM za pomocą komendy **chdev**, wpisz:

```
$ chdev -l sys0 -a ngroups_allowed=2048
sys0 changed
$
```

Kontrola dostępu oparta na rolach

Administrowanie systemem to ważna część codziennie wykonywanych czynności. Zapewnianie bezpieczeństwa jest nieodłączną częścią pracy administratora. Oprócz zabezpieczania środowiska operacyjnego, niezbędne jest uważne monitorowanie działania systemu.

W większości środowisk wymagane jest, aby różni użytkownicy pełnili różne obowiązki administracyjne. Konieczne jest zapewnienie rozłączności tych obowiązków, aby jedna osoba z uprawnieniami administracyjnymi nie mogła przypadkowo lub złośliwie ominąć zabezpieczeń systemowych. W tradycyjnym administrowaniu systemem UNIX nie można tego osiągnąć, ale jest to możliwe przy użyciu kontroli dostępu opartej na rolach (Role-Based Access Control - RBAC).

Ograniczenia w administrowaniu tradycyjnym systemem UNIX
Kontrola RBAC rozwiązuje niektóre zagadnienia związane z administrowaniem tradycyjnym systemem UNIX. Zagadnienia te są następujące:

Konto administracyjne użytkownika root

Tradycyjnie w systemie AIX i innych systemach operacyjnych UNIX jest zdefiniowane jedno konto administratora systemu o nazwie **root** (zwykle oznaczone identyfikatorem UID równym 0). Konto to umożliwia wykonywanie wszystkich uprzywilejowanych zadań administracyjnych w systemie. Zależność od jednego użytkownika wykonującego wszystkie zadania administrowania stanowi problem w związku z rozdzielaniem obowiązków. W niektórych środowiskach jedno konto administracyjne jest akceptowalne, jednak większość środowisk wymaga wielu administratorów, a każdy z nich powinien być odpowiedzialny za różne zadania administrowania systemem.

W celu współużytkowania zakresu odpowiedzialności administratorów przez wielu użytkowników systemu starą praktyką było współużytkowanie hasła użytkownika root albo tworzenie innego użytkownika o takim samym identyfikatorze UID, co użytkownik root. Taka metoda współużytkowania obowiązków administratora systemu stanowi problem z punktu widzenia bezpieczeństwa, ponieważ każdy administrator ma pełną kontrolę nad systemem i nie ma możliwości ograniczenia operacji, które może wykonać. Ponieważ użytkownik root jest najbardziej uprzywilejowanym użytkownikiem, użytkownicy root mogą wykonywać nieautoryzowane operacje i usuwać wszystkie zapisy kontrolne dotyczące swoich działań, uniemożliwiając śledzenie czynności administracyjnych.

Eskalacja uprawnień za pomocą bitu SUID

Przy kontroli dostępu w systemach operacyjnych UNIX do określenia praw dostępu była używana wartość UID powiązana z procesem. Jednak identyfikator UID użytkownika root równy 0 tradycyjnie zezwalał na ominięcie wszystkich kontroli uprawnień. Dlatego proces uruchomiony z prawami użytkownika root może przejść dowolne sprawdzenie praw dostępu i wykonać każdą operację. Jest to zagadnienie bezpieczeństwa związane z wywodzącą się z systemu UNIX koncepcją aplikacji z bitem **setuid**.

Bit **setuid** umożliwia uruchomienie komendy z tożsamością inną niż użytkownika wywołującego tę komendę. Jest to niezbędne, gdy zwykły użytkownik musi wykonać uprzywilejowane zadanie. Przykładem jest komenda AIX **passwd**. Zwykły użytkownik nie ma prawa dostępu do pliku przechowującego hasła użytkowników, a do zmiany hasła użytkownika jest potrzebne dodatkowe uprawnienie, dlatego komenda **passwd** jest przy użyciu bitu **setuid** wykonywana z uprawnieniami użytkownika root. Gdy zwykły użytkownik uruchamia komendę **passwd**, w systemie operacyjnym wygląda to tak, jakby użytkownik root uzyskiwał dostęp do pliku, więc dostęp ten jest przyznawany.

Wprawdzie pojęcie to zapewnia żądaną funkcjonalność, jednak niesie ze sobą nieodłącznie ryzyko. Ponieważ program **setuid** jest efektywnie uruchamiany w kontekście użytkownika root, jeśli atakujący pomyślnie przejmie program przed jego zakończeniem, wtedy uzyska pełnię władzy użytkownika root i następnie może ominąć wszystkie kontrole dostępu systemu operacyjnego i wykonywać wszystkie operacje. Lepszym rozwiązaniem jest przypisanie tylko podzbioru uprawnień użytkownika root do programu. Spełniona jest wtedy “Zasada najmniejszych uprawnień” na stronie 85, a zagrożenie zmniejszone.

Elementy kontroli RBAC

Kontrola RBAC umożliwia tworzenie ról do administrowania systemem oraz delegację zadań związanych z administrowaniem do zaufanych użytkowników systemu. W systemie AIX kontrola RBAC udostępnia mechanizm, dzięki któremu funkcje administracyjne, zwykle zarezerwowane dla użytkownika root, można przypisać do zwykłych użytkowników systemu.

Jest to osiągane dzięki zdefiniowaniu funkcji zadań (ról) w organizacji i przypisaniu tych ról do konkretnych użytkowników. Kontrola RBAC jest środowiskiem umożliwiającym administrację systemem poprzez wykorzystanie ról. Zwykle zasięg zarządzania definiowanych ról dotyczy jednego lub kilku aspektów administracyjnych w środowisku. Przypisanie roli użytkownikowi to przyznanie mu zestawu uprawnień i możliwości. Na przykład jedna rola związana z zarządzaniem może służyć do zarządzania systemami plików, a inna może umożliwiać tworzenie kont użytkowników.

Administrowanie z kontrolą RBAC ma następujące zalety w porównaniu z tradycyjną administracją w systemach UNIX:

- Systemem może administrować wielu użytkowników, którzy nie muszą współużytkować dostępu do jednego konta.
- Rozdzielenie zabezpieczeń zapewnione przez administrację szczegółową, ponieważ administratorzy nie potrzebują mieć więcej uprawnień, niż wymagają ich zadania.
- Możliwość wymuszenia modelu zabezpieczeń z najmniejszymi uprawnieniami. Użytkownicy i aplikacje mają nadane tylko niezbędne uprawnienia, gdy są one wymagane, co pozwala zmniejszyć wpływ atakującego w przypadku wystąpienia ataku na system.
- Możliwość zaimplementowania i wymuszenia spójnej strategii bezpieczeństwa dla całego przedsiębiorstwa dotyczącej zarządzania systemem i kontroli dostępu.

- Definicję roli można utworzyć raz, a następnie przypisywać ją do użytkowników lub usuwać przypisanie, gdy zmieniają się funkcje użytkowników.

Środowisko RBAC jest skoncentrowane na następujących trzech pojęciach podstawowych:

- Autoryzacje
- Role
- Uprawnienia

Wszystkie te pojęcia umożliwiają wymuszenie przez kontrolę RBAC zasady najmniejszych uprawnień.

Autoryzacje
Autoryzacja to łańcuch tekstowy powiązany z funkcjami lub komendami związanymi z bezpieczeństwem. Autoryzacje zapewniają mechanizm nadawania praw użytkownikom, aby mogli oni wykonywać akcje uprzywilejowane oraz udostępniania różnych poziomów funkcjonalności różnym klasom użytkowników.

Gdy działa komenda zarządzana przez autoryzację, dostęp jest nadawany, tylko jeśli użytkownik wywołujący ma żądaną autoryzację. Autoryzację można uznać za klucz, którym można odblokować dostęp do jednej lub kilku komend. Autoryzacje nie są przypisywane bezpośrednio użytkownikom. Użytkownikom są przypisywane role, będące kolekcjami autoryzacji.

Role
Role umożliwiają utworzenie grupy z zestawu funkcji zarządzania systemem. Używając porównania autoryzacji do klucza, możemy porównać rolę do kółka z kluczami, może ona przechować wiele autoryzacji. Autoryzacje można przypisać do roli bezpośrednio lub pośrednio z użyciem roli podrzędnej. Rola podrzędna jest po prostu inną rolą, z której dana rola dziedziczy autoryzacje.

Rola sama w sobie nie zapewnia użytkownikowi żadnych dodatkowych możliwości, ale służy jako mechanizm kolekcjonowania autoryzacji i narzędzie do przypisywania autoryzacji do użytkownika. Definiując rolę i przypisując ją do użytkownika, można określić zadania administracyjne, które może on wykonać. Po zdefiniowaniu roli, administrator roli może ją przypisać do jednego lub wielu użytkowników, aby zarządzali operacjami uprzywilejowanymi reprezentowanymi przez tę rolę. Ponadto jednemu użytkownikowi można przypisać wiele ról. Użytkownik z przypisaną rolą może użyć autoryzacji przypisanych do roli, aby odblokować dostęp do komend administracyjnych w systemie.

Strategie i procedury organizacyjne określają sposób przydzielania ról do użytkowników. Nie należy przypisywać zbyt wielu autoryzacji do roli ani przypisywać roli do zbyt wielu użytkowników. Większość ról powinna być przypisana wyłącznie do użytkowników należących do obsługi administracyjnej. Tak jak dotąd uprawnienia użytkownika root były nadawane tylko zaufanym użytkownikom, tak również role należy przypisywać tylko zaufanym użytkownikom. Role należy nadawać tylko użytkownikom zgłaszającym taką potrzebę i tylko na tyle, na ile są potrzebne. Stosowanie takiej praktyki zmniejsza szansę uzyskania lub nadużycia autoryzacji przez nieuprawnionego użytkownika.

Uprawnienia
Uprawnienie jest atrybutem procesu, które umożliwia obejście konkretnych ograniczeń i limitów w systemie.

Mechanizm uprawnień udostępnia zaufane aplikacje, o możliwościach niedostępnych dla aplikacji niezaufanych. Na przykład uprawnień można używać do nadpisania ograniczeń zabezpieczeń, do zezwolenia na większe wykorzystanie pewnych zasobów systemowych, takich jak pamięć czy miejsce na dysku, oraz do dostosowania wydajności i priorytetu procesu. O uprawnieniu można myśleć jako o zdolności pozwalającej procesowi pokonać konkretne ograniczenie zabezpieczeń w systemie.

Autoryzacje i role są narzędziami używanymi na poziomie użytkownika do konfigurowania możliwości dostępu użytkownika do operacji uprzywilejowanych. Z drugiej strony uprawnienia są mechanizmem służącym do ograniczania, używanym przez jądro w celu określenia, czy proces ma prawo wykonać konkretne działanie.

Uprawnienia są powiązane z procesem i są zwykle uzyskiwane przez wywołanie komendy uprzywilejowanej. Dzięki tym przypisanym uprawnieniom proces może wykonać odpowiednie operacje uprzywilejowane. Na przykład, jeśli użytkownik używa roli, która ma autoryzację do uruchomienia komendy, w momencie uruchomienia tej komendy do procesu jest przypisywany zestaw uprawnień.

Zasada najmniejszych uprawnień
W systemie operacyjnym niektóre operacje są uprzywilejowane, a uprawnienie do ich wykonywania jest zastrzeżone tylko dla autoryzowanych użytkowników. Operacje te zwykle obejmują zadania takie jak restartowanie systemu, dodawanie i zmiana systemów plików, dodawanie i usuwanie użytkowników oraz zmiana daty i czasu systemowego.

W tradycyjnych systemach UNIX proces lub użytkownik może być w trybie normalnym lub uprzywilejowanym (zwanym również trybem administratora lub użytkownika root). Proces uruchomiony w trybie użytkownika root może wykonywać dowolne komendy oraz operacje w systemie, a w trybie normalnego użytkownika nie może wykonywać operacji uprzywilejowanych. W tradycyjnym systemie UNIX pojęcie uprawnień jest prymitywne, definiujące wszystko-albo-nic, a bezpieczeństwo zależy od nadmiernie uprawnionego administratora.

Rozwiązanie z tradycyjnego systemu UNIX, w którym jeden tryb uprzywilejowany gwarantuje pełen dostęp do całego systemu, jest zbyt mało finezyjne, aby sprostać wymaganiom stawianym systemom o wysokim poziomie bezpieczeństwa. System zaprojektowany jako bezpieczny wymaga, aby każdy proces dostawał najbardziej okrojony zestaw uprawnień potrzebnych do wykonania zadania. Zaletą systemu uprawnień jest to, że trzeba nadać uprawnienia tylko procesom, które ich wymagają. Takie okrojenie uprawnień jest znane jako zasada najmniejszych uprawnień i pomaga ograniczyć uszkodzenia systemu spowodowane przez niedbałych lub złośliwych administratorów i operatorów.

Na przykład zmiana hasła wymaga określonych uprawnień, w celu dostępu do plików, które nie są zwykle dostępne dla zwykłego użytkownika. Gdyby użytkownicy zawsze mieli te uprawnienia, mogliby również podjąć inne działania, niepożądane z punktu widzenia bezpieczeństwa. Dlatego wymagane uprawnienia są nadawane tylko do komendy **passwd**, a nie wszystkim użytkownikom.

W środowisku RBAC sami użytkownicy nie mają żadnych nieodłącznych uprawnień. Użytkownicy mogą po prostu uruchomić pewne komendy, którym są nadawane uprawnienia. Jeśli użytkownik ma nadane mu bezpośrednio uprawnienia, może ich używać w każdej chwili i w dowolny sposób. Ograniczając uprawnienia do poszczególnych komend, można wymusić kontekst, w jakim będą one stosowane. Powoduje to rozbudowanie zabezpieczeń, ponieważ jeśli atakujący przełamie zabezpieczenia zaufanej aplikacji, uzyska dostęp do ograniczonego zestawu uprawnień, a nie pełną władzę użytkownika root ze wszystkimi uprawnieniami.

Zaufane aplikacje należy starannie sprawdzić przed nadaniem im uprawnień. Ponadto uprawnienia należy nadać wtedy, gdy jest to konieczne dla aplikacji, i tylko tam, gdzie jest to niezbędne. Aplikacje zaufane są takie, jak inne programy, jedyna różnica polega na tym, że aplikacje zaufane mogą wykonywać działania zabronione dla aplikacji niezaufanych.

Kontrola RBAC w systemie AIX
AIX udostępniał ograniczoną implementację kontroli RBAC w wersjach wcześniejszych niż AIX 6.1.

Począwszy od systemu AIX 6.1 wprowadzono nową implementację kontroli RBAC, zapewniającą dokładny mechanizm granulacji do dzielenia zadań administrowania systemem. Stosowane są dwa terminy służące do rozgraniczenia obu implementacji RBAC różniących się znacznie funkcjonalnością:

Wcześniejszy tryb RBAC
Historyczne zachowanie ról w systemie AIX, stosowane w wersjach sprzed AIX 6.1

Rozszerzony tryb RBAC
Nowa implementacja wprowadzona w systemie AIX 6.1

Obsługiwane są oba tryby operacji. Domyślnie w nowo instalowanym systemie AIX 6.1 jest ustawiany rozszerzony tryb RBAC. W poniższych sekcjach przedstawiono krótkie omówienie obydwu trybów i różnic między nimi oraz informacje dotyczące konfigurowania żądanego trybu RBAC w systemie.

Wcześniejszy tryb RBAC
W systemach wcześniejszych niż AIX 6.1 system AIX udostępniał ograniczoną funkcjonalność RBAC umożliwiającą wykonywanie pewnych zadań związanych z administrowaniem systemem użytkownikom innym niż root.

W tej implementacji kontroli RBAC, gdy daną komendę administracyjną wywołuje użytkownik inny niż root, jej kod określa, czy do użytkownika jest przypisana rola z wymaganą autoryzacją. Gdy zostanie

znaleziony pasujący wpis, wykonanie komendy jest kontynuowane. Jeśli nie, komenda zakończy się niepowodzeniem i błędem. Często jest wymagane, aby komenda podlegająca kontroli autoryzacji była wykonywana z uprawnieniami użytkownika root przy użyciu bitu **setuid**, aby autoryzowany użytkownik ją wywołujący miał uprawnienia niezbędne do wykonania danej operacji.

Ta implementacja kontroli RBAC wprowadza również predefiniowany zestaw autoryzacji, które użytkownik może rozszerzyć, a które służą do określenia dostępu do komend administracyjnych. Ponadto udostępnione jest również środowisko administracyjnych komend i interfejsów do tworzenia ról, przypisywania autoryzacji do ról oraz przypisywania ról do użytkowników.

Implementacja umożliwia częściowe podzielenie administrowania systemem, jednak działa ono z następującymi ograniczeniami:

1. Środowisko wymaga zmian komend i aplikacji na obsługujące kontrolę RBAC.
2. Predefiniowane autoryzacje nie są szczegółowe, a mechanizmy do tworzenia autoryzacji nie są odporne.
3. Często do uruchomienia komendy jest wymagane członkostwo w konkretnej grupie oraz rola z daną autoryzacją.
4. Rozdzielenie obowiązków jest trudne do zaimplementowania. Jeśli użytkownik ma przypisanych wiele ról, nie ma możliwości działania w pojedynczej roli. Użytkownik zawsze ma wszystkie autoryzacje dla wszystkich swoich ról.
5. W systemie operacyjnym nie przyjęto zasady najmniejszych uprawnień. Komendy zazwyczaj muszą mieć ustawiony bit SUID do użytkownika root.

Wcześniejszy tryb RBAC jest obsługiwany z uwagi na kompatybilność, jednak domyślnym trybem RBAC jest tryb rozszerzony. Rozszerzony tryb RBAC jest preferowany w systemie AIX.

Rozszerzony tryb RBAC

Z systemem AIX 6.1 jest dostarczana bardziej rozbudowana implementacja RBAC. Aplikacje wymagające uprawnień administratora do niektórych operacji mają nowe opcje integracji z rozszerzoną infrastrukturą RBAC w systemie AIX.

Opcje te koncentrują się na użyciu granulacji uprawnień i autoryzacji oraz możliwości skonfigurowania każdej komendy w systemie jako komendy uprzywilejowanej. Opcje rozszerzonego trybu RBAC są domyślnie instalowane i włączane we wszystkich instalacjach systemu AIX począwszy od systemu AIX 6.1.

Rozszerzony tryb RBAC udostępnia konfigurowalny zestaw autoryzacji, ról, uprzywilejowanych komend, urządzeń i plików w wymienionych poniżej bazach danych RBAC. Bazy danych rozszerzonej kontroli RBAC mogą znajdować się w lokalnym systemie plików lub mogą być zarządzane zdalnie za pomocą LDAP.

- Baza danych autoryzacji
- Baza danych ról
- Baza danych komend uprzywilejowanych
- Baza danych urządzeń uprzywilejowanych
- Baza danych plików uprzywilejowanych

Rozszerzony tryb RBAC wprowadza nową konwencję nazewnictwa dla autoryzacji, umożliwiającą tworzenie hierarchii autoryzacji. W systemie AIX jest udostępniony szczegółowy zestaw autoryzacji definiowanych przez system, a administrator może utworzyć w razie konieczności dodatkowe autoryzacje definiowane przez użytkownika.

Zachowanie ról zostało rozbudowane, aby zapewnić rozdzielenie funkcjonalności obowiązków. Rozszerzona kontrola RBAC wprowadza pojęcie sesji roli. Sesja roli to proces z jedną lub kilkoma powiązanymi rolami. Użytkownik może utworzyć sesję roli dla dowolnej roli, którą ma przypisaną, aktywując jedną lub kilka wybranych ról jednocześnie. Domyślnie nowy proces w systemie nie ma żadnych przypisanych ról. Role zostały rozbudowane o obsługę wymagania dotyczącego uwierzytelnienia użytkownika przed aktywacją roli. Umożliwia to ochronę na wypadek przejęcia sesji użytkownika przez atakującego, który musi się uwierzytelnić, zanim aktywuje role użytkownika.

Wprowadzenie bazy danych komend uprzywilejowanych jest implementacją zasady najmniejszych uprawnień. Zwiększono granulację uprawnień w systemie, komendom można nadawać uprawnienia jawne, a wykonanie komendy może być określane przez autoryzację. Zapewnia to funkcjonalność wymuszenia sprawdzenia uprawnienia do wykonania komendy bez zmiany kodu samej komendy. Użycie bazy danych komend uprzywilejowanych eliminuje potrzebę aplikacji SUID i SGID, ponieważ można przypisać tylko wymagane uprawnienia.

Baza danych urządzeń uprzywilejowanych umożliwia dostęp do urządzeń określany uprawnieniami, a baza danych plików uprzywilejowanych umożliwia użytkownikom bez uprawnień dostęp do plików o ograniczonym dostępie w oparciu o autoryzacje. Wszystkie te bazy danych zwiększają granulację zadań administracji systemem, które można przypisać do użytkowników nieuprawnionych do innych czynności administracyjnych.

Informacje znajdujące się w bazie danych RBAC są gromadzone i sprawdzane, a następnie wysyłane do obszaru jądra w postaci tabel bezpieczeństwa jądra (Kernel Security Tables - KST). Należy pamiętać, że stan danych w tabelach KST wyznacza strategię bezpieczeństwa w systemie. Pozycje zmieniane w bazach danych RBAC na poziomie użytkownika nie są wykorzystywane w decyzjach związanych z bezpieczeństwem, dopóki informacje te nie zostaną wysłane do tabel KST komendą **setkst**.

Konfigurowanie trybu RBAC
Tryb RBAC podlega kontroli zmiennej konfiguracyjnej o zasięgu całego systemu znajdującej się w jądrze. Zmienna ta określa, czy rozszerzony tryb RBAC jest włączony, czy wyłączony.

Rozszerzony tryb RBAC jest domyślnie włączony w systemie AIX 6.1 i w nowszych jego wersjach. Aby wyłączyć rozszerzony tryb RBAC i przywrócić wcześniejszy tryb RBAC, można uruchomić komendę **chdev** na urządzeniu **sys0** i podać wartość **false** atrybutu **enhanced_RBAC**. Aby zmiana atrybutu **enhanced_RBAC** odniosła skutek, należy zrestartować system. Aby włączyć rozszerzony tryb RBAC, należy nadać atrybutowi **enhanced_RBAC** wartość **true**. Z poziomu programistycznego można również ustawić lub sprawdzić tryb korzystając z wywołania systemowego **sys_parm()**.

Uruchom w systemie następującą komendę, aby pobrać bieżący tryb RBAC:

```
lsattr -E -l sys0 -a enhanced_RBAC
```

Aby wyłączyć rozszerzony tryb RBAC, uruchom następującą komendę i zrestartuj system:

```
chdev -l sys0 -a enhanced_RBAC=false
```

W środowisku partycji WPAR tryb RBAC można konfigurować tylko z systemu globalnego i będzie on jednakowo dotyczył zarówno tego systemu, jak i wszystkich partycji WPAR w systemie.

Porównanie wcześniejszego trybu RBAC z trybem rozszerzonym
Zarówno istniejące, jak i nowe interfejsy zmieniono, aby sprawdzały konfigurację systemu i uruchamiały nowy kod lub postępowały jak dotąd.

We wcześniejszym trybie RBAC wymuszane są tylko autoryzacje sprawdzane w kodzie samej komendy. Tabele bezpieczeństwa jądra (KST) nie mają wpływu na wykonanie komendy ani sprawdzenie autoryzacji. Określenie, czy użytkownik ma autoryzację, następuje zgodnie z zachowaniem we wcześniejszym trybie RBAC, polegającym na pobraniu autoryzacji wszystkich użytkowników i odszukaniu pasującej. We wcześniejszym trybie RBAC są niedostępne nowe opcje, takie jak komenda **swrole** czy atrybuty **default_roles** i **auth_mode**. Są w nim jednak obsługiwane nowe autoryzacje, uprawnienia i komendy do zarządzania autoryzacjami.

W poniższej tabeli zebrano niektóre różnice między trybami RBAC wcześniejszym i rozszerzonym.

Tabela 9. Różnice między trybami RBAC wcześniejszym i rozszerzonym

Opcja	Wcześniejszy tryb RBAC	Rozszerzony tryb RBAC
Aktywowanie roli.	Wszystkie role użytkowników są zawsze aktywne.	Domyślnie role są nieaktywne do momentu ich bezpośredniego przyjęcia komendą **swrole**.

Tabela 9. Różnice między trybami RBAC wcześniejszym i rozszerzonym (kontynuacja)		
Opcja	**Wcześniejszy tryb RBAC**	**Rozszerzony tryb RBAC**
Atrybut **default_roles**.	Niedostępne	Obsługiwane
Komenda **swrole**.	Niedostępne	Obsługiwane
Komendy do zarządzania rolami.	Obsługiwane	Obsługiwane
Komendy do zarządzania autoryzacjami.	Obsługiwane	Obsługiwane
Hierarchia autoryzacji.	Każda autoryzacja jest niezależna. Nie ma funkcjonalności hierarchii.	Obsługuje pojęcie hierarchii autoryzacji, w której jedne autoryzacje mogą być nadrzędne wobec innych.
Sprawdzanie autoryzacji.	Wymuszane tylko jeśli sama komenda sprawdzi autoryzację.	Wymuszane przez bazę danych komend uprzywilejowanych i/lub samą komendę.
Granulacja uprawnień.	Obsługiwane	Obsługiwane
Komenda **pvi**.	Niedostępne	Obsługiwane
Tabele bezpieczeństwa jądra.	Niedostępne	Obsługiwane
Położenie bazy danych RBAC.	Pliki lokalne.	Pliki lokalne lub LDAP.

Korzystanie z rozszerzonego trybu RBAC
Aby efektywnie korzystać z rozszerzonego trybu RBAC, administratorzy systemów powinni zapoznać się z poniżej wymienionymi zagadnieniami.

Autoryzacje RBAC
Autoryzacje są istotną częścią kontroli dostępu na podstawie ról (RBAC). System operacyjny używa łańcuchów autoryzacji do określenia uprawnień przed wykonaniem operacji uprzywilejowanej. Związane z tym operacje sprawdzenia mogą być wykonane bezpośrednio z kodu lub przez program ładujący w momencie uruchamiania chronionych uprzywilejowanych programów wykonywalnych.

Nazewnictwo łańcuchów autoryzacji wskazuje operację uprzywilejowaną, którą reprezentują i nadzorują. Konwencja nazewnictwa w systemie AIX dla autoryzacji obsługuje hierarchiczną strukturę wskazywaną przez nazwę tekstową autoryzacji. Łańcuchy autoryzacji w systemie AIX używają formatu notacji kropkowej do opisania hierarchii autoryzacji. Na przykład autoryzacja do tworzenia nowych systemów plików jest następująca: **aix.fs.manage.create**. Jeśli autoryzacja ta jest zawarta w roli, a rola przypisana do użytkownika, może on tworzyć systemy plików w systemie AIX. Jeśli w roli jest zawarta autoryzacja nadrzędna, **aix.fs.manage**, użytkownik mający przypisaną tę rolę może oprócz tworzenia systemów plików wykonywać inne zadania związane z zarządzaniem systemem plików.

Kontrola RBAC w systemie AIX wprowadza rozróżnienie między autoryzacjami udostępnionymi przez system (autoryzacjami zdefiniowanymi przez system), a autoryzacjami utworzonymi po instalacji (autoryzacje zdefiniowane przez użytkownika).

Autoryzacje zdefiniowane przez system
System AIX udostępnia predefiniowany i niezmienialny zestaw autoryzacji. Autoryzacje te nazywa się autoryzacjami zdefiniowanymi przez system. Są one powiązane z różnymi uprzywilejowanymi operacjami systemu AIX, a powiązanie to jest określone w bazie danych komend uprzywilejowanych.

Na szczycie hierarchii autoryzacji zdefiniowanych przez system znajduje się autoryzacja **aix**. Jest ona nadrzędna wobec wszystkich pozostałych autoryzacji zdefiniowanych przez system. Nadanie tej autoryzacji do roli nadaje tej roli wszystkie autoryzacje zdefiniowane przez system. Aby wyświetlić pełen

zestaw autoryzacji zdefiniowanych przez system w systemie AIX wraz z krótkim opisem każdej z nich, uruchom następującą komendę:

```
lsauth –f –a description ALL_SYS
```

Dane wyjściowe powyższej komendy pokazują, że lista autoryzacji zdefiniowanych przez system jest hierarchią wielopoziomową. Na przykład autoryzacja **aix** ma kilku bezpośrednich potomków. Każdy z nich jest następnie nadrzędny wobec innej hierarchii. Autoryzacja **aix.fs** obejmuje wiele autoryzacji potomnych, w tym autoryzację **aix.fs.manage**, która również obejmuje wiele autoryzacji, na przykład **aix.fs.manage.change** i **aix.fs.manage.create**.

Autoryzacje zdefiniowane przez użytkownika
Oprócz autoryzacji zdefiniowanych przez system, kontrola RBAC systemu AIX umożliwia administratorom systemu definiowanie w bazie danych (/etc/security/authorizations) własnych niestandardowych autoryzacji. Autoryzacje te nazywa się autoryzacjami zdefiniowanymi przez użytkownika.

Administrator systemu może dodawać, modyfikować i usuwać autoryzacje zdefiniowane przez użytkownika. Na przykład administrator systemu może umożliwić pewnym użytkownikom uruchamianie komend uprzywilejowanych; w tym celu tworzy autoryzację zdefiniowaną przez użytkownika, łączy ją z komendą i dodaje do roli, która jest przypisana do tych użytkowników.

Autoryzacje zdefiniowane przez użytkownika bazują na tym samym pojęciu hierarchii, co autoryzacje zdefiniowane przez system. Jednak w nazewnictwie autoryzacji zdefiniowanych przez użytkownika w systemie AIX należy uwzględnić kilka ograniczeń.

- Autoryzacje zdefiniowane przez użytkownika muszą być zdefiniowane poniżej nowego nadrzędnego najwyższego poziomu. Oznacza to, że autoryzacje zdefiniowane przez użytkownika nie mogą być potomkami autoryzacji zdefiniowanych przez system (**aix**).
- Nazwa autoryzacji może zawierać maksymalnie 63 widoczne znaki.
- Hierarchia nadrzędna autoryzacji może zawierać maksymalnie osiem poziomów.
- Autoryzacja może mieć dowolną liczbę bezpośrednich potomków, ale tylko jedną bezpośrednią autoryzację nadrzędną. Dwie niezależne autoryzacje nie mogą mieć tego samego bezpośredniego potomka.

Z uwagi na to, że hierarchia nie zezwala na wiele bezpośrednich autoryzacji nadrzędnych danego elementu, nie można zdefiniować autoryzacji definiowanej przez użytkownika, która byłaby nadrzędna dla istniejącej autoryzacji zdefiniowanej przez system. Dlatego próba utworzenia autoryzacji o nazwie **aix.custom** nie powiedzie się, a utworzenie autoryzacji o nazwie **custom.aix** spowoduje utworzenie nowej gałęzi autoryzacji, która nie będzie działała, jak autoryzacja nadrzędna wobec zdefiniowanej przez system autoryzacji **aix**.

Aby uniknąć konfliktów między nazwami autoryzacji w wielu komponentach oprogramowania, sugerowane jest używanie następującej składni przy tworzeniu autoryzacji zdefiniowanych przez użytkownika:

nazwa_dostawcy.*nazwa_produktu*.*funkcja*.*funkcja1*.*funkcja2*...

nazwa_dostawcy
Identyfikuje nazwę dostawcy modułu oprogramowania.

nazwa_produktu
Nazwa najwyższego poziomu produktu zarządzanego z kontrolą RBAC.

***funkcja*, *funkcja1*, *funkcja2* ...**
Łańcuchy reprezentują funkcje, które są zarządzane przez kontrolę RBAC. Łańcuchy te stanowią również hierarchiczną reprezentację zorganizowania tych funkcji.

Na przykład **ibm.db2.manage** może potencjalnie reprezentować aspekty zarządzania pakietem bazy danych IBM DB2. Jak wspomniano wcześniej, łańcuch **aix** jako *nazwa_dostawcy* jest zarezerwowany do użytku przez system AIX i jest niedozwolony dla autoryzacji zdefiniowanych przez użytkownika.

Istnieje kilka komend, których administrator systemu może użyć do zarządzania autoryzacjami zdefiniowanymi przez użytkownika, ich wyświetlenia, utworzenia, modyfikowania i usuwania. Autoryzacje

zdefiniowane przez użytkownika można utworzyć przy użyciu komendy **mkauth**, zmodyfikować przy użyciu komendy **chauth**, usunąć przy użyciu komendy **rmauth** i wyświetlić przy użyciu komendy **lsauth**. Aby wyświetlić wszystkie autoryzacje systemowe zdefiniowane przez użytkownika wraz z krótkim opisem każdej z nich, uruchom następującą komendę:

```
lsauth –f –a description ALL_USR
```

Przed utworzeniem autoryzacji zdefiniowanych przez użytkownika należy rozważyć następujące zagadnienia:

- Czy nie lepiej użyć istniejącej autoryzacji zdefiniowanej przez system, zamiast tworzyć nową autoryzację zdefiniowaną przez użytkownika?
- Czy nowa autoryzacja znajduje się poniżej istniejącej hierarchii autoryzacji zdefiniowanej przez użytkownika czy jest pierwszą autoryzacją nowej hierarchii?
- Jeśli jest to nowa hierarchia, jaka jest jej struktura?
- Jaki jest opis tekstowy tej autoryzacji?
- Czy wymagane jest tłumaczenie opisu autoryzacji na inne języki?
- Czy jest jakiś powód, aby określić konkretny identyfikator autoryzacji podczas jej tworzenia? Zaleca się, aby do wygenerowania identyfikatora autoryzacji użyć komendy **mkauth**.

Po rozważeniu powyższych zagadnień, wykonaj następujące czynności, aby utworzyć autoryzację:

1. Jeśli wymagane jest tłumaczenie na inne języki, utwórz lub dodaj opis do katalogu komunikatów.
2. Użyj komendy **mkauth** do utworzenia wszystkich autoryzacji nadrzędnych w hierarchii, jeśli jeszcze nie istnieją.
3. Użyj komendy **mkauth** do utworzenia żądanej autoryzacji. Podaj w komendzie atrybut **id**, jeśli wymagana jest konkretna wartość.

Migracja wcześniejszych autoryzacji
Systemy operacyjne wcześniejsze niż AIX wersja 6.1 miały ograniczony, predefiniowany zestaw autoryzacji rozpoznawanych przez system operacyjny. Autoryzacje te nie zostały zdefiniowane w żadnym pliku w systemie, ale można było je szybko przypisać do ról. Aby wcześniejsze autoryzacje były obsługiwane w nowym środowisku RBAC w systemie AIX wersja 6.1 lub nowszym, zostały zdefiniowane jako autoryzacje zdefiniowane przez użytkownika i są udostępniane domyślnie w bazie danych autoryzacji.

Odkąd w systemie operacyjnym AIX zaczęto stosować nową konwencję nazewnictwa autoryzacji, wszystkie operacje sprawdzenia starych nazw autoryzacji w systemie operacyjnym AIX zostały zmienione i teraz dodatkowo sprawdzają odpowiednią nową autoryzację i zezwalają na dostęp, jeśli dla procesu istnieje jakaś autoryzacja. W poniższej tabeli znajdują się wcześniej predefiniowane autoryzacje i odpowiadające im nowe autoryzacje zdefiniowane przez system.

Istniejąca autoryzacja w systemie AIX	Odpowiadająca jej nowa autoryzacja
Backup (kopia zapasowa)	aix.fs.manage.backup
Diagnostics (diagnostyka)	aix.system.config.diag
DiskQuotaAdmin (administrator limitu pamięci dyskowej)	aix.fs.manage.quota
GroupAdmin (administrator grup)	aix.security.group
ListAuditClasses (lista klas kontroli)	aix.security.audit.list
PasswdAdmin (administrator haseł)	aix.security.passwd
PasswdManage (zarządzanie hasłami)	aix.security.passwd.normal
UserAdmin (administrator użytkowników)	aix.security.user
UserAudit (kontrola użytkowników)	aix.security.user.change
RoleAdmin (administrator ról)	aix.security.role

Istniejąca autoryzacja w systemie AIX	Odpowiadająca jej nowa autoryzacja
Restore (odtwarzanie)	aix.fs.manage.restore

Role RBAC
Role są mechanizmem służącym do przypisywania autoryzacji do użytkownika oraz do grupowania razem zestawu zadań do administrowania systemem. Rola w systemie AIX jest przede wszystkim kontenerem na kolekcję autoryzacji.

System AIX obsługuje bezpośrednie przypisanie autoryzacji do ról i pośrednie przypisanie autoryzacji przez rolę podrzędną. Rolę podrzędną dla roli można podać w jej atrybucie **rolelist**. Skonfigurowanie dla roli wyznaczonych ról podrzędnych w rzeczywistości przypisuje do niej wszystkie autoryzacje zawarte w roli podrzędnej.

Przypisanie roli do użytkownika umożliwia mu dostęp do roli i użycie autoryzacji w niej zawartych. Administrator systemu może przypisać rolę do wielu użytkowników i wiele ról do jednego użytkownika. Użytkownik z przypisanymi wieloma rolami może, jeśli jest to potrzebne do wykonania funkcji związanych z zarządzaniem systemem, aktywować równocześnie więcej niż jedną rolę (maksymalnie do ośmiu ról).

System AIX udostępnia zestaw predefiniowanych ról do zarządzania systemem. Zakłada się jednak, że klient będzie tworzył własne role niestandardowe lub zmieniał istniejące predefiniowane role. Do wyświetlania, tworzenia, zmiany i usuwania ról w systemie AIX udostępniono komendy do zarządzania rolami. Role można utworzyć przy użyciu komendy **mkrole**, modyfikować przy użyciu komendy **chrole**, usuwać przy użyciu komendy **rmrole** i wyświetlać przy użyciu komendy **lsrole**.

Podczas tworzenia nowej roli w systemie AIX należy rozważyć następujące zagadnienia:

- Jaka będzie nazwa tej roli?
- Nazwa roli jest łańcuchem tekstowym, ale powinna dawać wyobrażenie o możliwościach roli. Nazwy ról mogą zawierać maksymalnie 63 widoczne znaki.
- Jakie autoryzacje są wymagane dla tej roli? Należy zastanowić się, czy autoryzacje powinny być przypisywane bezpośrednio do roli, czy przypisywane pośrednio - z użyciem ról podrzędnych.
- Czy użytkownik powinien się uwierzytelnić podczas aktywowania roli?

Aktywowanie roli
Domyślnie, w systemie AIX wersja 6.1 lub nowszym z rozszerzoną kontrolą RBAC, po uwierzytelnieniu się użytkownika w systemie do sesji użytkownika nie są przypisane żadne role ani autoryzacje. Aby powiązać role z sesją, użytkownik musi wywołać osobną komendę uwierzytelniania (jest to komenda **swrole**), przełączając się na rolę lub role.

Użytkownik może aktywować tylko role, które zostały wcześniej do niego przypisane. Domyślnie użytkownik powinien uwierzytelnić się swoją nazwą użytkownika podczas rozpoczynania sesji roli lub podczas dodawania roli do swojej sesji. Można tak skonfigurować role, aby nie wymagały uwierzytelniania: do tego celu służy atrybut roli **auth_mode**.

Podczas przełączania sesji do nowej roli zostaje utworzona nowa powłoka (sesja), która nie zawiera ról z poprzedniej sesji. Realizowane jest to przez utworzenie nowej powłoki procesu dla roli i przypisanie nowego identyfikatora roli (RID) do procesu. Tworzenie nowej sesji przypomina korzystanie z komendy **su**, jednak w tym przypadku jest zmieniany tylko identyfikator roli procesu, a nie takie parametry, jak identyfikatory UID i GID. Komenda **swrole** umożliwia użytkownikowi tworzenie sesji roli złożonej z jednej lub wielu ról. Nie istnieją ograniczenia uniemożliwiające użytkownikowi przełączenie do nowej sesji roli z bieżącej sesji roli. Z uwagi na to, że nowa sesja jest nowym procesem, nie zawiera ona żadnych ról z wcześniejszej sesji. Aby odtworzyć wcześniejszą sesję, użytkownik musi zakończyć bieżącą sesję roli. Role przyjęte w sesji (zestaw aktywnych ról) można wyświetlić, uruchamiając w sesji komendę **rolelist**. Administrator może również użyć komendy **rolelist** w celu wyświetlenia zestawu aktywnych ról danego procesu systemowego.

Użytkownikowi można opcjonalnie przypisać domyślny zestaw ról za pomocą nowego atrybutu użytkownika **default_roles**. Atrybut ten powinien być używany w sytuacjach, gdy procesy tworzone w imieniu użytkownika zawsze muszą być powiązane z danym zestawem ról, przykładem jest komenda **cron**. Komenda cron działa w tle i uruchamia komendy w imieniu zdefiniowanego użytkownika. Niektóre z

uruchamianych komend mogą wymagać autoryzacji. To zaś wymaga możliwości określenia, że zestaw ról dla identyfikatora użytkownika będzie zawsze aktywny, ponieważ nie ma żadnego mechanizmu umożliwiającego komendzie **cron** późniejsze ich uzyskanie. Atrybut **default_roles** może zawierać do ośmiu nazw ról lub wartość specjalną **ALL**. Ustawienie wartości **default_roles=ALL** przypisuje wszystkie role użytkownika do tej sesji. Jeśli do użytkownika przypisano więcej niż osiem ról, dla sesji będzie włączonych tylko osiem pierwszych.

Maksymalna liczba ról na jedną sesję
W rozszerzonym trybie RBAC administrator systemu może skonfigurować dla całego systemu maksymalną liczbę ról, które użytkownik może aktywować w danej sesji roli. Domyślnie użytkownik może aktywować maksymalnie osiem ról w sesji.

Różne środowiska mogą wymagać większego rozdzielenia obowiązków, w nich użytkownik może jednocześnie aktywować tylko jedną rolę. W takich środowiskach atrybut **maxroles** sekcji **usw** w pliku `/etc/security/login.cfg` można zmienić, ograniczając maksymalną dopuszczalną liczbę ról na jedną sesję. Atrybut **maxroles** może mieć wartość z zakresu od 1 do 8 i określa maksymalną dopuszczalną liczbę ról na jedną sesję.

Aby wyświetlić bieżącą wartość ograniczenia dotyczącego liczby ról na jedną sesję, uruchom następującą komendę:

```
lssec –f /etc/security/login.cfg –s usw –a maxroles
```

Aby system pozwalał użytkownikowi na jednoczesne aktywowanie tylko jednej roli, uruchom następującą komendę:

```
chsec –f /etc/security/login.cfg –s usw –a maxroles=1
```

Zmiana wartości atrybutu **maxroles** odnosi skutek natychmiast i dotyczy wszystkich nowo tworzonych sesji ról, nie wymaga restartu systemu. Zmiana nie dotyczy sesji ról istniejących przed zmianą wartości tego atrybutu. Wymuszenie maksymalnej liczby ról na jedną sesję następuje w momencie inicjacji sesji.

Predefiniowane role
Predefiniowany zestaw ról w nowej instalacji systemu AIX wersja 6.1 lub nowszego jest zdefiniowany w lokalnej bazie danych ról (`/etc/security/roles`). Ten zestaw ról ma na celu zgrupowanie typowych zakresów odpowiedzialności związanych z administrowaniem.

Ten zestaw ról to sugerowana metoda podzielenia obowiązków administracyjnych. Administratorzy ról w danym środowisku mogą zmieniać lub usuwać te role, a także w razie potrzeby tworzyć nowe. Poniżej znajduje się lista udostępnianych ról oraz krótki opis możliwości każdej z nich.

Nazwa roli	Opis roli
auditadm	Administrator kontroli. Rola auditadm ponosi odpowiedzialność za skonfigurowanie kontroli i rejestrowanie strategii systemu, w tym atrybutów całego systemu, pojedynczego użytkownika i pojedynczej roli. Ta rola ma dostęp do przeglądania zapisu kontrolnego.
fsadm	Administrator systemu plików. Rola fsadm umożliwia tworzenie systemów plików i udostępnianie ich użytkownikom systemu. Poniżej przedstawiono niektóre z obszarów, za które rola fsadm ponosi odpowiedzialność: • określanie strategii podłączania, • współużytkowanie strategii, • przypisywanie limitów, • określanie poziomu kompresji, • ustanawianie formatów systemów plików, • tworzenie i odtwarzanie kopii zapasowych.

Nazwa roli	Opis roli
isso	Osoba odpowiedzialna za bezpieczeństwo systemu informacyjnego. Osoba taka jest odpowiedzialna za tworzenie i przypisywanie ról, dlatego jest to rola o największych możliwościach w systemie. Zakres obowiązków takiej osoby obejmuje między innymi: • Ustanawianie strategii bezpieczeństwa i zarządzanie nią • Ustawianie haseł użytkowników • Konfiguracja sieci • Administrowanie urządzeniami
pkgadm	Administrator pakietu oprogramowania. Rola pkgadm ponosi odpowiedzialność za oprogramowanie zainstalowane w systemie i ma domyślne uprawnienia do instalowania, aktualizowania i usuwania oprogramowania systemowego.
sa	Administrator systemu. Rola ta udostępnia funkcjonalność niezbędną przy codziennym administrowaniu, a osoba pełniąca tę rolę jest odpowiedzialna za: • Administrowanie użytkownikami (bez ustawiania haseł) • Administrowanie systemem plików • Aktualizację instalacji oprogramowania • Zarządzanie demonem sieciowym • Alokację urządzeń
secadm	Administrator ochrony. Rola secadm odpowiada za konserwację ustawień ochrony w systemie. Rola secadm umożliwia przypisywanie użytkownikom atrybutów, takich jak członkostwo w grupach, autoryzacje i zezwolenia, i przypisywanie ról, które nie są jeszcze określone za pomocą ich ról. Ponadto rola secadm umożliwia przypisywanie atrybutów ochrony do obiektów systemowych, w tym ustawień RBAC, list kontroli dostępu, praw własności i członkostwa. Poniżej podano niektóre z obszarów, za które rola secadm ponosi odpowiedzialność: • przypisywanie haseł dla nowych kont użytkowników, • odblokowywanie zablokowanych kont.
so	Operator systemu. Rola ta udostępnia funkcjonalność codziennych zadań, a zakres obowiązków osoby pełniącej tę rolę obejmuje: • Zamykanie systemu i jego restartowanie • Tworzenie kopii zapasowych systemu plików, ich odtwarzanie i limity • Rejestrowanie błędów, śledzenie i statystyki • Administrowanie obciążeniem
svcadm	Administrator usług. Rola svcadm umożliwia aktywowanie, konfigurowanie i wyłączanie usług systemowych. Ta rola umożliwia konfigurowanie atrybutów sieciowych, takich jak adresy IP, trasy, nazwy hostów i strategie firewalli.
sysop	Operator systemu. Rola sysop odpowiada za konserwację całego systemu. Ma ona uprawnienia umożliwiające uruchamianie diagnostyki systemu i wykonywanie rutynowej konserwacji systemu. Poniżej przedstawiono niektóre zadania, za które rola sysop ponosi odpowiedzialność: • usuwanie plików dzienników i kolejek wydruków, • zatrzymywanie i restartowanie systemów.
useradm	Administrator użytkowników. Rola useradm ponosi odpowiedzialność za czynności na wyższym poziomie dotyczące konserwacji użytkowników bez zarządzania hasłami. Rola useradm umożliwia tworzenie, modyfikowanie i usuwanie kont użytkowników zgodnie ze

Nazwa roli	Opis roli
	zdefiniowanymi ustawieniami zabezpieczeń. Ponadto ta rola umożliwia tworzenie dodatkowych ról i grup z domyślnymi ustawieniami zabezpieczeń.

Migracja ról
Jeśli system AIX wcześniejszy niż AIX wersja 6.1 jest aktualizowany za pomocą instalacji migracyjnej do poziomu rozszerzonego trybu RBAC systemu AIX, podczas migracji pliku `/etc/security/roles` podejmowana jest próba aktualizacji pliku do nowej funkcjonalności z zachowaniem istniejących możliwości ról.

Definicje ról w pliku są zachowywane i w prosty sposób modyfikowane, tak aby zawierały unikalny identyfikator roli, umożliwiający roli poprawne działanie w nowym środowisku. Zakłada się, że wszystkie autoryzacje w pliku `/etc/security/roles`, niebędące autoryzacjami predefiniowanymi są autoryzacjami zdefiniowanymi przez użytkownika. Podczas migracji te nazwy autoryzacji są dodawane jako pozycje w lokalnej bazie danych autoryzacji `/etc/security/authorizations`. Oprócz migracji definicji dotychczasowych ról do pliku są dodawane nowe predefiniowane role. Po migracji administrator systemu musi sprawdzić, czy autoryzacje i role zostały zdefiniowane zgodnie z potrzebami danego środowiska.

Uprawnienia RBAC
Środowisko rozszerzonego trybu RBAC bardzo mocno polega na uprawnieniach systemowych przy zezwalaniu użytkownikom bez uprawnień na wykonywanie zadań uprzywilejowanych. Uprawnienie jest mechanizmem używanym do nadania procesowi zwiększonej funkcjonalności w wywołaniach systemowych.

Pojęcie uprawnień wywodzi się z konstrukcji na poziomie jądra, ponieważ definiowanie oraz większość operacji sprawdzania następuje w jądrze. Zostały jednak udostępnione interfejsy na poziomie użytkownika, służące do obsługi przypisania uprawnień do komend, urządzeń i procesów.

Ważne jest rozgraniczenie między uprawnieniami a autoryzacjami. Zarówno uprawnienia, jak i autoryzacje, służą do kontroli określonych dopuszczalnych wyjątków w strategii bezpieczeństwa systemu. Różnią się przede wszystkim tym, że uprawnienia są powiązane z konkretnymi procesami, a autoryzacje są wiązane z użytkownikami przy pomocy ról. Autoryzacje należą do roli i użytkownika mającego tę rolę, a nie zależą od uruchamianego programu. Uprawnienia istnieją z programem i zapewniają mechanizm precyzyjnego dostrojenia strategii bezpieczeństwa systemu. Dzięki tym przypisanym uprawnieniom proces może wykonać odpowiednie operacje uprzywilejowane.

Uprawnienia są definiowane w jądrze systemu AIX jako poszczególne bity maski bitowej, która wymusza kontrolę dostępu do operacji uprzywilejowanych. Z systemem AIX dostarczanych jest ponad 100 uprawnień, umożliwiających precyzyjną i szczegółową kontrolę operacji uprzywilejowanych. Podczas określania dostępu w wywołaniu systemowym jądro określa, czy proces ma wymagany powiązany bit uprawnienia i następnie zezwala na żądanie lub je odrzuca.

Uprawnienia są przypisywane do wywołań komendy w bazie danych komend uprzywilejowanych, a uprawnienia używane przy kontroli dostępu do urządzeń znajdują się w bazie danych urządzeń uprzywilejowanych.

Nazewnictwo i hierarchia uprawnień
Uprawnienia w systemie AIX nie mogą być tworzone, modyfikowane ani usuwane przez administratora systemu.

Listę dostępnych uprawnień wraz z krótkim opisem można w systemie wyświetlić przy użyciu komendy:

```
lspriv -v
```

Uprawnienia udostępnione w systemie AIX są wymienione w sekcji Uprawnienia w systemie AIX. Wszystkie uprawnienia w systemie AIX mają tekstową reprezentację bitu uprawnienia rozpoczynającą się od łańcucha **PV_**. Konwencja nazewnictwa użyta po przedrostku **PV_** oznacza relację hierarchiczną między uprawnieniami. Na przykład uprawnienie kontroli **PV_AU_** jest nadrzędne dla uprawnień **PV_AU_ADD**, **PV_AU_ADMIN**, **PV_AU_READ**, **PV_AU_WRITE** i **PV_AU_PROC**. Podczas sprawdzania uprawnień system

wpierw określa, czy proces ma najniższe potrzebne uprawnienia, a następnie podąża w górę hierarchii, sprawdzając, czy istnieją większe uprawnienia. Uprawnienie **PV_ROOT** jest uprawnieniem specjalnym, nadrzędnym dla wszystkich uprawnień oprócz **PV_SU_**. Proces z przypisanym uprawnieniem **PV_ROOT** zachowuje się tak, jakby miał wszystkie uprawnienia istniejące w systemie oprócz uprawnienia **PV_SU_**.

Zestawy uprawnień procesu
W jądrze zdefiniowano wiele zestawów uprawnień, aby zapewnić operacjom uprzywilejowanym różne kombinacje elementów sterujących. Wiele zestawów uprawnień umożliwia systemowi operacyjnemu wymuszenie dynamicznego sterowania uprawnieniami i umożliwia aplikacjom kierowanie się zasadami najmniejszych uprawnień.

Uprawnienia są powiązane z procesem przez następujące zestawy uprawnień:

Ograniczający zestaw uprawnień (Limiting Privilege Set - LPS)
Definiuje twardy limit uprawnień dla danego procesu. Żadna eskalacja uprawnień w systemie nie podniesie uprawnień procesu powyżej tej wartości. Oznacza to, że proces nie może uzyskać więcej uprawnień, używając zdefiniowanych interfejsów systemu, niż wynosi ta wartość. Innymi słowy, proces jest w każdym momencie ograniczony do tych uprawnień. Oznacza to również, że reszta zestawów uprawnień będzie zawsze podzbiorem tego zestawu LPS. Zestaw LPS nie może zostać rozbudowany, ale każdy proces ma prawo go zmniejszyć. Jednak po zmniejszeniu nie można przywrócić jego początkowej wartości. Zmniejszenie zestawu LPS umożliwia procesowi narzucenie granic w związanych z nim uprawnieniach. Na przykład proces może zmniejszyć zestaw LPS przed uruchomieniem niestandardowego programu dostarczonego przez użytkownika. Domyślnie w zestawie LPS dla procesu są ustawiane wszystkie uprawnienia dostępne w systemie.

Maksymalny zestaw uprawnień (Maximum Privilege Set - MPS)
Pełen zestaw uprawnień, do używania których jest autoryzowany proces. Zestaw MPS może zawierać wszystkie uprawnienia istniejące w zestawie LPS, ale nie może mieć ich więcej. Zestaw MPS z różnych powodów może się zmieniać w czasie życia procesu. Przyczyny tych zmian mogą być następujące:

- Gdy bieżący proces wykonuje inną komendę uprzywilejowaną, a następnie uzyskuje pokrewne uprawnienia dodatkowe.
- Jeśli proces ma odpowiednie uprawnienie, może dynamicznie rozszerzyć zestaw MPS na poziomie programowym.

Obowiązujący zestaw uprawnień (Effective Privilege Set - EPS)
Lista bieżących aktywnych uprawnień procesu. Zestaw EPS jest zawsze podzbiorem zestawu MPS procesu i jest używany przez jądro do kontroli dostępu przy operacjach uprzywilejowanych. Zestaw EPS może być modyfikowany przez proces i może być równoważny zestawowi MPS, ale nie może go przekroczyć. Proces może przeprowadzić dynamiczne modyfikowanie zestawu EPS w celu wymuszenia zasady najmniejszych uprawnień. Na przykład kod w przestrzeni użytkownika może potencjalnie podnieść bit uprawnienia kontroli w zestawie EPS, korzystając z funkcji API **priv_raise** przed użyciem związanego z kontrolą wywołania systemowego lub jądra. Następnie po powrocie z wywołania kontroli można obniżyć uprawnienie funkcją API **priv_lower**.

Odziedziczony zestaw uprawnień (Inheritable Privilege Set - IPS)
Uprawnienia przekazane z procesu nadrzędnego do zestawów MPS i EPS procesu potomnego. Zestaw IPS może zawierać wszystkie uprawnienia istniejące w zestawie LPS, ale nie może mieć ich więcej. Zestaw IPS w procesie można ustawić następująco:

- Jeśli proces ma odpowiednie uprawnienia, może dynamicznie rozszerzyć zestaw IPS na poziomie programowym, korzystając z wywołania systemowego **setppriv**.
- Podczas uruchamiania komendy uprzywilejowanej uprawnienia podane w atrybucie **inheritprivs** powiązanym z komendą są przypisywane do zestawu IPS.

Użyty zestaw uprawnień (Used Privilege Set - UPS)
Oznacza uprawnienia, które były używane do sprawdzania dostępu w trakcie życia procesu. Zestawu UPS można użyć w celu określenia uprawnień wymaganych przez proces. Gdy jądro sprawdza, czy proces ma dane uprawnienie, zapisuje sprawdzenie zakończone pomyślnie w zestawie UPS dla uprawnienia.

Zestaw uprawnień partycji zarządzania obciążeniem (Workload Partition Privilege Set - WPS)
Systemową partycję WPAR można ograniczyć, aby nie zezwalać na wszystkie operacje uprzywilejowane dopuszczalne w globalnej partycji WPAR. Operacje uprzywilejowane dopuszczalne w systemowej partycji WPAR można kontrolować, korzystając z zestawu WPS. Globalny użytkownik root może przypisać ograniczony zestaw uprawnień do partycji WPAR, korzystając z zestawu WPS. Zestaw WPS można podać w pliku konfiguracyjnym `/etc/wpar/secattrs` lub podczas uruchamiania partycji WPAR komendą **/usr/sbin/startwpar**. Wszystkie procesy działające w partycji WPAR mają zestawy LPS identyczne jak zestawy WPS.

Administrator systemu może użyć komend administracyjnych do wyświetlenia i zmiany różnych zestawów uprawnień procesu. Komendą **lssecattr** można wyświetlić zestawy LPS, MPS, EPS, IPS i UPS. Komendą **setsecattr** można zmienić zestawy LPS, MPS, EPS i IPS. Zestawu UPS nie można zmienić komendą **setsecattr**, ponieważ zestaw UPS jest atrybutem tylko do odczytu.

Baza danych komend uprzywilejowanych
Autoryzacje, role i uprawnienia umożliwiają zaimplementowanie dokładniejszych mechanizmów zabezpieczeń. Jednak eksploatacja kontroli RBAC w różnych operacjach systemowych umożliwia wymuszenie strategii bezpieczeństwa RBAC.

W przeszłości niektóre komendy systemu AIX same sprawdzały autoryzacje, a to wymagało odpowiedniej modyfikacji kodu wykonywalnego. Rozszerzony tryb RBAC zapewnia środowisko do wymuszania sprawdzenia autoryzacji i nadawania uprawnień na podstawie bazy danych komend uprzywilejowanych i nie trzeba w tym celu wprowadzać zmian w kodzie wykonywalnym systemu.

Baza danych komend uprzywilejowanych nadaje dostęp i odpowiednie uprawnienia użytkownikom do komend, których inaczej nie mogliby uruchomić lub do których nie mieliby odpowiednich uprawnień niezbędnych do wykonania zadania. W bazie danych są zapisane informacje o autoryzacji dla odpowiednich komend oraz uprawnienia nadawane procesowi, gdy sprawdzenie autoryzacji zakończy się pomyślnie. Jeśli baza danych jest przechowywana lokalnie, znajduje się w pliku `/etc/security/privcmds` i zawiera sekcje informacji w postaci komenda-atrybuty bezpieczeństwa. Poniżej znajduje się kilka kluczowych atrybutów z tej bazy danych (pełen opis wszystkich atrybutów zawiera plik `/etc/security/privcmds`).

accessauths (uprawnienia dostępu)
Lista autoryzacji dostępu zabezpieczających wykonanie komendy. Użytkownik z dowolną z wymienionych autoryzacji może uruchomić komendę i wykonać niektóre lub wszystkie operacje uprzywilejowane w niej zawarte.

innateprivs (uprawnienia wrodzone)
Uprawnienia wrodzone są przypisywane do procesu, jeśli użytkownik wywołujący pomyślnie przejdzie sprawdzanie autoryzacji dostępu.

authprivs (uprawnienia autoryzowane)
Uprawnienia autoryzowane są dodatkowymi uprawnieniami przypisanymi do procesu, jeśli użytkownik ma powiązaną autoryzację. Atrybut ten umożliwia bardziej szczegółową kontrolę komendy, umożliwiając ograniczonej liczbie użytkowników wykonywanie dodatkowych operacji uprzywilejowanych.

inheritprivs (uprawnienia dziedziczone)
Uprawnienia odziedziczone są przekazywane przez proces do procesów potomnych.

secflags (opcje bezpieczeństwa)
Lista opcji bezpieczeństwa. Opcja FSF_EPS powoduje w momencie uruchomienia komendy załadowanie maksymalnego zestawu uprawnień (MPS) do obowiązującego zestawu uprawnień (EPS).

Gdy użytkownik systemu z rozszerzonym trybem RBAC uruchamia komendę, jest ona najpierw sprawdzana w bazie danych komend uprzywilejowanych. Jeśli zostanie tam znaleziona, sprawdzane są autoryzacje powiązane z sesją użytkownika oraz wartość atrybutu **accessauths** komendy. Jeśli sesja ma jedną z wymienionych autoryzacji, użytkownik może uruchomić komendę, niezależnie od tego, czy pomyślnie przejdzie sprawdzanie wykonania DAC dla tej komendy. Po wywołaniu procesu komendy uprawnienia wymienione w atrybucie **innateprivs** zostają przeniesione do jego maksymalnego zestawu uprawnień (MPS). Dodatkowe sprawdzanie autoryzacji jest wykonywane z parami autoryzacja-uprawnienie wymienionymi w atrybucie **authprivs**. Jeśli sesja ma jedną z wymienionych autoryzacji, do

maksymalnego zestawu uprawnień procesu komendy są dodawane również powiązane uprawnienia. Pozycja komendy w bazie danych komend uprzywilejowanych, mająca wartość **FSF_EPS** ustawioną w atrybucie **secflags**, przypisuje wszystkie uprawnienia z maksymalnego zestawu uprawnień do obowiązującego zestawu uprawnień w momencie wywołania komendy.

Komenda staje się komendą uprzywilejowaną, jeśli zostanie umieszczona w bazie danych komend uprzywilejowanych. Wprawdzie programy z bitem setuid, które nie są wymienione w tej bazie danych, z technicznego punktu widzenia nadal są komendami uprzywilejowanymi, jednak podczas opisywania zachowania kontroli RBAC nie są one omawiane jako komendy uprzywilejowane. Jeśli komenda nie ma swojej pozycji w bazie danych komend uprzywilejowanych, nie jest komendą uprzywilejowaną, a dostęp do niej jest wymuszany przez DAC i samą komendę. Ponadto, jeśli komenda jest wymieniona w bazie danych komend uprzywilejowanych, ale sesja użytkownika nie ma autoryzacji pozwalającej ją wywołać, system powraca do sprawdzenia dostępu DAC i jeśli to sprawdzenie zakończy się pomyślnie, komenda będzie mogła być uruchomiona.

W celu wykonywania operacji na bazie danych komend uprzywilejowanych i zadawania do niej zapytań utworzono kilka komend do zarządzania. Pozycje w bazie danych komend uprzywilejowanych można tworzyć i zmieniać komendą **setsecattr**, wyświetlać komendą **lssecattr**, a usuwać komendą **rmsecattr**.

Określanie autoryzacji wymaganych dla komendy
Wiele aplikacji do administrowania systemem wymaga autoryzacji do poprawnego działania. W bazie danych komend uprzywilejowanych jest zestaw predefiniowanych komend, jednak administratorzy systemu mogą potrzebować dodać pozycje charakterystyczne dla używanego środowiska. Do bazy danych komend uprzywilejowanych można dodawać nowe pozycje. Aby uzyskać dostęp do komendy, odpowiednie autoryzacje muszą być podane w atrybucie **accessauths**.

Istnieją dwa sposoby użycia autoryzacji i jej sprawdzenia w systemie operacyjnym AIX za pomocą rozszerzonego środowiska RBAC:

- Access Auths (Autoryzacja dostępu): Atrybut określony w bazie danych komend uprzywilejowanych zawierających listę oddzielonych przecinkiem nazw autoryzacji. Użytkownik, którego bieżąca sesja ma jedną z autoryzacji podanych na liście, może uruchomić daną komendę. Sprawdzanie jest wykonywane przez program ładujący systemu podczas uruchamiania zabezpieczonych uprzywilejowanych plików wykonywalnych.
- Check Auths (checkauths()): Konkretna autoryzacja lub lista autoryzacji może być sprawdzona programowo za pomocą funkcji API checkauths(). Podane autoryzacje są sprawdzane względem autoryzacji znajdujących się w roli w obrębie bieżącej sesji. Na podstawie danych wyjściowych tego sprawdzania program może wykonać uprzywilejowane operacje.

Przed dodaniem komendy do bazy danych komend uprzywilejowanych muszą być określone zastawy autoryzacji, aby sprawdzić, czy wykonanie danej komendy jest dozwolone. Program lub aplikacja może wewnętrznie wykonać dodatkowe sprawdzenia autoryzacji. Należy określić listę autoryzacji używanych w procesie, które można przypisać podczas tworzenia roli niestandardowej.

Poniżej przedstawiono podstawową strategię określania autoryzacji wymaganych dla komendy:

1. Przypisz uprawnienie **PV_ROOT** do powłoki wywołującej lub przyjmij rolę z autoryzacją *aix*.

   Ważne: W globalnej WPAR uprawnienie **PV_ROOT** musi być przypisane do efektywnego i maksymalnego zestawu uprawnień procesu powłoki wywołującej. W obrębie systemowej WPAR to uprawnienie musi być także dodane do zestawu uprawnień dziedziczenia procesu.
2. Uruchom komendę.
3. Odnotuj autoryzacje używane dla procesu.
4. Zapisz autoryzacje zgłoszone w *Access Auths* w atrybucie **accessauths** komendy w bazie danych komend uprzywilejowanych. Autoryzacji zgłoszonych w *Check Auths* można użyć podczas tworzenia ról w systemie.

Kroki te należy wykonać w środowisku kontrolowanym, ponieważ do powłoki jest przypisane uprawnienie **PV_ROOT** lub przyjęto rolę z autoryzacją *aix*, a obie te metody są bardzo silne. Ponadto uruchomienie komendy może wpłynąć na system i może dotyczyć innych użytkowników. W rzeczywistości przypomina

to metodę prób i błędów. Aby uzyskać pełny zestaw autoryzacji, komenda będzie prawdopodobnie musiała być uruchamiana wielokrotnie, z różnymi opcjami i flagami, i możliwe, że przez długi czas w przypadku aplikacji długotrwałych. Zestaw wymaganych autoryzacji procesu można łatwo uzyskać, stosując jedną z poniżej przedstawionych procedur, które może wykonać administrator z odpowiednimi uprawnieniami:

traceauth
Określ argument będący komendą, która ma być wykonana. Komenda **traceauth** uruchamia podaną komendę i odnotowuje oba typy autoryzacji używane w cyklu życia procesu. Po zakończeniu działania obserwowanej komendy, komenda **traceauth** wyświetla użyte autoryzacje na **wyjściu standardowym**.

lssecattr
Jeśli komenda jest długotrwałym procesem, do wyświetlenia autoryzacji używanych przez ten proces można użyć komendy **lssecattr**. Aby w systemie włączyć śledzenie autoryzacji, uruchom następującą komendę:

setrunmode –c; setsecconf –o traceauth=enable

Aby wyświetlić autoryzację użytą przez proces, uruchom komendę **lssecattr** w sposób przedstawiony poniżej, zastępując PID identyfikatorem PID monitorowanego procesu:

lssecattr –p –A *PID*

Po określeniu wymaganych autoryzacji wykonaj kroki przedstawione w sekcji “Dodawanie komendy do bazy danych komend uprzywilejowanych” na stronie 99, aby dodać komendę do bazy danych komend uprzywilejowanych. Następnie komenda powinna być uruchomiona przez uprawnionego użytkownika, w celu skontrolowania poprawności jej działania.

Określanie uprawnień wymaganych dla komendy
Wiele aplikacji do poprawnego działania wymaga konkretnych uprawnień. W bazie danych komend uprzywilejowanych jest zestaw predefiniowanych komend, jednak administrator systemu może potrzebować dodać pozycje charakterystyczne dla używanej aplikacji lub środowiska. Do bazy danych komend uprzywilejowanych można dodawać pozycje dla komend i powiązanych z nimi uprawnień.

Przed dodaniem komendy do bazy danych komend uprzywilejowanych należy określić minimalny zestaw wymaganych uprawnień, aby zapewnić najlepsze możliwe zabezpieczenie podczas wykonywania komendy. Uprawnienia przekraczające minimum niezbędne do poprawnego wykonania naruszają zasadę najmniejszych uprawnień. Dlatego ważnym krokiem przy dodawaniu komend uprzywilejowanych do systemu jest określenie ich minimalnych wymaganych uprawnień.

Poniżej przedstawiono podstawową strategię określania minimalnych uprawnień wymaganych dla komendy:

1. Osoba odpowiedzialna za bezpieczeństwo systemu informacyjnego (ISSO) lub użytkownik pełniący rolę isso może przypisać uprawnienie **PV_ROOT** administratorowi systemu wykonującemu komendę, która ma być przypisana do bazy danych komend uprzywilejowanych. Przypisanie uprawnienia **PV_ROOT** do wywołującej powłoki wykonuje się za pomocą komendy setsecattr. Na przykład:

   setsecattr -p eprivs=PV_ROOT mprivs=PV_ROOT $$
2. Uruchom komendę, aby zebrać zestaw uprawnień.
3. Odnotuj zestaw uprawnień użyty dla procesu.
4. Zapisz niezbędne uprawnienia w atrybucie **innateprivs** komendy w bazie danych komend uprzywilejowanych.

Czynności te należy wykonać w środowisku kontrolowanym, ponieważ do powłoki jest przypisywane uprawnienie **PV_ROOT**, najsilniejsze z możliwych. Ponadto uruchomienie komendy może wpłynąć na system i może dotyczyć innych użytkowników. W rzeczywistości przypomina to metodę prób i błędów. Aby uzyskać pełny zestaw uprawnień, komenda będzie prawdopodobnie musiała być uruchamiana wielokrotnie, z różnymi opcjami i flagami, i możliwe, że przez długi czas w przypadku aplikacji długotrwałych. Zestaw wymaganych uprawnień procesu można łatwo uzyskać, stosując jedną z poniżej przedstawionych procedur, które może wykonać administrator z odpowiednimi uprawnieniami:

tracepriv
Pobiera jako argument komendę, która ma być wykonana. Komenda **tracepriv** uruchamia podaną komendę i odnotowuje uprawnienia używane w cyklu życia powstałego procesu. Po zakończeniu działania obserwowanej komendy, komenda **tracepriv** wyświetla użyte uprawnienia na **wyjściu standardowym**.

lssecattr
Jeśli komenda jest długotrwałym procesem, do wyświetlenia uprawnień używanych przez ten proces można użyć komendy **lssecattr**. Aby wyświetlić zestaw uprawnień użyty przez proces, uruchom komendę w sposób przedstawiony poniżej, zastępując PID identyfikatorem PID monitorowanego procesu:

lssecattr –p –a uprivs *PID*

Po określeniu minimalnych wymaganych uprawnień wykonaj kroki przedstawione w sekcji “Dodawanie komendy do bazy danych komend uprzywilejowanych” na stronie 99, aby dodać komendę do bazy danych komend uprzywilejowanych. Następnie komenda powinna być uruchomiona przez uprawnionego użytkownika, w celu skontrolowania poprawności jej działania.

Eskalacja uprawnień
Gdy wywołanie systemowe **fork** tworzy nowy proces, nadaje mu takie same uprawnienia, jakie ma proces nadrzędny (proces, który wywołał wywołanie systemowe **fork**). Gdy proces wykonuje wywołanie systemowe **exec** dla pliku wykonywalnego, wywołanie systemowe **exec** ponownie oblicza uprawnienia dla pliku wykonywalnego w oparciu o posiadane już uprawnienia i uprawnienia pliku wykonywalnego.

Uprawnienia eskalowane są obliczane następująco:

1. Najpierw obliczana jest suma (operacja OR na poziomie bitowym) uprawnień odziedziczonych starego (nadrzędnego) procesu z zestawem uprawnień wrodzonych pliku wykonywalnego.
2. Jeśli użytkownik ma odpowiednią autoryzację, obliczana jest suma (bitowa operacja OR) wyniku z poprzedniego kroku oraz uprawnień autoryzowanych.
3. Jeśli istnieje ograniczanie uprawnień, obliczana jest część wspólna wyniku z poprzedniego kroku oraz ograniczonych uprawnień. Ograniczone uprawnienia, jeśli istnieją, są dziedziczone przez wywołanie systemowe **exec**.
4. Zestaw uprawnień wynikający z tej sumy staje się zestawem maksymalnych uprawnień dla nowego procesu.
5. Jeśli w pliku wykonywalnym istnieją uprawnienia dziedziczone, są one przypisywane do zestawu uprawnień odziedziczonych w nowym procesie. W przeciwnym razie do zestawu uprawnień odziedziczonych nowego procesu jest przekazywany zestaw uprawnień odziedziczonych starego (nadrzędnego) procesu.

Jeśli plik wykonywalny ma ustawioną swoją opcję bezpieczeństwa pliku **FSF_EPS**, zestaw obowiązujących uprawnień dla nowego procesu jest taki sam, jak jego zestaw maksymalnych uprawnień. W przeciwnym razie uprawnienia obowiązujące nowego procesu są takie same, jak uprawnienia odziedziczone należące do starego (nadrzędnego) procesu.

Dodawanie komendy do bazy danych komend uprzywilejowanych
Decyzję o dodaniu komendy do bazy danych komend uprzywilejowanych należy dokładnie przemyśleć, aby zapewnić przypisanie odpowiednich autoryzacji i uprawnień.

Plik `/etc/security/privcmds` zawiera pełny opis poprawnych atrybutów komendy. Poniższe pytania mogą służyć jako przewodnik podczas określania wpisu wymaganego dla komendy:

1. Czy autoryzacja steruje dostępem do uruchamiania komendy?

   TAK
   Jeśli autoryzacja nie istnieje, utwórz ją przy użyciu komendy **mkauth**. Autoryzację określ w atrybucie **accessauths**.

   NIE
   Jeśli wszyscy użytkownicy mają mieć prawo do uruchamiania tej komendy, podaj w atrybucie **accessauths** autoryzację **ALLOW_ALL**.

2. Czy właściciel lub grupa komendy mają mieć prawo do uruchamiania komendy, nawet jeśli nie mają odpowiedniej autoryzacji?

   TAK
   Dodaj autoryzację **ALLOW_OWNER** lub **ALLOW_GROUP** do listy autoryzacji w atrybucie **accessauths**.

3. Czy podczas wykonywania komenda wymaga jasno sprecyzowanego zestawu uprawnień?

   TAK
   Uruchom komendę z różnymi opcjami, z poziomu użytkownika root, używając komendy **tracepriv**, aby określić żądane uprawnienia w atrybucie **innateprivs**.

4. Czy użytkownicy z konkretną autoryzacją powinni mieć nadawane dodatkowe uprawnienia?

   TAK
   Określ dodatkowe pary autoryzacja-uprawnienie w atrybucie **authprivs**.

5. Czy komenda ma się zachowywać jak program SUID lub SGID?

   TAK
   Podaj odpowiednio EUID lub EGID.

6. Czy uprawnienia przypisane do tej komendy mają być przekazane do procesów potomnych?

   TAK
   Określ uprawnienia w atrybucie **inheritprivs**.

7. Czy obowiązujący zestaw uprawnień komendy ma być taki sam, jak maksymalny zestaw uprawnień w momencie wywołania komendy?

   TAK
   Podaj opcję **FSF_EPS** atrybutu secflags.

   NIE
   Nie podawaj atrybutu **secflags**. Kod komendy będzie podnosił i obniżał swoje uprawnienia zgodnie z potrzebami, jeśli nie zostanie podana opcja **FSF_EPS**.

8. Czy komenda musi być uruchamiana z użyciem specjalnego rzeczywistego identyfikatora użytkownika 0?

   TAK
   Podaj atrybut RUID.

9. Czy komenda jest newralgiczna i czy wymaga kontroli oraz czy jej wywołanie wymaga obecności co najmniej dwóch osób?

   TAK
   Podaj atrybut **authroles** i przypisz mu wartość, używając listy ról. Użytkownicy należący do każdej roli będą musieli zostać uwierzytelnieni przed wykonaniem tej komendy.

Gdy odpowiesz na te pytania, uruchom komendę **setsecattr** z odpowiednimi parametrami, aby dodać komendę do bazy danych. Jeśli jest to istniejąca komenda SUID lub SGID, należy rozważyć usunięcie bitów **SUID** i **SGID** z pliku, aby wymusić zastosowanie modelu najmniejszych uprawnień.

Baza danych urządzeń uprzywilejowanych
Baza danych urządzeń uprzywilejowanych przechowuje listę uprawnień zezwalających na odczyt z urządzenia lub zapis do niego. Stanowi ona mechanizm dla administratora służący do lepszej od metod tradycyjnych kontroli dostępu do urządzenia.

Baza danych przechowywana lokalnie znajduje się w pliku `/etc/security/privdevs`. W bazie danych w następujących atrybutach są zapisane uprawnienia niezbędne w celu dostępu do danego urządzenia dla operacji zapisu lub odczytu:

readprivs
Pokazuje listę uprawnień umożliwiających odczyt z urządzenia.

writeprivs
Pokazuje listę uprawnień umożliwiających zapis do urządzenia.

W przypadku żądania otwarcia urządzenia uprzywilejowanego w trybie do odczytu, realizacja żądania jest dozwolona, tylko jeśli jedno z uprawnień podanych w atrybucie **readprivs** istnieje w obowiązującym zestawie uprawnień (EPS) procesu. Podobnie w przypadku otwierania urządzenia w trybie do zapisu, w zestawie EPS musi istnieć uprawnienie w atrybucie **writeprivs**.

Proces dodawania urządzenia do bazy danych komend uprzywilejowanych zwykle nie jest częstą operacją. Do wyświetlania zawartości bazy danych i operacji na niej służą komendy **lssecattr** i **setsecattr**, jednak dodawanie i zmiana wpisów w bazie danych wymagają dokładniejszej analizy. Uprawnienia odczytu i zapisu dotyczące urządzenia są sterowane uprawnieniami, należy jednak przeprowadzić gruntowne sprawdzenie komend i aplikacji wymagających dostępu do urządzenia, aby zagwarantować określenie prawidłowych uprawnień.

Baza danych plików uprzywilejowanych

Wiele plików konfiguracyjnych systemu w tradycyjnych systemach UNIX należy do użytkownika root i inni użytkownicy nie mogą ich bezpośrednio modyfikować. Kontrola RBAC umożliwia użytkownikowi modyfikowanie tych plików konfiguracyjnych systemu dzięki aktywacji roli i uruchomieniu komendy w celu uzyskania uprawnień potrzebnych do modyfikowania pliku.

Niektóre pliki konfiguracyjne systemu AIX nie mają interfejsów komend umożliwiających ich modyfikację. W takich przypadkach niezbędne jest narzędzie umożliwiające administratorowi z odpowiednią autoryzacją bezpośrednią edycję i zapisanie pliku, do którego inaczej nie ma dostępu.

Baza danych plików uprzywilejowanych zapewnia metodę użycia autoryzacji w celu określenia dostępu do plików konfiguracyjnych systemu. Baza danych przechowywana lokalnie znajduje się w pliku `/etc/security/privfiles`. Odwzorowuje ona pliki konfiguracyjne na autoryzacje wymagane do ich przeglądania i modyfikowania. Dostęp do pliku konfiguracyjnego określają w tej bazie danych następujące atrybuty:

readauths
Lista autoryzacji umożliwiających odczyt z pliku.

writeauths
Lista autoryzacji umożliwiających zapis do pliku (i niejawna autoryzacja odczytu).

Pozycje w bazie danych plików uprzywilejowanych można wyświetlać komendą **lssecattr**, a tworzyć i modyfikować komendą **setsecattr**. Dostęp do plików zdefiniowanych w bazie danych plików uprzywilejowanych dla użytkowników z odpowiednią autoryzacją zapewnia komenda **/usr/bin/pvi**. Komenda **pvi** jest uprzywilejowaną i ograniczoną wersją edytora **vi** opartą na komendzie **/usr/bin/tvi**. Komenda **pvi** narzuca takie same środki ostrożności, jak komenda **tvi** (na przykład brak opcji **–r** i **-t**, brak wyjść do powłoki, brak makrodefinicji definiowanych przez użytkownika), a także wymusza następujące ograniczenia:

- System musi być w rozszerzonym trybie RBAC.
- Można otwierać tylko pliki zdefiniowane w bazie danych komend uprzywilejowanych.
- Jednocześnie można otworzyć tylko jeden plik.
- Wyłączona jest możliwość zapisania pliku pod nazwą inną niż podana w wierszu komend.
- Pliku `/etc/security/privfiles` nie można edytować komendą **pvi**.
- Nie powiedzie się próba otwarcia dowiązań. Można edytować tylko zwykłe pliki.

Sprawdzanie autoryzacji odbywa się przed otworzeniem pliku. Jeśli autoryzacja zostanie potwierdzona, zestaw uprawnień procesu jest podnoszony, tak aby zawierał **PV_DAC_R** lub **PV_DAC_W** (w zależności od tego, czy plik jest otwierany do odczytu czy do zapisu). Jeśli autoryzacja nie zostanie potwierdzona, jest wyświetlany komunikat o błędzie i następuje odmowa dostępu do pliku za pomocą komendy **pvi** dla tego użytkownika.

Tabele bezpieczeństwa jądra

Informacje zawarte w bazach danych autoryzacji, ról, komend uprzywilejowanych i urządzeń uprzywilejowanych nie są uwzględniane przez system bezpieczeństwa systemu, dopóki nie zostaną załadowane do wydzielonego obszaru w jądrze nazywanego tabelami bezpieczeństwa jądra (KST). W

rozszerzonym trybie RBAC sprawdzanie autoryzacji i uprawnień jest wykonywane w jądrze, dlatego bazy danych przed użyciem należy przesłać do jądra.

W skład tabel KST wchodzą następujące tabele:

- Tabela autoryzacji jądra (Kernel Authorization Table - KAT)
- Tabela ról jądra (Kernel Role Table - KRT)
- Tabela komend jądra (Kernel Command Table - KCT)
- Tabela urządzeń jądra (Kernel Device Table - KDT)

Wszystkie te tabele lub tylko wybrane tabele można przesłać do jądra z przestrzeni użytkownika komendą **setkst**. Tabele KRT i KCT zależą od tabeli KAT, dlatego, jeśli tabela KAT zostanie wybrana do aktualizacji, obie te tabele zostaną również zaktualizowane, aby zapewnić ich synchronizację. Preferowaną metodą dodawania zaktualizowanych danych do tabeli KST jest utworzenie lub zmiana wszystkich niezbędnych baz danych na poziomie użytkownika (komendami takimi jak **mkauth**, **chauth**, **mkrole** i **setsecattr**), a następnie przesłanie tabel do jądra komendą **setkst**. Po załadowaniu tabel do jądra można wyświetlić informacje w nich zawarte używając komendy **lskst**.

Dana tabela z tabel KST jest wysyłana zawsze w całości. Innymi słowy, tabele KST nie umożliwiają zmiany pojedynczego wpisu, musi być wymieniona cała tabela. Przed wysłaniem tabel do jądra komenda **setkst** sprawdza tabele oraz relacje między nimi. Komenda **setkst** znajduje się również w pliku `inittab`, aby zapewnić przesłanie baz danych do tabel KST na początku przetwarzania startowego.

Jeśli z pewnych powodów nie można utworzyć tabel ani załadować ich do jądra i wcześniej nie zostały załadowane żadne tabele, system działa tak, jakby nie istniały żadne autoryzacje ani role. Komendy, funkcje API i wywołania systemowe z żądaniem autoryzacji oraz sprawdzanie ról zwraca w takim wypadku niepowodzenie, ponieważ nie można znaleźć pasujących wpisów. Działanie systemu w tym stanie przypomina działanie we wcześniejszym trybie RBAC, jednak żaden użytkownik nie ma dostępu do sekcji kodu w komendach, które wymuszają autoryzacje.

Wyłączenie użytkownika root

W rozszerzonym trybie RBAC można tak skonfigurować system, aby użytkownik root nie miał przypisanych specjalnych możliwości i był traktowany w tym systemie jak zwykły użytkownik.

Z powodów historycznych wartość identyfikatora użytkownika root wynosząca 0 powodowała traktowanie tego identyfikatora przez system operacyjny jako uprawnionego i umożliwiała omijanie wymuszonych procedur kontroli bezpieczeństwa. Wyłączenie użytkownika root w rzeczywistości powoduje usunięcie sprawdzenia przez system operacyjny, które umożliwia użytkownikowi o identyfikatorze równym 0 ominięcie kontroli bezpieczeństwa. W zamian wymagane jest, aby proces miał uprawnienie do przejścia kontroli bezpieczeństwa. Wyłączenie użytkownika root minimalizuje zniszczenia, które może spowodować włamywacz komputerowy, ponieważ w systemie nie ma już jednej tożsamości użytkownika o nieograniczonych możliwościach. Po wyłączeniu użytkownika root administracja systemem należy do użytkowników z przypisanymi rolami uprzywilejowanymi.

Nieograniczone możliwości użytkownika root można wyłączyć komendą **/usr/sbin/setsecconf**. Uruchom następującą komendę, a następnie zrestartuj system, aby wyłączyć możliwości użytkownika root:

```
setsecconf –o root=disable
```

Po uruchomieniu powyższej komendy dostęp do konta użytkownika root jest blokowany przez logowanie zdalne, lokalne i komendę su. Konto użytkownika root pozostaje właścicielem plików w systemie plików i gdyby zostało ono włączone, użytkownik miałby prawo dostępu do plików uprzywilejowanych.

W systemie z wyłączonym użytkownikiem root procesy, których jest on właścicielem, nie mają już żadnych specjalnych uprawnień ani możliwości. Należy o tym pamiętać, jeśli w systemie są aplikacje z bitem setuid należące do użytkownika root, które nie zostały dodane do bazy danych komend uprzywilejowanych. Takie aplikacje prawdopodobnie nie zadziałają w środowisku z wyłączonym użytkownikiem root, ponieważ proces nie będzie mógł wykonać operacji uprzywilejowanych. W systemie z wyłączonym użytkownikiem root każda komenda, która ma wykonać operacje uprzywilejowane, powinna być dodana do bazy danych komend uprzywilejowanych i należy przypisać do niej odpowiednie uprawnienia. Dlatego przed

wyłączeniem możliwości użytkownika root należy przeprowadzić wnikliwą analizę systemu i używanych w nim aplikacji.

Obsługa zdalnej bazy danych RBAC
W środowisku korporacyjnym może być potrzebne zaimplementowanie i wymuszenie wspólnej strategii bezpieczeństwa na wszystkich systemach należących do tego środowiska. Jeśli bazy danych sterujące strategią są przechowywane niezależnie na poszczególnych systemach, zarządzanie strategią bezpieczeństwa staje się obciążeniem dla wyznaczonego administratora systemu. Rozszerzony tryb RBAC systemu AIX umożliwia przechowywanie baz danych RBAC w LDAP, dzięki temu strategia bezpieczeństwa dla wszystkich systemów w środowisku może być zarządzana centralnie.

W systemie AIX dodano obsługę przechowywania w LDAP istotnych baz danych kontroli RBAC. Istotne bazy danych kontroli RBAC są następujące:

- Baza danych autoryzacji
- Baza danych ról
- Baza danych komend uprzywilejowanych
- Baza danych urządzeń uprzywilejowanych
- Baza danych plików uprzywilejowanych

Uwaga: Baza danych autoryzacji przechowywana w LDAP zawiera tylko autoryzacje zdefiniowane przez użytkownika. Autoryzacje zdefiniowane przez system nie mogą być przechowywane w LDAP i pozostają lokalne w każdym systemie klienckim.

System AIX udostępnia programy użytkowe do łatwego eksportu lokalnych danych RBAC do LDAP, do konfigurowania klienta, aby używał danych RBAC w LDAP, do sterowania wyszukiwaniem danych RBAC i do zarządzania danymi LDAP z poziomu systemu klienckiego. Poniższe sekcje zawierają więcej informacji o opcjach LDAP udostępnianych w rozszerzonym trybie RBAC.

Eksportowanie danych RBAC do LDAP
Przygotowanie początkowe do korzystania z serwera LDAP jako repozytorium bazy danych RBAC wymaga zapełnienia serwera LDAP danymi RBAC.

Serwer LDAP musi mieć zainstalowany schemat RBAC dla LDAP zanim klienty LDAP będą mogły użyć serwera dla danych RBAC. Schemat RBAC dla LDAP jest dostępny w systemie AIX w pliku `/etc/security/ldap/sec.ldif`. Schemat serwera LDAP należy zaktualizować o ten plik, używając komendy **ldapmodify**.

Plik **/usr/sbin/rbactoldif** może służyć do odczytu danych w lokalnych bazach danych RBAC i do wyprowadzenia ich w formacie odpowiednim dla serwera LDAP. Dane wyjściowe wygenerowane przez komendę **rbactoldif** można zapisać do pliku, a następnie wstawić do serwera LDAP komendą **ldapadd**. W systemie lokalnym komenda **rbactoldif** używa następujących baz danych do generowania danych RBAC dla LDAP:

- `/etc/security/authorizations`
- `/etc/security/privcmds`
- `/etc/security/privdevs`
- `/etc/security/privfiles`
- `/etc/security/roles`

Należy poświęcić nieco uwagi miejscu składowania przez LDAP danych RBAC. Zaleca się, aby dane RBAC na serwerze LDAP należały do tej samej nadrzędnej nazwy wyróżniającej, co dane grupy i użytkownika. Listy kontroli dostępu do tych danych należy następnie dostosować do wybranej strategii bezpieczeństwa.

Konfiguracja klienta LDAP dla RBAC
Aby system mógł używać danych RBAC przechowywanych na serwerze LDAP, musi być skonfigurowany jako klient LDAP.

Do konfigurowania systemu AIX jako klienta LDAP służy komenda **/usr/sbin/mksecldap**. Komenda **mksecldap** dynamicznie przeszukuje podany serwer LDAP, aby określić położenie danych autoryzacji, ról,

komend uprzywilejowanych, urządzeń i plików, a wyniki zapisuje w pliku /etc/security/ldap/ldap.cfg.

Po pomyślnym skonfigurowaniu systemu jako klienta LDAP komendą **mksecldap**, należy następnie go skonfigurować, tak aby włączyć LDAP jako domenę wyszukiwania dla danych RBAC. Plik /etc/nscontrol.conf musi zostać zmieniony: powinien zawierać LDAP w atrybucie **secorder** dla baz danych przechowywanych na serwerze LDAP.

W systemie skonfigurowanym jako klient LDAP i domena wyszukiwania dla danych RBAC demon kliencki **/usr/sbin/secldapclntd** okresowo pobiera dane RBAC z LDAP i wysyła je komendą **setkst** do tabel bezpieczeństwa jądra (KST). Przedział czasu pomiędzy pobieraniem przez demon danych RBAC z LDAP można skonfigurować, używając atrybutu **rbacinterval** w pliku /etc/security/ldap/ldap.cfg. Domyślna wartość tego atrybutu wynosi 3600, czyli dane RBAC są pobierane z LDAP, a tabele KST są aktualizowane co godzinę. Tabele KST można zaktualizować również samodzielnie, w tym celu administrator może uruchomić komendę **setkst**.

Plik sterujący usługi nazw
Dane RBAC mogą znajdować się tylko w plikach lokalnych, tylko w bazie danych LDAP lub scalone w plikach lokalnych i bazie danych LDAP dzięki skonfigurowaniu podanej bazy danych w pliku sterującym usługi nazw /etc/nscontrol.conf.

Kolejność wyszukiwania baz danych autoryzacji, ról, komend uprzywilejowanych, uprzywilejowanych urządzeń i plików jest określana indywidualnie w pliku /etc/nscontrol.conf. Kolejność wyszukiwania bazy danych jest podana w pliku w atrybucie **secorder**, zawierającym oddzieloną przecinkami listę domen. Poniżej przedstawiono przykład konfiguracji bazy danych autoryzacji:

```
authorizations:
        secorder = LDAP,files
```

W przykładzie określono, że zapytania dotyczące autoryzacji powinny najpierw przeszukiwać bazę danych LDAP, a następnie, jeśli autoryzacja nie zostanie znaleziona, pliki lokalne. Kolekcja autoryzacji dostępna w systemie jest scalana w autoryzacje udostępniane przez LDAP i udostępniane w plikach lokalnych. Scalenie nie jest prostym połączeniem wartości z dwóch domen, ale raczej sumą wartości. W przypadku powyższej konfiguracji uwzględniane są wszystkie autoryzacje LDAP, a następnie do wyników są dodawane tylko unikalne autoryzacje z plików lokalnych.

Modyfikacje (w tym usuwanie) są wprowadzane w pierwszej wymienionej domenie, a w następnych domenach tylko jeśli pozycja nie zostanie znaleziona w pierwszej domenie. W przedstawionym przykładzie najpierw sprawdzana jest baza danych LDAP, a jeśli autoryzacja nie zostanie znaleziona, sprawdzane są pliki lokalne. Nowe pozycje zawsze są tworzone w pierwszej domenie wymienionej w atrybucie **secorder**. W powyższym przykładzie nowa autoryzacja zostanie utworzona w bazie danych LDAP.

Jeśli w pliku /etc/nscontrol.conf nie ma żadnego wpisu dotyczącego bazy danych lub jeśli plik nie istnieje, zapytania do bazy danych oraz wszystkie modyfikacje dotyczą bazy danych plików lokalnych. Konfigurację bazy danych w pliku można ustawić komendą **chsec**, a wyświetlić komendą **lssec**. Aby skonfigurować wyszukiwanie danych autoryzacji najpierw w bazie danych LDAP, a następnie w plikach lokalnych, uruchom następującą komendę:

```
chsec –f /etc/nscontrol.conf –s authorizations –a secorder=LDAP,files
```

Konfiguracja w pliku /etc/nscontrol.conf steruje zarówno interfejsem biblioteki, jak i wiersza komend. Aplikacje mogą pobrać bieżącą wartość atrybutu **secorder** dla bazy danych za pomocą interfejsu **getsecorder**. Wartość **secorder** dla procesu można nadpisać interfejsem **setsecorder**.

Włączenie komend RBAC dla LDAP
Wszystkie komendy do zarządzania bazą danych RBAC używają konfiguracji znajdującej się w pliku /etc/nscontrol.conf i mogą modyfikować, tworzyć i usuwać pozycje w domenie lub w domenach zdefiniowanych dla danej bazy danych oraz wysyłać zapytania o te pozycje.

Domyślnie domeny są przetwarzane zgodnie z definicją w atrybucie **secorder** dla bazy danych, może ona jednak być przesłonięta za pomocą opcji **–R** w wierszu komend. Podanie dla komendy opcji **–R** wymusza wykonanie operacji na podanej domenie i przesłania konfigurację wpisaną do pliku /etc/

`nscontrol.conf`. Do obsługi domeny zdalnej służą następujące komendy do zarządzania bazą danych RBAC:

- **mkauth**, **chauth**, **lsauth** i **rmauth**
- **mkrole**, **chrole**, **lsrole** i **rmrole**
- **setsecattr**, **lssecattr** i **rmsecattr**

Ponadto komenda **setkst** może używać konfiguracji znajdującej się w pliku `/etc/nscontrol.conf`. Komenda **setkst** pobiera scaloną kopię pozycji dla danej bazy danych zdefiniowaną w pliku, a następnie ładuje dane wynikowe do tabel bezpieczeństwa jądra.

Przypisanie międzydomenowe
Podczas projektowania środowiska, w którym dane RBAC są udostępniane przez dwie domeny, na przykład pliki lokalne i LDAP, należy rozważyć zagadnienia związane z przypisaniem międzydomenowym. Przykładem przypisania międzydomenowego jest przypisanie roli zdefiniowanej w LDAP użytkownikowi lokalnemu lub przypisanie roli zdefiniowanej lokalnie użytkownikowi LDAP.

Przypisanie elementu zdalnego (rola LDAP) do lokalnego (użytkownik lokalny) nie wymaga tyle zachodu, ponieważ nie wpływa na inne systemy w danym środowisku. Jednak przypisanie elementu lokalnego (rola lokalna) do zdalnego (użytkownik LDAP) należy wykonać z zachowaniem największej ostrożności. Element zdalny (użytkownik LDAP) ma zasięg wielu klientów, dlatego nie ma gwarancji, że przypisany do niego element lokalny (rola lokalna) jest zdefiniowany w każdym systemie klienckim lub że w każdym z tych systemów będzie to taka sama definicja. Na przykład rola zdefiniowana lokalnie na każdym kliencie może mieć przypisane różne autoryzacje. Użytkownik zdalny, mający przypisaną tę rolę lokalną, może mieć różne autoryzacje na każdym z tych klientów, a to może spowodować nieprzewidywalne konsekwencje związane z bezpieczeństwem.

Aby zapobiec możliwym problemom z bezpieczeństwem przy przypisywaniu lokalnego elementu do elementu LDAP, zaleca się, aby serwer LDAP implementował kontrolę dostępu do baz danych RBAC, w celu ochrony klientów przed zmianami wpisów. Tylko klient łączący się z serwerem LDAP z konta uprzywilejowanego powinien mieć możliwość zmiany wpisów RBAC LDAP. Inne klienty powinny mieć tylko dostęp do odczytu baz danych RBAC LDAP.

Limity wielkości w rozszerzonym trybie RBAC
W poniższej tabeli są wymienione różne ograniczenia elementów związanych z trybem RBAC:

Tabela 10. Różne ograniczenia elementów związanych z trybem RBAC

Opis	**Maksymalna wielkość**
Nazwa roli	63 widoczne znaki
Maksymalna liczba ról na jedną sesję	8
Maksymalna wielkość nazwy autoryzacji	63 widoczne znaki
Maksymalna liczba poziomów w hierarchii autoryzacji	9
Maksymalna liczba autoryzacji dostępu na jedną komendę	8
Maksymalna liczba zestawów uprawnień autoryzacji na jedną komendę	8

Administrowanie rozszerzonym trybem RBAC
W sekcji opisano najczęściej stosowaną składnię wiersza komend do administrowania trybem RBAC. Przykłady ilustrują główne aspekty funkcjonalności. W systemie są dostępne również interfejsy programu SMIT do administrowania RBAC. Krótka ścieżka do menu programu SMIT dla trybu RBAC to `smit rbac`.

Tworzenie autoryzacji zdefiniowanej przez użytkownika
Do sterowania wykonywaniem komend można utworzyć autoryzacje zdefiniowane przez użytkownika.

Aby utworzyć autoryzacje zdefiniowane przez użytkownika, można użyć komendy mkauth. Zmiany w bazie danych autoryzacji zaczną obowiązywać dopiero po ich pobraniu do jądra komendą **setkst**.

- Uruchom następującą komendę, aby utworzyć autoryzację zdefiniowaną przez użytkownika:

  mkauth *nazwa_autoryzacji*

Tworzenie i modyfikowanie ról
Rolę można utworzyć komendą **mkrole**.

Role są tworzone komendą **mkrole**. Zmiany w bazie danych ról zaczną obowiązywać dopiero po pobraniu ich do jądra komendą **setkst**. Do modyfikowania ról służy komenda **chrole**.

- Uruchom następującą komendę, aby utworzyć rolę:

  mkrole dflt_msg="*Moja rola***"** *nazwa_roli*
- Aby utworzyć rolę i zawrzeć w niej autoryzacje z istniejących ról, uruchom następującą komendę:

  mkrole rolelist=*rola_potomna_1***,***rola_potomna_2 nazwa_roli*
- Aby zmodyfikować definicję roli, uruchom następującą komendę:

  chrole rolelist=*rola_potomna_3 nazwa_roli*

Przypisywanie autoryzacji do ról
W celu przypisania autoryzacji do ról można użyć komendy **mkrole** lub **chrole**.

- Uruchom komendę **mkrole**, aby przypisać autoryzacje **nazwa_autoryzacji1** i **nazwa_autoryzacji2** do roli **nazwa_roli**:

```
mkrole
authorizations=nazwa_autoryzacji1,nazwa_autoryzacji2 nazwa_roli
```

- Uruchom komendę **chrole**, aby przypisać autoryzacje **nazwa_autoryzacji1** i **nazwa_autoryzacji2** do roli **nazwa_roli**:

```
chrole
authorizations=nazwa_autoryzacji1,nazwa_autoryzacji2 nazwa_roli
```

Ustawianie trybu uwierzytelniania dla roli
Do sterowania aktywowaniem ról służy atrybut roli **auth_mode**.

Poprawne wartości atrybutu **auth_mode**:

NONE
Uwierzytelnianie nie jest konieczne.

INVOKER
Użytkownik wywołujący musi wprowadzić swoje hasło. Jest to wartość domyślna.

Wpisz następującą komendę, aby wymusić na użytkownikach uwierzytelnianie się podczas przyjmowania danej roli:

chrole auth_mod=INVOKER *nazwa_roli*

Przypisywanie ról do użytkownika
W celu przypisania ról do użytkownika można użyć komendy **chuser**.

Uruchom następującą komendę, aby przypisać role **nazwa_roli_1** i **nazwa_roli_2** do użytkownika **nazwa_użytkownika**:

```
chuser
roles=nazwa_roli_1,nazwa_roli_2 nazwa_użytkownika
```

Aktywowanie ról
Domyślnie użytkownik musi aktywować rolę w sesji, aby wykonać komendy uprzywilejowane.

- Aby aktywować role **nazwa_roli_1** i **nazwa_roli_2**, uruchom następującą komendę:

```
swrole nazwa_roli_1,nazwa_roli_2
```

- Niektóre role przypisane do użytkowników są klasyfikowane jako role domyślne. Role takie są aktywowane automatycznie w momencie logowania się użytkownika. Pozostają aktywne przez całą sesję użytkownika. Aby przypisać rolę nazwa_roli_1 jako domyślną rolę użytkownika, uruchom następującą komendę:

```
chuser roles=nazwa_roli_1,nazwa_roli2 default_roles=nazwa_roli_1
nazwa_użytkownika
```

Wyświetlanie aktywnego zestawu ról
Aby wyświetlić informacje o obowiązującym aktywnym zestawie ról dla sesji, można użyć komendy **rolelist** z opcją -e.

- Aby wyświetlić obowiązujący aktywny zestaw ról dla sesji, uruchom następującą komendę:

```
rolelist -e
```

Wyświetlanie ról użytkownika
Komenda **rolelist** udostępnia informacje o rolach i autoryzacji dotyczące bieżących ról użytkownika lub ról przypisanych do niego.

Domyślnie komenda **rolelist** wyświetla listę ról przypisanych do użytkownika. Są to te same informacje, które wyświetla komenda `lsuser -a roles użytkownik1`, jednak wyświetla ona również opis tekstowy roli, jeśli istnieje.

- Aby wyświetlić przypisane role oraz powiązane autoryzacje, uruchom następującą komendę:

```
rolelist -a
```

Kontrola ról sesji
Role aktywne w sesji użytkownika są kontrolowane wraz z innymi atrybutami, takimi jak identyfikatory UID i GID. Do wyświetlenia tych ról służy komenda **auditpr**.

Aby wyświetlić role z zapisu kontrolnego, uruchom następującą komendę:

```
auditpr -h eli -i /audit/trail
```

Przypisywanie uprawnień do działającego procesu
Komendy **setsecattr** można użyć w celu zmiany uprawnień działającego procesu.

- Aby zaktualizować obowiązujący zestaw uprawnień powiązany z procesem, uruchom następującą komendę:

  setsecattr –p eprivs=*uprawnienia pid*

```
```

- Przed dodaniem uprawnienia do obowiązującego zestawu uprawnień procesu należy sprawdzić, czy to uprawnienie już istnieje w maksymalnym zestawie uprawnień. Aby zmienić maksymalny zestaw uprawnień, uruchom następującą komendę:

  setsecattr –p mprivs=*uprawnienia pid*

Administrowanie uprawnieniami partycji WPAR
Każda partycja WPAR jest powiązana z zestawem uprawnień określającym jej możliwości. Taki zestaw jest nazywany zestawem uprawnień WPAR (WPS).

Procesy uruchomione w danej partycji WPAR mogą używać tylko uprawnień dostępnych w zestawie WPS.

- Aby zmienić zestaw WPS z globalnej partycji WPAR, uruchom następującą komendę:

  chwpar –S privs+=*uprawnienia nazwa_wpar*

Określanie uprawnień wymaganych przez komendę
Niektóre komendy wymagają specjalnych uprawnień do wykonania operacji uprzywilejowanych. Uprawnienia są używane w jądrze do ominięcia ograniczeń związanych z bezpieczeństwem.

Komenda **tracepriv** pozwala określić uprawnienia, które muszą być przydzielone innej komendzie, aby było możliwe jej wykonanie. Komenda **tracepriv** zapisuje uprawnienia używane przez inną komendę, gdy jest ona uruchamiana. Komendę należy uruchamiać z uprawnieniem **PV_ROOT**, aby powiodła się każda próba użycia uprawnień. Po zakończeniu działania komendy zestaw użytych uprawnień jest wysyłany do wyjścia standardowego.

- Aby określić uprawnienia danej komendy, uruchom następującą komendę:

  tracepriv –ef *nazwa_komendy*

Korzystanie z autoryzacji do sterowania komendami
Autoryzacje mogą służyć do sterowania działaniem komend.

Za pomocą komendy **setsecattr** można powiązać autoryzacje z komendą. Komenda **setsecattr** dodaje sekcję do bazy danych komend uprzywilejowanych (/etc/security/privcmds). Modyfikacje wprowadzone w tej bazie danych muszą być pobrane do jądra komendą **setkst**.

- Aby powiązać autoryzacje z komendą, uruchom następującą komendę:

  setsecattr –c accessauths=*nazwa_autoryzacji* **innateprivs=***uprawnienia* **proxyprivs=***uprawnienia* **authprivs=***nazwa_autoryzacji***=***uprawnienia nazwa_komendy*

Kontrola dostępu do urządzeń
Kontrola RBAC udostępnia mechanizm do dalszej kontroli dostępu do urządzeń. Administrator systemu może określić uprawnienia wymagane przy otwieraniu urządzenia w trybie do odczytu lub zapisu.

Na przykład zapis na nagrywarki DVD może zależeć od uprawnienia **PV_DEV_CONFIG**, więc jedynie procesy z tym uprawnieniem będą mogły tworzyć dyski DVD.

- Aby dodać urządzenie do bazy danych urządzeń, uruchom następującą komendę:

  setsecattr –d readprivs=*uprawnienia* **writeprivs=***uprawnienia nazwa_urządzenia*

Aktualizacja tabel bezpieczeństwa jądra kontroli RBAC
Komenda **setkst** odczytuje bazy danych bezpieczeństwa i ładuje informacje w nich zawarte do tabel bezpieczeństwa jądra (KST).

Domyślnie wszystkie bazy danych bezpieczeństwa są wysyłane do tabel KST. Alternatywnie można podać konkretną bazę danych, używając w tym celu opcji -t. Jednak określenie, że tylko baza danych autoryzacji powinna być wysłana do tabel KST, powoduje również aktualizację baz danych ról i komend uprzywilejowanych w tabelach KST, ponieważ te bazy danych są zależne od bazy danych autoryzacji.

- Aby wysłać wszystkie najnowsze bazy danych RBAC do jądra, uruchom następującą komendę:

```
setkst
```

Korzystanie z przełącznika rozszerzonego trybu RBAC
Można wyłączyć możliwości rozszerzonej kontroli RBAC i powrócić do wcześniejszej wersji kontroli RBAC używając przełącznika konfiguracji dla całego systemu.

Administrator systemu może wyłączyć rozszerzony tryb RBAC: w tym celu musi uruchomić komendę **chdev** dla urządzenia **sys0**, podać atrybut **enhanced_RBAC** z wartością **false**, a następnie zrestartować system. Aby przywrócić rozszerzony tryb RBAC, należy nadać atrybutowi **enhanced_RBAC** wartość **true** i zrestartować system.

- Aby powrócić do wcześniejszego trybu RBAC, uruchom następującą komendę:

```
chdev -l sys0 -a enhanced_RBAC=false
```

- Aby wyświetlić wartości atrybutu **enhanced_RBAC**, uruchom następującą komendę:

```
lsattr -E -l sys0 -a enhanced_RBAC
```

W środowisku partycji WPAR tryb RBAC można konfigurować tylko z systemu globalnego i dotyczy on zarówno tego systemu, jak i wszystkich partycji WPAR.

Uwaga: Wyłączenie rozszerzonego trybu RBAC może zmniejszyć próg bezpieczeństwa systemu, zwłaszcza w partycji WPAR.

Komendy związane z kontrolą RBAC
Poniższa tabela zawiera komendy związane z kontrolą RBAC dostępne w systemie operacyjnym AIX do zarządzania środowiskiem RBAC i używania tego środowiska.

Komenda	Opis
chauth	Modyfikuje atrybuty autoryzacji zdefiniowane przez użytkownika.
chrole	Modyfikuje atrybuty roli.
ckauth	Sprawdza autoryzację bieżącego procesu.
lsauth	Wyświetla atrybuty autoryzacji zdefiniowane przez użytkownika i system.
lskst	Wyświetla pozycje tabel bezpieczeństwa jądra.
lspriv	Wyświetla uprawnienia dostępne w systemie.
lsrole	Wyświetla atrybuty roli.
lssecattr	Wyświetla atrybuty bezpieczeństwa komendy, urządzenia, procesu lub pliku.
mkauth	Tworzy nową autoryzację zdefiniowaną przez użytkownika.
mkrole	Tworzy nową rolę.
pvi	Edytor plików uprzywilejowanych.
rbacqry	Włącza kontrolę RBAC dla aplikacji.
rbactoldif	Dane wyjściowe baz danych na poziomie użytkownika kontroli RBAC w formacie zgodnym z LDAP.
rmauth	Usuwa autoryzacje zdefiniowane przez użytkownika.
rmrole	Usuwa rolę.
rmsecattr	Usuwa definicję atrybutów bezpieczeństwa komendy, urządzenia lub pliku.
rolelist	Wyświetla informacje o roli użytkownika lub procesu.
setkst	Wysyła pozycje z baz danych na poziomie użytkownika kontroli RBAC do tabel bezpieczeństwa jądra.
setsecattr	Ustawia atrybuty bezpieczeństwa komendy, urządzenia, procesu lub pliku.
setsecconf	Modyfikuje opcje bezpieczeństwa jądra.
swrole	Tworzy nową sesję roli.
tracepriv	Śledzi uprawnienia, których potrzebuje komenda do pomyślnego uruchomienia.

Pliki związane z kontrolą RBAC
Poniższa tabela przedstawia pliki związane z kontrolą RBAC dostępne w systemie AIX do konfigurowania i przechowywania informacji bazy danych.

Plik	Opis
/etc/nscontrol.conf	Plik sterujący usługi nazw dla różnych baz danych bezpieczeństwa
/etc/security/authorizations	Baza danych autoryzacji zdefiniowanych przez użytkownika
/etc/security/privcmds	Baza danych komend uprzywilejowanych
/etc/security/privfiles	Baza danych plików uprzywilejowanych
/etc/security/privdevs	Baza danych urządzeń uprzywilejowanych
/etc/security/roles	Baza danych ról

Korzystanie z rozszerzonego trybu RBAC w aplikacjach
Wiele aplikacji do pomyślnego działania w środowisku rozszerzonego trybu RBAC nie wymaga wprowadzania żadnych modyfikacji. Wystarczy po prostu zdefiniować autoryzację dostępu aplikacji oraz powiązane z nią uprawnienia, a następnie przypisać aplikację do bazy danych komend uprzywilejowanych.

Jednak aplikacja może używać rozszerzonego trybu RBAC, wywołując interfejsy RBAC w celu dokładniejszej kontroli nad wykonaniem komendy, a tym samym stając się bardziej bezpieczną aplikacją. Integracja aplikacji z rozszerzonym trybem RBAC przynosi korzyści w przypadku następujących aplikacji:

- Aplikacje, których użycie jest ograniczone tylko dla użytkownika root lub członków konkretnej grupy. Aplikacje te zwykle sprawdzają obowiązującą tożsamość użytkownika lub przynależność do grupy; można je zmienić, tak aby sprawdzały w zamian autoryzację.
- Aplikacje korzystające z mechanizmu włączania bitu **setuid** lub **setgid** w celu umożliwienia nieuprawnionym użytkownikom uzyskania uprawnień na czas wywołania komendy. Aplikacje te zwykle będą bardziej bezpieczne dzięki mechanizmowi zmiany zakresu uprawnień, zapewniającemu wykonywanie zadań z jak najmniejszymi uprawnieniami.

Sprawdzanie autoryzacji
Aplikacje dotąd używające identyfikatora użytkownika lub grupy użytkownika wywołującego do określenia, czy może on wykonać operacje uprzywilejowane, powinny zostać zmienione, aby sprawdzały w tym celu autoryzację.

Rozważmy na przykład aplikację wykonującą zadania konfiguracji systemu plików i umożliwiającą obecnie użytkownikowi root (UID = 0) wykonywanie niektórych operacji uprzywilejowanych:

```
if (getuid() == 0) {
            /* zezwolenie na kontynuację operacji uprzywilejowanej */
}
```

Aby aplikacja zamiast tego umożliwiała użytkownikom z konkretną autoryzacją (**aix.fs.config**) wykonywanie operacji uprzywilejowanej, można zmienić kod, aby używał funkcji API **checkauths** do sprawdzenia autoryzacji:

```
if (checkauths(“aix.fs.config", CHECK_ALL)) {
        /* zezwolenie na kontynuację operacji uprzywilejowanej */
    }
```

Funkcja **checkauths** jest włączona dla trybu "legacy mode" oraz rozszerzonej kontroli RBAC i zwraca kod powodzenia **0**, jeśli proces ją wywołujący ma żądaną autoryzację. Funkcja API **checkauths** sprawdza również, czy włączone są uprawnienia użytkownika root, a następnie w zależności od nich odpowiednio umożliwia lub uniemożliwia użytkownikowi root ominięcie sprawdzenia autoryzacji. W wersjach systemu wcześniejszych niż AIX wersja 6.1 do sprawdzenia autoryzacji były zwykle używane funkcje API **MatchAllAuths**, **MatchAnyAuths**, **MatchAllAuthsList** i **MatchAnyAuthsList**. Aplikacje udostępnione w systemie AIX wersja 6.1 i nowszych powinny w zamian używać funkcji API **checkauths** z uwagi na jej obsługę zarówno trybu "legacy mode", jak i rozszerzonej kontroli RBAC oraz możliwość wyłączenia uprawnień użytkownika root.

Podobnie jak w powyższym przykładzie, aplikacje wywołujące funkcje **getuid**, **getgid** lub zbliżone tylko w celu umożliwienia różnym użytkownikom wykonywania konkretnych zadań, można zmodyfikować, aby używały funkcji **checkauths** do sprawdzenia w zamian autoryzacji. Jeśli identyfikator sprawdzanego użytkownika lub grupy nie jest identyfikatorem użytkownika root, najpierw można użyć wywołania systemowego **sys_parm** do sprawdzenia, czy jest włączona rozszerzona kontrola RBAC. Jeśli nie, program może wywołać istniejące funkcje sprawdzania. W przeciwnym razie, jeśli rozszerzona kontrola RBAC jest włączona, program powinien sprawdzić odpowiednie autoryzacje systemowe i zdefiniowane przez użytkownika.

Zmienianie zakresu uprawnień
Aplikację zmodyfikowaną o sprawdzanie autoryzacji można dalej modyfikować, aby wykorzystać bardzo szczegółowe zmienianie zakresu uprawnień w trakcie wykonywania operacji.

Aplikacje mogą użyć funkcji API **priv_raise** do podniesienia uprawnień wymaganych do wykonania operacji i obniżyć uprawnienia funkcją API **priv_lower**. Podniesienie uprawnień bezpośrednio przed próbą wykonania operacji uprzywilejowanej i obniżanie ich po zakończeniu wykonywania tej operacji nazywa się zmianą zakresu uprawnień. Taka technika jest preferowaną metodą używania uprawnień przez aplikacje. Aby można było podnieść uprawnienie, musi ono być dostępne w maksymalnym zestawie uprawnień aplikacji w bazie danych komend uprzywilejowanych. Podniesienie uprawnienia powoduje jego umieszczenie w obowiązującym zestawie uprawnień (EPS) procesu. Obniżenie uprawnienia powoduje jego usunięcie z zestawu EPS. Poniższy kod jest przykładem zmiany zakresu uprawnień w okolicy funkcji API **auditproc**.

```
priv_raise(PV_AU_ADMIN, -1);    /* podniesienie uprawnienia, gdy jest to potrzebne */
auditproc();              /* wywołanie systemowe kontroli */
priv_lower(PV_AU_ADMIN, -1);    /* obniżenie uprawnienia */
```

Aplikacje korzystające z kontroli RBAC
Tradycyjnie w systemach AIX i systemach z włączoną przez użytkownika root rozszerzoną kontrolą RBAC użytkownik root oraz należący do niego program **z bitem setuid** (dla którego numer UID=0), który nie znajduje się w bazie danych komend uprzywilejowanych, ma zawsze nadane wszystkie uprawnienia w jądrze. Sprawdzanie uprawnień w jądrze zawsze się powiedzie, nawet jeśli żądane uprawnienie nie znajduje się w obowiązującym zestawie uprawnień (effective privilege set - EPS).

Takie zachowanie nadal musi dotyczyć istniejących aplikacji **z bitem setuid**, jednak może stanowić zagrożenie bezpieczeństwa, ponieważ program **setuid** ma wszystkie możliwości użytkownika root.

Aby umożliwić poprawne traktowanie uprawnień w procesach w systemie z kontrolą RBAC włączoną przez użytkownika root, wprowadzono nowy bit w strukturze procesu. Jeśli ten bit jest ustawiony, proces korzysta z kontroli RBAC, a efektywna wartość numeru UID wynosząca 0 nie zapewnia mu żadnych dodatkowych uprawnień. Do ustawienia tego bitu w programie służy wywołanie systemowe **proc_rbac_op**. Dowolne programy **z bitem setuid**, niewymienione w bazie danych komend uprzywilejowanych, mogą użyć tej funkcjonalności do zmniejszenia liczby słabych punktów zabezpieczeń dzięki obniżeniu dostępnych uprawnień. Należy zauważyć, że programy zdefiniowane w bazie danych komend uprzywilejowanych są automatycznie oznaczane jako procesy korzystające z kontroli RBAC i mają przypisane tylko uprawnienia wymienione w tej bazie danych.

Poniższy kod przedstawia sposób, w jaki aplikacje mogą oznaczyć, że korzystają z kontroli RBAC, a następnie otrzymać odpowiednie uprawnienia.

```
#include <userpriv.h
#include <sys/priv.h>

privg_t effpriv;

int rbac_flags = SEC_RBACAWARE;

/* Zaznaczenie, że proces korzysta z kontroli RBAC. */
proc_rbac_op(-1, PROC_RBAC_SET, &rbac_flags);

/* Ustawienie pustego obowiązującego zestawu uprawnień. */
priv_clrall(effpriv);
setppriv(-1, &effpriv, NULL, NULL, NULL);

/* Podniesienie uprawnień, gdy jest to wymagane. */
```

```
priv_raise(PV_AU_ADMIN, -1);
auditproc();

/* Obniżenie uprawnień, gdy nie są już potrzebne. */
priv_lower(PV_AU_ADMIN, -1);
```

Funkcje API RBAC

W tabeli poniżej podano dostępne w systemie funkcje API związane z kontrolą RBAC. Więcej informacji zawierają opisy konkretnych funkcji API.

API	Opis
checkauths	Porównuje przekazaną listę autoryzacji z autoryzacjami powiązanymi z bieżącym procesem.
GetUserAuths	Pobiera zestaw autoryzacji przypisany do bieżącego procesu.
MatchAllAuths, MatchAllAuthsList, MatchAnyAuths, MatchAnyAuthsList	Porównuje autoryzacje. Lepsza od powyższych funkcji API jest funkcja checkauths.
getauthattr, putauthattr	Modyfikuje autoryzacje zdefiniowane w bazie danych autoryzacji lub wysyła zapytania o te autoryzacje.
getauthattrs	Pobiera wiele atrybutów autoryzacji z bazy danych autoryzacji.
putauthattrs	Aktualizuje wiele atrybutów autoryzacji w bazie danych autoryzacji.
getcmdattr, putcmdattr	Modyfikuje w bazie danych komend uprzywilejowanych informacje dotyczące bezpieczeństwa komendy lub wysyła zapytania do tej bazy.
getcmdattrs	Pobiera wiele atrybutów komend z bazy danych komend uprzywilejowanych.
putcmdattrs	Aktualizuje wiele atrybutów komend w bazie danych komend uprzywilejowanych.
getdevattr, putdevattr	Modyfikuje w bazie danych urządzeń uprzywilejowanych informacje dotyczące bezpieczeństwa urządzenia lub wysyła zapytania do tej bazy.
getdevattrs	Pobiera wiele atrybutów urządzeń z bazy danych urządzeń uprzywilejowanych.
putdevattrs	Aktualizuje wiele atrybutów urządzeń w bazie danych urządzeń uprzywilejowanych.
getpfileattr, putpfileattr	Modyfikuje w bazie danych plików uprzywilejowanych informacje dotyczące bezpieczeństwa pliku lub wysyła zapytania do tej bazy.
getpfileattrs	Pobiera wiele atrybutów plików z bazy danych plików uprzywilejowanych.
putpfileattrs	Aktualizuje wiele atrybutów plików w bazie danych plików uprzywilejowanych.
getroleattr, putroleattr	Modyfikuje role zdefiniowane w bazie danych ról lub wysyła zapytania o te role.
getroleattrs	Pobiera wiele atrybutów ról z bazy danych ról.
putroleattrs	Aktualizuje wiele atrybutów ról w bazie danych ról.
getsecorder	Pobiera kolejność domen dla różnych baz danych bezpieczeństwa.
setsecorder	Ustawia kolejność domen dla różnych baz danych bezpieczeństwa.

Uprawnienia w systemie AIX
Uprawnienia dostępne w systemie AIX zostały wymienione w tabeli poniżej. Znajduje się w niej opis każdego uprawnienia oraz związane z nim wywołania systemowe. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkim prawa powiązane z innym uprawnieniem.

Podczas sprawdzania uprawnień system najpierw określa, czy proces ma najniższe potrzebne uprawnienie, a następnie podąża w górę hierarchii, sprawdzając, czy istnieją większe uprawnienia. Na przykład proces z uprawnieniem **PV_AU_** automatycznie ma uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** oraz **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** automatycznie ma wszystkie uprawnienia wymienione poniżej oprócz uprawnień **PV_SU_**.

Uprawnienie	**Opis**	**Odniesienie do wywołania systemowego**
PV_ROOT	Nadaje procesowi równoważnik wszystkich poniżej wymienionych uprawnień oprócz uprawnienia PV_SU_ (i dominuje nad innymi uprawnieniami).	
PV_AU_ADD	Umożliwia procesowi zarejestrowanie lub dodanie rekordu kontroli.	auditlog
PV_AU_ADMIN	Umożliwia procesowi skonfigurowanie systemu kontroli i wysyłanie do niego zapytań.	audit, auditbin, auditevents, auditobj
PV_AU_PROC	Umożliwia procesowi odczytanie lub ustawienie stanu kontroli dla procesu.	auditproc
PV_AU_READ	Umożliwia procesowi odczytanie pliku oznaczonego jako plik kontroli w modelu Trusted AIX.	
PV_AU_WRITE	Umożliwia procesowi zapisanie lub usunięcie pliku oznaczonego jako plik kontroli lub oznaczenie pliku jako plik kontroli w modelu Trusted AIX.	
PV_AU_	Odpowiada połączeniu wszystkich powyższych uprawnień kontrolnych (PV_AU_*).	
PV_AZ_ADMIN	Umożliwia procesowi modyfikowanie tabel zabezpieczeń jądra.	sec_setkst
PV_AZ_READ	Umożliwia procesowi odtwarzanie tabel zabezpieczeń jądra.	sec_getkat, sec_getkpct, sec_getkpdt, sec_getkrt itp.
PV_AZ_ROOT	Powoduje, że proces pomyślnie przechodzi kontrolę autoryzacji podczas komendy exec() (używane w celu dziedziczenia).	
PV_AZ_CHECK	Powoduje, że proces pomyślnie przechodzi wszystkie kontrole autoryzacji.	sec_checkauth
PV_DAC_R	Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących odczytu.	access, creat, accessx, open, read, faccessx, mkdir, getea, rename, statx, _sched_getparam, _sched_getscheduler, statea, listea
PV_DAC_W	Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących zapisu.	Wiele z powyższych i setea, write, symlink, _setpri, _sched_setparam,

Uprawnienie	Opis	Odniesienie do wywołania systemowego
		_sched_setscheduler, fsetea, rmdir, removeea
PV_DAC_X	Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących wykonania.	Wiele z powyższych i execve, symlink, rmdir, chdir, fchdir, ra_execve
PV_DAC_O	Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących praw własności.	chmod, utimes, setacl, revoke, mprotect
PV_DAC_UID	Umożliwia procesowi zmianę własnego identyfikatora użytkownika.	setuid, seteuid, setuidx, setreuid, ptrace64
PV_DAC_GID	Umożliwia procesowi ustawienie nowego identyfikatora grupy lub zmianę istniejącego.	setgid, setgidx, setgroups, ptrace64
PV_DAC_RID	Umożliwia procesowi ustawienie nowego identyfikatora roli lub zmianę istniejącego.	setroles, getroles
PV_DAC_	Odpowiada połączeniu wszystkich powyższych uprawnień DAC (PV_DAC_*).	
PV_FS_MOUNT	Umożliwia procesowi podłączanie i odłączanie systemu plików.	vmount, umount
PV_FS_MKNOD	Umożliwia procesowi utworzenie pliku dowolnego typu lub użycie wywołania systemowego mknod.	mknod
PV_FS_CHOWN	Umożliwia procesowi zmianę właściciela pliku.	chown, chownx, fchownx, lchown
PV_FS_QUOTA	Umożliwia procesowi zarządzanie operacjami dotyczącymi limitów pamięci dyskowej.	quotactl
PV_FS_LINKDIR	Umożliwia procesowi utworzenie dowiązania stałego do katalogu.	link, unlink, remove
PV_FS_CNTL	Umożliwia procesowi wykonywanie różnych operacji sterujących oprócz rozszerzania i zmniejszania systemu plików.	fscntl
PV_FS_RESIZE	Umożliwia procesowi wykonywanie operacji rozszerzania i zmniejszania systemu plików.	fscntl
PV_FS_CHROOT	Umożliwia procesowi zmianę własnego katalogu głównego.	chroot
PV_FS_PDMODE	Umożliwia procesowi utworzenie lub ustawienie katalogu typu partycjonowanego.	pdmkdir
PV_FS_	Odpowiada połączeniu wszystkich powyższych uprawnień systemu plików (PV_FS_*).	
PV_PROC_PRIV	Umożliwia procesowi modyfikowanie lub wyświetlanie zestawów uprawnień powiązanych z procesem.	setppriv, getppriv
PV_PROC_PRIO	Umożliwia procesowi lub wątkowi zmianę priorytetu, strategii oraz innych parametrów planowania.	_prio_requeue, _setpri, _setpriority, _getpri, _sched_setparam, _sched_setscheduler,

Uprawnienie	Opis	Odniesienie do wywołania systemowego
		_thread_setsched, thread_boostceiling, thread_setmystate, thread_setstate
PV_PROC_CORE	Umożliwia procesowi wykonanie zrzutu pamięci.	gencore
PV_PROC_RAC	Umożliwia procesowi tworzenie większej liczby procesów, niż dopuszcza limit na użytkownika.	appsetrlimit, setrlimit64, mlock, mlockall, munlock, munlockall, plock, upfget, upfput, restart, brk, sbrk
PV_PROC_RSET	Umożliwia dołączanie zestawu zasobów (rset) do procesu lub wątku.	bindprocessor, ra_attachrset, ra_detachrset, rs_registername, rs_setnameattr, rs_discardname, rs_setpartition, rs_getassociativity, kra_mmapv
PV_PROC_ENV	Umożliwia procesowi ustawienie informacji o użytkowniku w strukturze użytkowników.	ue_proc_register, ue_proc_unregister, usrinfo
PV_PROC_CKPT	Umożliwia procesowi wykonanie operacji checkpoint lub restartowania innego procesu.	setcrid, restart
PV_PROC_CRED	Umożliwia procesowi ustawianie atrybutów referencji.	__pag_setvalue, __pag_setvalue64, __pag_genpagvalue
PV_PROC_SIG	Umożliwia procesowi wysyłanie sygnału do niepowiązanego procesu.	_sigqueue, kill, signohup, gencore, thread_post, thread_post_many
PV_PROC_TIMER	Umożliwia procesowi ustawianie i używanie liczników czasu o małej granulacji.	appresabs, appresinc, absinterval, incinterval, _poll, _select _timer_settime
PV_PROC_RTCLK	Umożliwia procesowi dostęp do zegara procesora.	_clock_getres, _clock_gettime, _clock_settime, _clock_getcpuclockid
PV_PROC_VARS	Umożliwia procesowi pobieranie i aktualizowanie parametrów strojonych procesu.	smttune
PV_PROC_PDMODE	Umożliwia procesowi zmianę trybu REAL katalogu partycjonowanego.	setppdmode
PV_PROC_	Odpowiada połączeniu wszystkich powyższych uprawnień procesu (PV_PROC_*).	
PV_TCB	Umożliwia procesowi modyfikację ścieżki biblioteki zaufanej jądra.	chpriv, fchpriv
PV_TP	Wskazuje, że proces jest procesem zaufanej ścieżki i umożliwia wykonywanie działań zastrzeżonych dla procesów zaufanej ścieżki. (Równoważne uprawnieniu BYPASS_TPATH w starym systemie AIX).	

Uprawnienie	Opis	Odniesienie do wywołania systemowego
PV_WPAR_CKPT	Umożliwia procesowi wykonanie operacji checkpoint/restartu w partycji WPAR.	smcr_proc_info, smcr_exec_info, smcr_mapinfo, smcr_net_oper, smcr_procattr, aio_suspend_io, aio_resume_io
PV_KER_ACCT	Umożliwia procesowi wykonywanie operacji zastrzeżonych dla podsystemu rozliczeniowego.	acct, _acctctl, projctl
PV_KER_DR	Umożliwia procesowi wywoływanie dynamicznej rekonfiguracji.	_dr_register, _dr_notify, _dr_unregister, dr_reconfig
PV_KER_TIME	Umożliwia procesowi modyfikowanie zegara i czasu systemowego.	adjtime, appsettimer, _clock_settime
PV_KER_RAC	Umożliwia procesowi używanie dużych (niepodzielnych na strony) stron dla segmentów pamięci współużytkowanej.	shmctl, vmgetinfo
PV_KER_WLM	Umożliwia procesowi zainicjowanie i zmodyfikowanie konfiguracji WLM.	_wlm_set, _wlm_tune, _wlm_assign
PV_KER_EWLM	Umożliwia procesowi inicjowanie i wysyłanie zapytań do środowiska eWLM.	
PV_KER_VARS	Umożliwia procesowi sprawdzanie i ustawianie wykonawczych parametrów strojonych jądra.	sys_parm, getkerninfo, __pag_setname, sysconfig, kunload64
PV_KER_REBOOT	Umożliwia procesowi zamknięcie systemu.	reboot
PV_KER_RAS	Umożliwia procesowi konfigurowanie i zapisywanie rekordów RAS, rejestrowania błędów, śledzenia oraz funkcji zrzutów.	mtrace_set, mtrace_ctl
PV_KER_LVM	Umożliwia procesowi skonfigurowanie podsystemu LVM.	
PV_KER_NFS	Umożliwia procesowi skonfigurowanie podsystemu NFS.	
PV_KER_VMM	Umożliwia procesowi modyfikowanie parametrów wymiany oraz innych parametrów strojonych VMM w jądrze.	swapoff, _swapon_ext, vmgetinfo
PV_KER_WPAR	Umożliwia procesowi skonfigurowanie partycji zarządzania obciążeniem.	brand, corral_config, corral_delete, corral_modify, wpar_mkdevexport, wpar_rmdevexport, wpar_lsdevexport
PV_KER_CONF	Umożliwia procesowi wykonywanie różnych operacji związanych z konfiguracją systemu.	sethostname, sethostid, unameu, setdomainname
PV_KER_EXTCONF	Umożliwia procesowi wykonywanie różnych czynności konfiguracyjnych w rozszerzeniach jądra (dla usług rozszerzeń jądra).	
PV_KER_IPC	Umożliwia procesowi zwiększanie wartości buforu kolejki komunikatów IPC oraz	msgctl, shm_open, shmget, ra_shmget, ra_shmgetv, shmctl

Uprawnienie	Opis	Odniesienie do wywołania systemowego
	wykonywanie komendy shmget z zakresami do dołączenia.	
PV_KER_IPC_R	Umożliwia procesowi odczytywanie kolejki komunikatów IPC, zestawu semaforów oraz segmentu pamięci współużytkowanej.	msgctl, __msgrcv, _mq_open, semctl, shmat, shm_open, __semop, shmctl, __semtimedop, sem_post, _sem_wait, __msgrcv, __msgxrcv
PV_KER_IPC_W	Umożliwia procesowi zapisywanie kolejki komunikatów IPC, zestawu semaforów oraz segmentu pamięci współużytkowanej.	_mq_open, shmat, _sem_open, semctl, shm_open, shmctl, mq_unlink, sem_unlink, shm_unlink, msgctl, __msgsnd
PV_KER_IPC_O	Umożliwia procesowi przesłonięcie prawa własności DAC dla wszystkich obiektów IPC.	msgctl, semctl, shmctl, fchmod, fchown
PV_KER_SECCONFIG	Umożliwia procesowi ustawianie opcji zabezpieczeń jądra.	sec_setsecconf, sec_setrunmode, sec_setsyslab, sec_getsyslab
PV_KER_PATCH	Umożliwia procesowi wprowadzenie poprawek do rozszerzeń jądra.	
PV_KER_	Odpowiada połączeniu wszystkich powyższych uprawnień jądra (PV_KER_*).	
PV_DEV_CONFIG	Umożliwia procesowi konfigurowanie rozszerzeń jądra i urządzeń w systemie.	sysconfig
PV_DEV_LOAD	Umożliwia procesowi ładowanie do pamięci i usuwanie z pamięci rozszerzeń jądra i urządzeń w systemie.	sysconfig
PV_DEV_QUERY	Umożliwia procesowi wysyłanie zapytań do modułów jądra.	sysconfig
PV_SU_ROOT	Nadaje procesowi wszystkie uprawnienia przypisane do standardowego administratora systemu AIX.	
PV_SU_EMUL	Nadaje procesowi wszystkie uprawnienia przypisane do standardowego administratora systemu AIX, jeśli numer UID wynosi 0.	
PV_SU_UID	Powoduje, że wywołanie systemowe funkcji getuid daje w wyniku 0.	getuidx
PV_SU_	Odpowiada połączeniu wszystkich powyższych uprawnień administratora (PV_SU_*).	
PV_NET_CNTL	Umożliwia procesowi modyfikowanie tabel sieciowych.	socket, bind, listen, _naccept, econnect, ioctl, rmsock, setsockopt
PV_NET_PORT	Umożliwia procesowi dowiązania do uprzywilejowanych portów.	bind
PV_NET_RAWSOCK	Umożliwia procesowi bezpośredni dostęp do warstwy sieciowej.	socket, _send, _sendto, sendmsg, _nsendmsg

Uprawnienie	Opis	Odniesienie do wywołania systemowego
PV_NET_CONFIG	Umożliwia procesowi konfigurowanie parametrów sieciowych.	
PV_NET_	Odpowiada połączeniu wszystkich powyższych uprawnień sieciowych (PV_NET_*).	

Uprawnienia wymienione w tabeli poniżej są charakterystyczne dla modelu Trusted AIX:

Uprawnienie w modelu Trusted AIX	Opis	Odniesienie do wywołania systemowego
PV_LAB_CL	Umożliwia procesowi modyfikowanie etykiet SCL tematu, pod warunkiem kontroli procesu.	
PV_LAB_CLTL	Umożliwia procesowi modyfikowanie etykiet TCL tematu, pod warunkiem kontroli procesu.	
PV_LAB_LEF	Umożliwia procesowi odczyt pliku kodowania etykiety.	
PV_LAB_SLDG	Umożliwia procesowi obniżanie etykiet SL, pod warunkiem kontroli procesu.	
PV_LAB_SLDG_STR	Umożliwia procesowi obniżanie etykiet SL pakietu, pod warunkiem kontroli procesu.	
PV_LAB_SL_FILE	Umożliwia procesowi zmianę etykiet SL obiektu, pod warunkiem kontroli procesu.	
PV_LAB_SL_PROC	Umożliwia procesowi zmianę etykiety SL tematu, pod warunkiem kontroli procesu.	
PV_LAB_SL_SELF	Umożliwia procesowi zmianę własnej etykiety SL, pod warunkiem kontroli procesu.	
PV_LAB_SLUG	Umożliwia procesowi podnoszenie etykiet SL, pod warunkiem kontroli procesu.	
PV_LAB_SLUG_STR	Umożliwia procesowi podnoszenie etykiet SL pakietu, pod warunkiem kontroli procesu.	
PV_LAB_TL	Umożliwia procesowi modyfikowanie etykiet TL podmiotu i obiektu.	
PV_LAB_	Odpowiada połączeniu wszystkich powyższych uprawnień do etykiet (PV_LAB_*).	
PV_MAC_CL	Umożliwia procesowi ominięcie ograniczeń dotyczących kontroli czułości.	
PV_MAC_R_PROC	Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC podczas odczytywania informacji o procesie, jeśli etykieta procesu docelowego jest w zakresie kontroli działającego procesu.	
PV_MAC_W_PROC	Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC podczas wysyłania sygnału do procesu, jeśli etykieta procesu docelowego jest w zakresie kontroli działającego procesu.	

Uprawnienie w modelu Trusted AIX	Opis	Odniesienie do wywołania systemowego
PV_MAC_R	Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC.	
PV_MAC_R_CL	Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC, jeśli etykieta obiektu jest w zakresie kontroli procesu.	
PV_MAC_R_STR	Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC podczas odczytu komunikatu ze strumienia, jeśli etykieta komunikatu jest w zakresie kontroli procesu.	
PV_MAC_W	Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC.	
PV_MAC_W_CL	Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, jeśli etykieta obiektu jest w zakresie kontroli procesu.	
PV_MAC_W_DN	Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, jeśli etykieta procesu dominuje nad etykietą obiektu, a etykieta obiektu jest w zakresie kontroli procesu.	
PV_MAC_W_UP	Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, jeśli etykieta procesu jest zdominowana przez etykietę obiektu, a etykieta obiektu jest w zakresie kontroli procesu.	
PV_MAC_OVRRD	Omija ograniczenia dotyczące MAC w przypadku plików oznakowanych jako wyłączone z MAC.	
PV_MAC_	Odpowiada połączeniu wszystkich powyższych uprawnień MAC (PV_MAC_*).	
PV_MIC	Umożliwia procesowi ominięcie ograniczeń dotyczących integralności.	
PV_MIC_CL	Umożliwia procesowi ominięcie ograniczeń dotyczących kontroli integralności.	

Domenowa kontrola RBAC

Kontrola dostępu oparta na rolach (Role-based access control - RBAC) została wprowadzona w systemie AIX 6.1. Udostępnia ona mechanizm służący do rozdzielenia różnych funkcji administratora na role, które można delegować do innych użytkowników w systemie. Kontrola RBAC umożliwia delegowanie obowiązków i poprawę bezpieczeństwa systemu, ułatwiając kontrolę i śledzenie działań w systemie. Kontrola RBAC umożliwia delegację odpowiedzialności do innego użytkownika (nazywanego autoryzowanym użytkownikiem), ale nie udostępnia mechanizmu do ograniczenia uprawnień administracyjnych autoryzowanego użytkownika do konkretnych zasobów systemu. Na przykład użytkownik z uprawnieniami administracyjnymi do sieci może zarządzać wszystkimi interfejsami sieciowymi w systemie. Nie można ograniczyć uprawnień autoryzowanego użytkownika tylko do modyfikacji zbioru interfejsów.

Opcja domeny dla kontroli RBAC służy do ograniczania dostępu dla autoryzowanych użytkowników. Użytkownicy i zasoby w systemie zostają oznaczeni przez przyłączenie znaczników nazywanych domenami i konkretne reguły dostępu określają dostęp do zasobów według użytkowników.

Definicje

Z regułami dostępu są związane następujące definicje:

podmiot: podmiot jest jednostką żądającą dostępu do obiektu. Przykładem podmiotu jest proces.

obiekt: obiekt jest jednostką zawierającą informacje o wartości. Przykładami obiektów są pliki, urządzenia i porty sieciowe.

domena: domena jest zdefiniowana jako kategoria, do której należy jednostka. Jeśli jednostka należy do domeny, kontrolą dostępu do jednostki zarządzają reguły dostępu w następujący sposób:

Reguły dostępu

- Podmiot może uzyskać dostęp do obiektu, jeśli ma wszystkie domeny, do których należy obiekt. Wymaga to, aby lista domen, do których należy podmiot, była nadzbiorem domen obiektu. Jest to zachowanie domyślne.
- Podmiot może uzyskać dostęp do obiektu, jeśli ma co najmniej jedną z domen obiektu. Oznacza to, że podmiot i obiekt mają jedną wspólną domenę. Takie zachowanie zależy od opcji bezpieczeństwa obiektu.
- Dostęp do obiektu może być zabroniony dla określonych domen. Jeśli dla obiektu zostanie zdefiniowany zestaw domen nazwany zestawami konfliktów i jedna z domen podmiotu będzie należeć do zestawu konfliktów, nastąpi odmowa dostępu do obiektu dla podmiotu.

Bazy danych domen

Domeny obsługiwane przez system muszą być przechowywane w pliku konfiguracyjnym w katalogu `/etc/security/domains`. Format sekcji w pliku jest następujący:

```
domain-name:
id = <liczba>
dfltmsg = <komunikat>
msgcat = <katalog komunikatów>
msgset = <Zestaw komunikatów w katalogu>
msgnum = <Identyfikator komunikatu w katalogu>
```

Do operacji na bazie danych służą komendy **mkdom** i **chdom**. Komenda **lsdom** umożliwia wyświetlenie bazy danych. Do usuwania pozycji służy komenda **rmdom**.

Pozycje w bazie danych nie są obowiązujące, dopóki nie zostaną przesłane do jądra za pomocą komendy **setkst**.

System obsługuje maksymalnie 1024 domeny i najwyższa możliwa wartość identyfikatora domeny (atrybut `ID`) wynosi 1024.

Obiekty przypisane do domeny

Aby przypisać domenę do obiektu, należy zdefiniować go w bazie danych obiektów przypisanych do domeny. Domeny dla wszystkich jednostek w systemie są przechowywane w pliku konfiguracyjnym w katalogu `/etc/security/domobjs`. Format sekcji w pliku przedstawiono poniżej. Jest to przykład przypisania domeny do obiektu.

```
/dev/hrvg:
domains=HR,IT
conflictsets=payroll
objtype=device
secflags=FSF_DOM_ANY
```

domains: określa domeny, które mają prawo dostępu do obiektu. Przykłady domen: IT, HR i Payroll.

objtype: oznacza typ obiektu przypisywany do domeny. Rodzaje typów obiektów: device, file, netint i netport.

conflict sets: oznacza, że podmiot należący do dowolnej domeny wymienionej w tym atrybucie w tym zestawie nie ma prawa dostępu do obiektu.

secflags: ta flaga określa specjalne właściwości obiektu. Można ustawić wartość **FSF_DOM_ANY** lub **FSF_DOM_ALL**. Jeśli flaga zostanie ustawiona na wartość **FSF_DOM_ANY**, podmiot może uzyskać dostęp do obiektu, jeśli zawiera dowolną z domen określonych na liście atrybutu domains. Jeśli ta flaga zostanie ustawiona na wartość **FSF_DOM_ALL**, aby podmiot uzyskał dostęp do obiektu, musi mieć wszystkie wymienione domeny. Jeśli nie zostanie podana żadna wartość, używana jest wartość **FSF_DOM_ALL**. Flaga **secflag** dotyczy tylko zachowania atrybutu domains obiektu.

Domeny można przypisywać do plików w systemach plików. Domyślnie wszystkie domeny obiektu muszą być podzbiorem domen procesu, aby proces mógł uzyskać dostęp do obiektu.

1. Urządzenia: do domeny można przypisać wszystkie urządzenia, włącznie z systemami plików. Sprawdzenie domeny jest przeprowadzane podczas działań związanych z zarządzaniem, na przykład podczas konfigurowania urządzenia.

   ```
   /dev/hrvg:
   domains=HR,IT
   conflictsets=payroll
   objtype=device
   secflags=FSF_DOM_ANY
   ```

2. Interfejsy sieciowe: jeśli interfejsy sieciowe, na przykład en0, są przypisane do domeny, działania związane z zarządzaniem, na przykład wyłączenie interfejsu, będą wymagać wykonania dla interfejsu kontroli domeny.

   ```
   en0:
   domains=NETIF,ADMIN
   objtype=netint
   flags=FSF_DOM_ALL
   ```

3. Porty sieciowe: porty TCP i UDP można przypisać do domeny. Sprawdzenia domeny są wymuszane w momencie, gdy aplikacja próbuje powiązać port.

   ```
   TCP_<nr_portu>:
   domains=NETIF,ADMIN
   type=netport
   flags=FSF_DOM_ALL
   ```

4. Procesy: proces dziedziczy domeny użytkownika, z którego prawami jest uruchomiony. Gdy użytkownik się loguje, proces powłoki użytkownika ma domeny użytkownika. Ustawione domeny procesu pozostają niezmienione w czasie życia tego procesu. Domen procesu nie można zmienić ani interfejsem użytkownika, ani wywołaniem systemowym. Jedynym procesem, który może ustawiać domeny, jest proces logowania. Procesy nie mają atrybutów **conflict set** ani **secflags**.

Obecne ograniczenia

Poniżej przedstawiono ograniczenia domenowej kontroli RBAC:

- Konfiguracja domeny jest obecnie obsługiwana w systemie lokalnym i na serwerze LDAP (Lightweight Directory Access Protocol).
- Domeny RBAC nie są obsługiwane w obrębie partycji zarządzania obciążeniem AIX (WPAR).
- Domen RBAC nie można stosować do plików przejściowych.

Wymagania rozszerzonego trybu RBAC

Domenowa kontrola RBAC jest utworzona na podstawie rozszerzonego trybu RBAC i do działania wymaga włączenia w systemie rozszerzonego trybu RBAC.

Tabele bezpieczeństwa jądra.

Domeny i obiekty przypisane do domeny zdefiniowane w bazie danych domen i bazie danych obiektów domen są obowiązujące od momentu przesłania do jądra za pomocą komendy **setkst**. Te dwie tabele są nazywane odpowiednio tabelą domen jądra (Kernel Domain Table - KDOMT) i tabelą obiektów domen jądra (Kernel Domain Object Table - KDOT).

Dodatkowe szczegóły dotyczące tabel zabezpieczeń jądra i komendy **setkst** zawiera temat Kontrola dostępu oparta na rolach (RBAC) w podręczniku bezpieczeństwa systemu AIX.

Komendy domen

Poniższa tabela zawiera komendy związane z domenową kontrolą RBAC udostępnione w systemie operacyjnym AIX do zarządzania środowiskiem domenowej kontroli RBAC i korzystania z niego:

Komenda	Opis
mkdom	Tworzy nową domenę
lsdom	Wyświetla atrybuty domeny
rmdom	Usuwa domenę
chdom	Zmienia atrybuty domeny
setsecattr	Ustawia atrybuty bezpieczeństwa bazy danych obiektów domen
lssecattr	Wyświetla atrybuty bezpieczeństwa bazy danych obiektów domen
rmsecattr	Usuwa definicję bazy danych obiektów domen
setkst	Wysyła pozycje z baz danych na poziomie użytkownika domenowej kontroli RBAC do tabel bezpieczeństwa jądra

Pliki związane z domenową kontrolą RBAC

Poniższa tabela zawiera pliki związane z kontrolą RBAC udostępnione w systemie operacyjnym AIX do konfigurowania i przechowywania informacji o bazie danych:

Plik	Opis
/etc/security/domains	Baza danych domen
/etc/security/domobjs	Baza danych obiektów domen

Korzystanie z domen

Definiowanie domen: domeny są definiowane w bazie danych domen za pomocą komendy **mkdom**.

```
mkdom id=24 HR
```

Przypisywanie domen: domeny można przypisać do jednostek, na przykład użytkowników, plików, urządzeń, portów sieciowych i interfejsów. Wszystkie jednostki oprócz użytkowników obsługują zestawy konfliktów i opcje bezpieczeństwa (**secflags**).

Użytkownicy: użytkownicy są przypisywani do domen za pomocą komend **chuser** i **chsec**.

Składnia:

```
chuser domains = <rozdzielona przecinkami lista domen> nazwa użytkownika
```

Przykład:

```
chuser domains=INET john
```

Podczas logowania następuje aktywowanie domen przypisanych do użytkownika. W przypadku zmiany domen podczas aktywności sesji, aby nowe domeny odniosły skutek, konieczne jest ponowne zalogowanie.

Obiekty: Aby ograniczyć dostęp do obiektów za pomocą domen, obiekty muszą zostać zdefiniowane w bazie danych obiektów domen za pomocą komendy **setsecattr**.

Składnia:

```
setsecattr -o domains=<rozdzielona przecinkami lista dozwolonych domen>
conflictsets=<rozdzielona przecinkami lista domen z ograniczeniami>
secflags=<FSF_DOM_ALL lub FSF_DOM_ANY>
objtype=<file lub device lub netint lub netport>
object-path
```

Przykład:

```
setsecattr -o domains=INET,WEB conflictsets=DB secflags=FSF_DOM_ANY objtype=netint en0
```

Listy kontroli dostępu (ACL)

Zazwyczaj lista ACL składa się z serii pozycji nazywanych pozycjami ACE (Access Control Entry). Każda pozycja ACE definiuje prawa dostępu dla użytkownika będącego w relacji z obiektem.

Podczas próby dostępu system operacyjny przegląda listę ACL związaną z danym obiektem i sprawdza, czy użytkownik ma odpowiednie prawo. Listy ACL razem ze związanym z nimi sprawdzaniem dostępu tworzą jądro mechanizmu indywidualnej kontroli dostępu (Discretionary Access Control - DAC) obsługiwanego przez system AIX.

System operacyjny obsługuje kilka typów obiektów systemowych, które umożliwiają przechowywanie lub wymianę informacji przez procesy użytkownika. Najważniejszymi typami obiektów z kontrolą dostępu są:

- pliki i katalogi,
- potoki nazwane,
- obiekty IPC takie jak kolejki komunikatów, segmenty pamięci współużytkowanej i semafory.

Wszystkie sprawdzenia uprawnień dostępu dla tych obiektów są wykonywane na poziomie wywołania systemowego podczas pierwszego dostępu do obiektu. Ponieważ dostęp do obiektów komunikacji międzyprocesorowej systemu System V (SVIPC) jest bezstanowy, sprawdzenia są wykonywane przy każdym dostępie. W przypadku obiektów z nazwami systemu plików konieczne jest tłumaczenie nazwy rzeczywistego obiektu. Nazwy są tłumaczone względnie (do katalogu roboczego procesu) lub bezwzględnie (do katalogu głównego procesu). Wszystkie tłumaczenia nazw rozpoczynają się od przeszukania tych dwóch katalogów.

Mechanizm indywidualnej kontroli dostępu umożliwia efektywną kontrolę dostępu do zasobów informacyjnych i zapewnia oddzielne zabezpieczenie poufności i integralności danych. Mechanizmy kontroli dostępu na poziomie użytkownika są efektywne zależnie od tego, jak zostaną ustawione przez użytkowników. Wszyscy użytkownicy muszą rozumieć sposób przydzielania i odbierania uprawnień oraz sposób ich ustawiania.

Na przykład lista ACL powiązana z obiektem systemu plików (plikiem lub katalogiem) może określać prawa dostępu do danego obiektu dla różnych użytkowników. Istnieje możliwość zdefiniowania w liście ACL różnych poziomów praw dostępu, takich jak odczyt lub zapis, dla różnych użytkowników.

Zazwyczaj każdy obiekt będzie miał zdefiniowanego właściciela i w niektórych przypadkach będzie powiązany z grupą podstawową. Właściciel danego obiektu kontroluje jego atrybuty dostępu indywidualnego. Atrybuty właściciela są ustawiane dla efektywnego identyfikatora użytkownika, który jest właścicielem procesu tworzącego.

Przedstawiona poniżej lista zawiera atrybuty kontroli dostępu bezpośredniego dla różnych typów obiektów:

Właściciel
W przypadku obiektów komunikacji międzyprocesorowej System V (SVIPC) prawa własności może zmienić twórca lub sam właściciel. Obiekty SVIPC mają przypisanego twórcę, który ma wszystkie prawa właściciela (w tym autoryzację dostępu). Twórca nie może jednak zostać zmieniony, nawet przez użytkownika root.

Obiekty SVIPC są inicjowane z efektywnym identyfikatorem grupy procesu tworzącego. W przypadku systemów plików, atrybuty kontroli dostępu bezpośredniego są inicjowane z efektywnym identyfikatorem grupy procesu tworzącego lub identyfikatorem grupy katalogu nadrzędnego (jest on określany przez opcję dziedziczenia grupy katalogu nadrzędnego).

Grupa
Właściciel obiektu może zmienić grupę. Nowa grupa musi mieć efektywny identyfikator grupy procesu tworzącego lub identyfikator grupy katalogu nadrzędnego. (Jak powyżej, do obiektów SVIPC jest przypisana grupa tworząca, która nie może zostać zmieniona i współużytkuje autoryzację dostępu grupy obiektu).

Tryb
Za pomocą komendy **chmod** (w trybie numerycznym z notacją ósemkową) można ustawiać podstawowe uprawnienia i atrybuty. Podprogram **chmod** wywoływany przez komendę wyłącza rozszerzone uprawnienia. Rozszerzone uprawnienia zostaną wyłączone, jeśli zostanie użyty tryb numeryczny komendy **chmod** w pliku, który ma listę ACL. Tryb symboliczny komendy **chmod** powoduje wyłączenie rozszerzonych list ACL typu NSF4, ale nie powoduje wyłączenia rozszerzonych uprawnień dla list ACL typu AIXC. Informacje na temat trybu numerycznego i symbolicznego można znaleźć w dokumentacji komendy **chmod**.

Wiele obiektów systemu operacyjnego, takich jak gniazda i obiekty systemu plików, ma powiązane listy ACL dla różnych podmiotów. Szczegóły list ACL dla tych typów obiektów mogą się różnić.

Tradycyjnie system AIX w celu kontrolowania praw dostępu do obiektów systemu plików obsługiwał bity trybu. Obsługiwał także unikalną formę bitów trybu listy ACL. Taka lista ACL składała się z podstawowych bitów trybu oraz z bitów trybu dozwolonych dla definicji wielu pozycji ACE; każda pozycja ACE definiuje prawa dostępu dla użytkownika lub grupy dotyczące bitów trybu. Tego typu klasyczne listy ACL będą nadal obsługiwane i są nazywane listami ACL o typie AIXC.

Należy zauważyć, że obsługa listy ACL w obiektach systemu plików zależy od podstawowego fizycznego systemu plików (physical file system - PFS). System PFS musi rozumieć dane listy ACL i mieć możliwość przechowywania, odtwarzania i narzucania dostępu dla różnych użytkowników. Istnieje możliwość, że niektóre fizyczne systemy plików nie będą obsługiwały żadnych list ACL (mogą obsługiwać tylko podstawowe bity trybu) w przeciwieństwie do fizycznego systemu plików, który obsługuje wiele typów list ACL. Niektóre systemy plików w systemie AIX zostały rozszerzone o obsługę wielu typów list ACL. Systemy JFS2 i GPFS mają także możliwość obsługi protokołu NFS w wersji 4 w oparciu o listę ACL. Ta lista ACL jest nazywana w systemie AIX listą ACL typu NFS4. Ta lista ACL jest zgodna z większą częścią definicji listy ACL ze specyfikacji protokołu NFS w wersji 4. Obsługuje także bardziej ziarnistą kontrolę dostępu w porównaniu do listy ACL typu AIXC i zapewnia możliwość dziedziczenia.

Obsługa struktury dla różnych typów list kontroli dostępu
Począwszy od wersji 5.3.0, system AIX obsługuje infrastrukturę dla różnych typów list kontroli dostępu (Access Control List - ACL) istniejących dla różnych obiektów systemu plików znajdujących się w obrębie systemu operacyjnego.

Ta infrastruktura zapewnia jednolite metody zarządzania listami ACL bez względu na typ listy ACL związanej z obiektem. Omawiana struktura obejmuje następujące komponenty:

Komendy administrowania listami ACL
Są to następujące komendy: **aclget**, **aclput**, **acledit** , **aclconvert**, **aclgetttypes**. Komendy te wywołują interfejsy biblioteczne, które z kolei wywołują moduły dla danego typu listy ACL.

Interfejsy biblioteczne list ACL
Interfejsy biblioteczne list ACL umożliwiają dostęp aplikacji do list ACL.

dynamicznie ładowane moduły list ACL dla konkretnego typu listy ACL
System operacyjny AIX udostępnia zestaw modułów przeznaczonych dla konkretnych typów list ACL: listy ACL AIX Classic (**AIXC**) i listy ACL NFS4 (**nfs4**).

Kompatybilność binarna
Problemy z kompatybilnością nie występują w przypadku aplikacji uruchamianych na istniejących systemach plików JFS2 z listami ACL systemu AIX lub bez tych list.

Jednak należy zauważyć, że aplikacje mogą nie uzyskać dostępu do plików, jeśli natrafią na obiekty systemu plików z bardziej wymagającymi listami (takimi jak NFS4). Proste sprawdzenie, czy plik istnieje, będzie wymagało poziomu uprawnień do odczytu na liście ACL typu NFS4.

Typy list kontroli dostępu obsługiwane w systemie operacyjnym AIX
System operacyjny AIX aktualnie obsługuje typy list ACL AIXC i NFS4.

Jak już wspomniano, obsługuje także infrastrukturę dla wszystkich pozostałych typów list ACL obsługiwanych przez podstawowy fizyczny system plików. Należy zauważyć, że fizyczny system plików JFS2 obsługuje listę ACL NFS4 w trybie rodzimym, jeśli instancja systemu plików tworzona jest za pomocą opcji Extended Attributes, wersja 2.

Lista kontroli dostępu typu AIXC
Typ AIXC listy kontroli dostępu reprezentuje zachowanie typu listy ACL obsługiwanej w wydaniach systemu AIX wcześniejszych niż 5.3.0. Listy ACL w systemie AIXC zawierają uprawnienia podstawowe i rozszerzone.

Typ AIXC listy kontroli dostępu (ACL) reprezentuje zachowanie typu listy ACL obsługiwanej w wydaniach systemu AIX wcześniejszych niż 5.3.0. Listy ACL w systemie AIXC zawierają uprawnienia podstawowe i rozszerzone. W systemie plików JFS2 maksymalna wielkość listy ACL typu AIXC to 4 kB.

Ustawianie uprawnień podstawowych dla listy ACL typu AIXC

Uprawnienia podstawowe to tradycyjne tryby dostępu do pliku przypisane do właściciela, grupy i innych użytkowników. Tryby dostępu to: odczyt (r), zapis (w) i przeszukiwanie/wykonywanie (x).

Na liście ACL uprawnienia podstawowe mają następujący format, w którym parametr *Mode* jest wyrażony w postaci rwx (przy czym nieokreślone uprawnienie jest zastępowane myślnikiem):

```
base permissions:
   owner(name): Mode
   group(group): Mode
   others: Mode
```

Ustawianie atrybutów dla listy ACL typu AIXC

Do listy ACL typu AIXC można dodać następujące atrybuty:

setuid (SUID)
Bit trybu Set-user-ID (ustaw ID użytkownika). Ten atrybut powoduje, że zarówno efektywny, jak i zapisany ID użytkownika, który jest właścicielem procesu, są takie same, jak ID właściciela uruchomionego pliku.

setgid (SGID)
Bit trybu Set-group-ID (ustaw ID grupy). Ten atrybut powoduje, że zarówno efektywny, jak i zapisany ID grupy, która jest właścicielem procesu, są takie same, jak ID grupy uruchomionego pliku.

savetext (SVTX)
W przypadku katalogów określa, że tylko właściciele pliku mogą tworzyć i usuwać dowiązania do plików w określonym katalogu.

Te atrybuty są dodawane w formacie opisanym poniżej.

```
attributes: SUID, SGID, SVTX
```

Ustawianie uprawnień rozszerzonych dla listy ACL typu AIXC

Uprawnienia rozszerzone umożliwiają właścicielowi pliku bardziej precyzyjne zdefiniowanie dostępu do tego pliku. Uprawnienia rozszerzone modyfikują podstawowe uprawnienia do pliku (właściciela, grupy, innych) przez nadawanie, odbieranie i określanie trybów dostępu dla poszczególnych użytkowników, grup lub kombinacji grup i użytkowników. Uprawnienia są modyfikowane przez użycie słów kluczowych.

Słowa kluczowe **permit**, **deny** i **specify** są definiowane w następujący sposób:

permit
Przyznaje użytkownikowi lub grupie określone prawa dostępu do pliku

deny
Uniemożliwia użytkownikowi lub grupie użycie określonego dostępu do pliku

specify
Precyzyjnie definiuje dostęp do pliku dla użytkownika lub grupy

Jeśli użytkownik ma odebrane określone prawa przez słowo kluczowe **deny** lub **specify**, żaden inny wpis nie może tego zmienić.

Aby możliwe było stosowanie uprawnień rozszerzonych, w liście ACL należy podać słowo kluczowe **enabled**. Wartością domyślną jest słowo kluczowe **disabled**.

W liście ACL uprawnienia rozszerzone mają następujący format:

```
extended permissions:
  enabled | disabled
    permit   Mode  UserInfo...
    deny     Mode  UserInfo...
    specify  Mode  UserInfo...
```

Należy użyć oddzielnych wierszy dla każdego wpisu **permit**, **deny** lub **specify**. Parametr *Mode* jest wyrażany jako **rwx** (przy czym nieokreślone uprawnienie jest zastępowane myślnikiem). Parametr *UserInfo* jest wyrażany jako u:NazwaUżytkownika, g:NazwaGrupy, lub jako rozdzielona przecinkiem kombinacja u:NazwaUżytkownika i g:NazwaGrupy.

Uwaga: Jeśli w pozycji zostanie podanych kilka nazw użytkowników, nie będzie można jej użyć do podjęcia decyzji związanej z kontrolą dostępu, ponieważ proces ma tylko jeden identyfikator użytkownika.

Tekstowa reprezentacja listy ACL typu AIXC

Następująca sekcja pokazuje postać tekstową listy ACL typu AIXC:

```
Attributes:  { SUID | SGID | SVTX }
Base Permissions:
   owner(name): Mode
   group(group): Mode
   others: Mode
Extended Permissions:
   enabled | disabled
     permit   Mode  UserInfo...
     deny     Mode  UserInfo...
     specify  Mode  UserInfo...
```

Format binarny listy ACL typu AIXC

Format binarny listy ACL typu AIXC jest zdefiniowany w pliku /usr/include/sys/acl.h i został zaimplementowany w bieżącym wydaniu systemu AIX.

Przykład listy ACL typu AIXC

Poniżej znajduje się przykładowa lista ACL typu AIXC:

```
attributes: SUID
base permissions:
      owner(frank):  rw-
      group(system): r-x
      others: ---
extended permissions:
      enabled
        permit  rw-  u:dhs
        deny    r--  u:chas, g:system
        specify r--  u:john, g:gateway, g:mail
        permit  rw-  g:account, g:finance
```

Pozycje listy ACL są następujące:

- Pierwszy wiersz wskazuje, że bit **setuid** jest włączony.
- Kolejny wiersz, który wprowadza uprawnienia podstawowe, jest opcjonalny.
- Następne trzy wiersze określają uprawnienia podstawowe. Nazwy właściciela i grupy są umieszczone w nawiasach tylko dla celów informacyjnych. Zmiana tych nazw nie powoduje zmiany właściciela pliku lub grupy pliku. Jedynie komenda **chown** i **chgrp** może zmienić te atrybuty plików.
- Kolejny wiersz, który wprowadza uprawnienia rozszerzone, jest opcjonalny.
- Kolejny wiersz określa, że uprawnienia rozszerzone zostały włączone.
- Ostatnie cztery wiersze są pozycjami rozszerzonymi. Pierwsza pozycja rozszerzona przyznaje użytkownikowi *dhs* uprawnienie odczytu (r) i zapisu (w) do pliku.

- Druga pozycja odbiera użytkownikowi *chas* dostęp do odczytu (r), tylko gdy jest on członkiem grupy *system*.
- Trzecia pozycja rozszerzona określa, że dopóki użytkownik *john* jest członkiem grupy *gateway* i grupy *mail*, ma prawo dostępu do odczytu (r). Jeśli użytkownik *john* nie jest członkiem obu grup, to uprawnienie rozszerzone nie jest przydzielane.
- Ostatnia pozycja rozszerzona przyznaje każdemu użytkownikowi, który należy do *obu* grup, *account* i *finance*, uprawnienia do odczytu (r) i zapisu (w).

  Uwaga: Do procesu, który żąda dostępu do obiektu kontrolowanego, można zastosować kilka pozycji rozszerzonych, przy czym wpisy odbierające uprawnienia mają pierwszeństwo nad wpisami przydzielającymi uprawnienia.

Opis pełnej składni znajduje się w opisie komendy **acledit** w podręczniku *Commands Reference*.

Lista kontroli dostępu typu NFS4

System AIX obsługuje także listy kontroli dostępu (ACL) typu NFS4.

Typ NFS4 listy ACL implementuje kontrolę dostępu zgodnie ze specyfikacją, którą zawiera dokument *Network File System (NFS) version 4 Protocol RFC 3530*. W systemie plików JFS2 maksymalna wielkość listy ACL typu NFS4 to 64 kB.

Listy ACL NFS V4 są obsługiwane tylko przez klienta NFS V4. Listy NFS V4 nie są obsługiwane przez Cachefs ani Proxy.

Tekstowa reprezentacja listy ACL typu NFS4

Tekstowa lista ACL typu NFS V4 jest listą pozycji ACE (pozycje kontroli dostępu), w której jedna pozycja znajduje się w jednym wierszu. Pozycja ACE zawiera cztery elementy w formacie opisanym poniżej.

```
IDENTITY    ACE_TYPE      ACE_MASK     ACE_FLAGS

gdzie:
IDENTITY => ma format 'IDENTITY_type:(IDENTITY_name lub IDENTITY_ID lub IDENTITY_who):'
         gdzie:
         IDENTITY_type => Jeden z następujących typów tożsamości:
                  u : użytkownik
                  g : grupa
                  s : specjalny łańcuch who (IDENTITY_who musi być specjalnym łańcuchem who)
                          IDENTITY_name => nazwa użytkownika/grupy
                          IDENTITY_ID   => identyfikator użytkownika/grupy
                          IDENTITY_who  => specjalny łańcuch who (np. OWNER@, GROUP@, EVERYONE@)
ACE_TYPE => jeden z następujących typów pozycji ACE:
                a : allow
                d : deny
                l : alarm
                u : audit
ACE MASK => jeden lub więcej z następujących kluczy wartości maski bez separatora:
                r : READ_DATA            lub LIST_DIRECTORY
                w : WRITE_DATA      lub ADD_FILE
                p : APPEND_DATA     lub ADD_SUBDIRECTORY
                R : READ_NAMED_ATTRS
                W : WRITE_NAMED_ATTRS
                x : EXECUTE         lub SEARCH_DIRECTORY
                D : DELETE_CHILD
                a : READ_ATTRIBUTES
                A : WRITE_ATTRIBUTES
                d : DELETE
                c : READ_ACL
                C : WRITE_ACL
                o : WRITE_OWNER
                s : SYNCHRONIZE
ACE_FLAGS (opcjonalnie) => jeden lub więcej kluczy atrybutu bez separatora:
                fi : FILE_INHERIT
                di : DIRECTORY_INHERIT
                oi : INHERIT_ONLY
                ni : NO_PROPAGATE_INHERIT
                sf : SUCCESSFUL_ACCESS_ACE_FLAG
                ff : FAILED_ACCESS_ACE_FLAG
```

Uwaga: System AIX nie podejmuje żadnych działań związanych z kluczem wartości maski Ace_Mask SYNCHRONIZE (s). System operacyjny AIX przechowuje i zachowuje klucz wartości s, ale nie ma on żadnego znaczenia dla systemu AIX.

Gdy maska Ace_Mask WRITE_OWNER jest ustawiona na typ Ace_Type `allow`, użytkownicy mogą zmieniać prawo własności pliku tylko na siebie.

Usunięcie pliku zależy od dwóch pozycji ACE: pozycji DELETE obiektu przeznaczonego do usunięcia i pozycji DELETE_CHILD jego katalogu macierzystego. System operacyjny AIX udostępnia użytkownikowi dwa tryby zachowania. W trybie *bezpiecznym* pozycja DELETE pełni rolę podobną do list ACL AIXC. W trybie *kompatybilności* pozycja DELETE pełni rolę podobną do innych głównych implementacji list ACL NFS4. Aby włączyć tryb kompatybilności, użyj komendy **chdev**:

```
chdev -l sys0 -a nfs4_acl_compat=compatible
```

Po uruchomieniu komendy **chdev** należy restartować system, aby zmiana konfiguracji została uwzględniona.

Jeśli system jest przełączany między tymi dwoma trybami, należy pamiętać, że listy ACL NFS4 wygenerowane przez system operacyjny AIX w trybie bezpiecznym mogą nie być akceptowane przez inne platformy, nawet jeśli przywrócono tryb kompatybilności w systemie.

```
Przykład:
        u:user1(aa@ibm.com):     a    rwp    fidi
        *s:(OWNER@):             d    x      dini          * Ten wiersz jest komentarzem
        g:staff(jj@jj.com):      a    rx
        s:(GROUP@):              a    rwpx   fioi
        u:2:                     d    r     di             * Ten wiersz pokazuje użytkownika bin (uid=2)
        g:7:                     a    ac    fi             * Ten wiersz pokazuje grupę security (gid=7)
        s:(EVERYONE@):           a    rca   ni
```

Format binarny listy ACL typu NFS4

Format binarny listy ACL typu NFS4 jest zdefiniowany w pliku `/usr/include/sys/acl.h` i został zaimplementowany w bieżącym wydaniu systemu AIX.

Przykład listy ACL typu NFS4

Następujący przykład pokazuje listę ACL w systemie NFS4 zainstalowaną próbnie w katalogu (na przykład w `j2eav2/d0`):

```
s:(OWNER@):         a         rwpRWxDdo         difi         * pierwsza pozycja ACE
s:(OWNER@):         d         D                 difi         * druga pozycja ACE
s:(GROUP@):         d         x                 ni           * trzecia pozycja ACE
s:(GROUP@):         a         rx                difi         * czwarta pozycja ACE
s:(EVERYONE@):      a         c                 difi         * piąta pozycja ACE
s:(EVERYONE@):      d         C                 difi         * szósta pozycja ACE
u:user1:            a         wp                oi           * siódma pozycja ACE
g:grp1:             d         wp                             * ósma pozycja ACE
u:101:              a         C                              * dziewiąta pozycja ACE
g:100:              d         c                              * dziesiąta pozycja  ACE
```

Pozycje listy ACL są następujące:

- Pierwsza pozycja ACE wskazuje, że właściciel ma następujące uprawnienia do katalogu `/j2eav2/d0` oraz do wszystkich obiektów potomnych utworzonych po zastosowaniu tej listy ACL.
  - READ_DATA (= LIST_DIRECTORY)
  - WRITE_DATA (=ADD_FILE)
  - APPEND_DATA (= ADD_SUBDIRECTORY)
  - READ_NAMED_ATTR
  - WRITE_NAMED_ATTR
  - EXECUTE (=SEARCH_DIRECTORY)
  - DELETE_CHILD
  - DELETE
  - WRITE_OWNER

- Druga pozycja ACE wskazuje, że właściciel ma odebrane uprawnienia DELETE_CHILD (usuwanie plików lub podkatalogów utworzonych poniżej katalogu /j2eav2), lecz nadal może je usuwać, ponieważ w pierwszej pozycji ACE nadano właścicielowi uprawnienia DELETE_CHILD.
- Trzecia pozycja ACE wskazuje, że wszyscy członkowie grupy mają odebrane uprawnienia EXECUTE (=SEARCH_DIRECTORY) do obiektu /j2eav2/d0, lecz właściciel nadal ma to uprawnienie określone w pierwszej pozycji ACE. Ta pozycja ACE nie może być przekazywana na wszystkie pozycje potomne, ponieważ została podana opcja NO_PROPAGATE_INHERIT. Pozycja ta ma zastosowanie tylko do katalogu /j2eav2/d0 oraz do jego bezpośrednich plików i katalogów potomnych.
- Czwarta pozycja ACE wskazuje, że każdy członek grupy obiektów (/j2eav2/d0) ma uprawnienie READ_DATA (= LIST_DIRECTORY) oraz EXECUTE (=SEARCH_DIRECTORY) do katalogu /j2eav2/d0 i jego wszystkich obiektów potomnych. Jednak trzecia pozycja ACE sprawia, że członkowie grupy (z wyjątkiem właściciela) nie mają uprawnienia EXECUTE (=SEARCH_DIRECTORY) do katalogu /j2eav2/d0 oraz jego bezpośrednich plików i podkatalogów potomnych.
- Piąta pozycja ACE wskazuje, że wszyscy użytkownicy mają uprawnienie READ_ACL do katalogu /j2eav2/d0 oraz do wszystkich jego obiektów potomnych utworzonych po zastosowaniu tej listy ACL.
- Szósta pozycja ACE wskazuje, że wszyscy użytkownicy mają odebrane uprawnienie WRITE_ACL do katalogu /j2eav2/d0 i wszystkich jego obiektów potomnych. W listach ACL w systemie NFS4 właściciel ma zawsze uprawnienie WRITE_ACL do plików i katalogów.
- Siódma pozycja ACE wskazuje, że użytkownik user1 ma uprawnienia WRITE_DATA (=ADD_FILE) i APPEND_DATA (= ADD_SUBDIRECTORY) do wszystkich obiektów potomnych katalogu /j2eav2/d0, ale nie do samego katalogu /j2eav2/d0.
- Ósma pozycja ACE wskazuje, że wszyscy członkowie grupy grp1 mają odebrane uprawnienia WRITE_DATA (=ADD_FILE) i APPEND_DATA (= ADD_SUBDIRECTORY). Pozycja ta nie ma zastosowania do właściciela, nawet jeśli jest członkiem grupy grp1, ze względu na pierwszą pozycję ACE.
- Dziewiąta pozycja ACE wskazuje, że użytkownik **UID 101** ma uprawnienia WRITE_ACL, ale nikt, z wyjątkiem właściciela, nie ma uprawnienia WRITE_ACL (ze względu na szóstą pozycję ACE).
- Dziesiąta pozycja ACE wskazuje, że wszyscy członkowie grupy **GID 100** mają odebrane uprawnienia READ_ACL, ale wszyscy członkowie tej grupy mają to uprawnienie - ze względu na piątą pozycję ACE.

Zarządzanie listami kontroli dostępu (ACL)
Do wyświetlania list ACL i ich ustawiania można użyć komend.

Programiści aplikacji i podsystemów mogą używać interfejsów bibliotecznych list ACL i procedur konwersji list ACL opisanych w poniższej sekcji.

Komendy administrowania listami ACL

Do pracy z listami ACL dla obiektu systemu plików można używać następujących komend:

aclget
Zapisuje do standardowego pliku wyjściowego listę ACL dla obiektu systemu plików o nazwie *obiekt_pliku* w czytelnym formacie, lub zapisuje ją do pliku wyjściowego o nazwie *plik_wyjściowy_ACL*.

aclput
Ustawia listę ACL dla obiektu *obiekt_pliku* w systemie plików przy użyciu wejścia standardowego lub pliku *plik_wejściowy_ACL*.

acledit
Uruchamia edytor w celu edytowania listy ACL wybranego obiektu *obiekt_pliku* .

aclconvert
Dokonuje konwersji listy ACL z jednego typu na inny. Komenda ta nie działa, jeśli konwersja nie jest obsługiwana.

aclgettypes
Pobiera typy list ACL obsługiwanych przez ścieżkę systemu plików.

Interfejsy biblioteczne list ACL

Interfejsy biblioteczne list ACL umożliwiają dostęp aplikacji do list ACL. Aplikacje (w tym również podane powyżej ogólne komendy administrowania listami ACL) nie wywołują bezpośrednio nieudokumentowanych procedur systemowych list ACL, lecz poprzez interfejsy biblioteczne uzyskują dostęp do ogólnych procedur systemowych i ładowalnych modułów zależnych od typu. Chroni to programistów aplikacji klienta przed wystąpieniem problemów z używaniem ładowalnych modułów oraz zmniejsza liczbę problemów związanych ze wsteczną kompatybilnością binarną dla przyszłych wydań systemu AIX.

Następujące interfejsy biblioteczne wywołują procedury systemowe.

aclx_fget i aclx_get
Funkcje **aclx_get** i **aclx_fget** pobierają informacje kontroli dostępu dla obiektu systemu plików i umieszczają je w regionie pamięci określonym przez **acl**. Rozmiar i typ informacji listy **acl** jest zapisany w zmiennych ***acl_sz** i ***acl_type**.

aclx_fput i aclx_put
Funkcje **aclx_put** i **aclx_fput** zapisują informacje kontroli dostępu podane w **acl** dla obiektu pliku wejściowego. Funkcje te nie dokonują konwersji typu listy ACL; aby przeprowadzić taką konwersję, należy jawnie wywołać funkcję konwersji **aclx_convert**.

aclx_gettypes
Funkcja **aclx_gettypes** pobiera listę typów list ACL obsługiwanych w konkretnym systemie plików. Jeden system plików może jednocześnie obsługiwać wiele typów list ACL. Każdy obiekt systemu plików jest skojarzony z unikalnym typem ACL należącym do listy typów list ACL obsługiwanych przez system plików.

aclx_gettypeinfo
Funkcja **aclx_gettypeinfo** pobiera parametry i możliwości typu listy ACL w określonym przez ścieżkę systemie plików. Należy zwrócić uwagę, że parametry listy ACL mają typ struktury danych, który jest uzależniony od konkretnego typu listy ACL. Struktura danych używana w listach ACL typu AIXC i NFS4 jest opisana w odrębnym dokumencie.

aclx_print i aclx_printStr
Obie te funkcje dokonują konwersji listy ACL w podanym formacie binarnym do postaci tekstowej. Funkcje te są wywoływane przez komendy **aclget** i **acledit**.

aclx_scan i aclx_scanStr
Funkcje te dokonują konwersji podanej postaci tekstowej listy ACL na format binarny.

aclx_convert
Dokonuje konwersji listy ACL z jednego typu na inny. Funkcja ta jest używana do niejawnej konwersji przy użyciu komend, takich jak **cp**, **mv** lub **tar**.

Konwersja listy ACL

Konwersja listy ACL umożliwia zmianę typu listy ACL. Obsługa wielu typów list ACL jest uzależniona od typu listy ACL w konkretnym fizycznym systemie plików. Żaden system plików nie obsługuje wszystkich typów list ACL. Na przykład jeden system plików może obsługiwać tylko listy ACL typu AIXC, a drugi system plików może obsługiwać zarówno listy ACL typu AIXC, jak i NFS4. Można kopiować listy ACL AIXC pomiędzy dwoma systemami plików, ale aby skopiować listę ACL typu NFS z jednego systemu do drugiego, należy dokonać konwersji listy ACL. Konwersja listy ACL chroni informacje kontroli dostępu w maksymalnie możliwym stopniu.

Uwaga: Proces konwersji jest procesem przybliżonym i może doprowadzić do utraty danych. Należy to uwzględnić, planując dokonanie konwersji listy ACL.

Konwersja listy ACL w systemie operacyjnym AIX jest obsługiwana przy użyciu następującej infrastruktury:

procedury biblioteczne
Procedury te wraz ze strukturą list ACL na poziomie użytkownika umożliwiają dokonanie konwersji listy ACL z jednego typu listy na inny.

komenda aclconvert
Komenda ta dokonuje konwersji list ACL.

komendy aclput i acledit
Komendy te są używane do modyfikowania typów list ACL.

komendy cp i mv
Komendy te zostały udostępnione w celu obsługi wielu typów list ACL i wykonywania - w razie potrzeby - wewnętrznych konwersji list ACL.

komenda backup
Komenda ta dokonuje konwersji informacji listy ACL do znanego typu i postaci (lista ACL typu AIXC), jeśli istnieje potrzeba utworzenia kopii zapasowej we wcześniejszym formacie. Aby pobrać listę ACL w jej formacie rodzimym, należy podać opcję **-U**. Więcej informacji zawiera opis komendy backup.

Każdy typ listy ACL jest unikalny i szczegółowe maski list kontroli dostępu różnych typów znacznie się różnią. Algorytmy konwersji są przybliżone i nie dają tego samego wyniku, co ręczna konwersja listy ACL. W niektórych przypadkach konwersja nie jest dokładna. Na przykład nie można wykonać dokładnej konwersji list ACL typu NFS4 na listy ACL typu AIXC, ponieważ listy ACL typu NFS4 udostępniają do 16 masek dostępu i mają opcję dziedziczenia, która nie jest obsługiwana w listach ACL typu AIXC. Nie należy używać funkcji konwersji list ACL i interfejsów, jeśli nie można dopuścić do utraty informacji kontroli dostępu.

Uwaga: Algorytmy konwersji list ACL są z natury przybliżone i są nadal udoskonalane.

Bity S i listy kontroli dostępu

Użytkownik ma możliwość użycia programów **setuid** i **setgid** oraz zastosowania bitów S do list ACL.

Używanie programów setuid i setgid

Mechanizm bitów uprawnień umożliwia efektywną kontrolę dostępu do zasobów w większości sytuacji. W celu uzyskania bardziej precyzyjnej kontroli dostępu, system operacyjny udostępnia programy **setuid** i **setgid**.

System operacyjny AIX definiuje tożsamość tylko w stosunku do identyfikatorów użytkowników i grup. Typy list ACL, które nie definiują tożsamości z identyfikatorami użytkowników i grup, są odwzorowywane do modelu tożsamości AIX. Na przykład typ NFS4 listy ACL definiuje tożsamość użytkownika jako łańcuch w postaci użytkownik@domena i łańcuch ten jest odwzorowywany na liczbowe identyfikatory użytkowników i grup.

Większość programów jest uruchamiana z prawami dostępu użytkownika i grupy, takimi jakie posiada użytkownik je wywołujący. Właściciele programów mogą przypisać prawa dostępu użytkownika, który je wykonuje, przez utworzenie programu jako **setuid** lub **setgid**, to znaczy, ustawić bit setuid lub setgid. Gdy taki program zostanie uruchomiony przez proces, proces uzyska prawa dostępu właściciela programu. Program **setuid** jest wykonywany z prawami dostępu jego właściciela, zaś program **setgid** ma prawa dostępu jego grupy, a oba bity mogą zostać ustawione w zależności od mechanizmu uprawnień.

Mimo iż proces ma przypisane dodatkowe prawa dostępu, są one kontrolowane przez program, który je posiada. Z tego względu programy **setuid** i **setgid** umożliwiają kontrolę dostępu programowaną przez użytkownika, w której prawa dostępu są przyznawane w sposób niebezpośredni. Program zachowuje się jak zaufany podsystem, strzegący praw dostępu użytkownika.

Mimo iż programy te mogą być używane z dużą skutecznością, istnieje ryzyko naruszenia bezpieczeństwa, jeśli nie zostaną one zaprojektowane uważnie. W szczególności program nie może nigdy zwracać sterowania do użytkownika, jeśli ma prawa dostępu właściciela, ponieważ umożliwiłoby to użytkownikowi nieograniczone wykorzystanie praw właściciela.

Uwaga: Ze względów bezpieczeństwa system operacyjny nie obsługuje wywołań programu **setuid** i **setgid** w skrypcie powłoki.

Zastosowanie bitów S do list ACL

Listy ACL typu NFS4 nie obsługują bitów S bezpośrednio. Listy ACL typu NFS4 nie określają, w jaki sposób te bity mogą być stosowane jako część listy. W systemie operacyjnym AIX ten problem został rozwiązany

w taki sposób, że bity S będą używane podczas przeprowadzania sprawdzania praw dostępu i będą spełniały warunki dostępu związane z każdą listą ACL typu NFS4. Do ustawienia lub zresetowania bitów S obiektów systemu plików z listami ACL typu NFS4 może być użyta komenda **chmod** dostarczana z systemem operacyjnym AIX.

Administracyjne prawa dostępu
System operacyjny zapewnia uprzywilejowane prawa dostępu dla celów administracji systemu.

Uprawnienie systemowe bazuje na identyfikatorze użytkownika i grupy. Użytkownicy z efektywnym identyfikatorem użytkownika lub grupy równym 0 są uważani za uprzywilejowanych.

Procesy z efektywnym identyfikatorem użytkownika równym 0 nazywane są procesami użytkownika root i mogą:

- odczytywać i zapisywać dowolny obiekt,
- wywoływać dowolną funkcję systemową,
- wykonywać określone operacje sterowania podsystemami, wykonując programy **setuid-root**.

Można zarządzać systemem za pomocą dwóch typów uprawnień: uprawnień komendy **su** i uprawnień programu **setuid-root**. Komenda **su** powoduje, że wszystkie wywoływane programy działają jako procesy użytkownika root. Komenda **su** stanowi elastyczny, ale niezbyt bezpieczny sposób zarządzania systemem.

Utworzenie programu jako programu **setuid-root** oznacza, że jest to program z ustawionym bitem setuid, którego posiadaczem jest użytkownik root. Program **setuid-root** oferuje funkcje administracyjne, które zwykły użytkownik może wykonać bez naruszania bezpieczeństwa; przywileje są umieszczone w programie, a nie są przyznawane bezpośrednio użytkownikowi. Może być trudno umieścić wszystkie wymagane funkcje administracyjne w programach **setuid-root**, ale jest to bezpieczniejszy sposób dla menedżerów systemu.

Autoryzacja dostępu
Gdy użytkownik loguje się na konto (za pomocą komend **login** lub **su**), identyfikator użytkownika i grupy przydzielony do konta jest przypisywany do procesów użytkownika. Te identyfikatory określają prawa dostępu procesu.

Proces z identyfikatorem użytkownika równym 0 jest znany jako *proces użytkownika root*. Procesy użytkowników root mają ogólnie przyznane pełne prawa dostępu. Jeśli jednak proces użytkownika żąda uprawnień do wykonywania programu, dostęp jest udzielany tylko wtedy, gdy uprawnienie wykonywania jest przyznane przynajmniej jednemu z użytkowników.

Autoryzacja dostępu dla list ACL typu AIXC

Właściciel zasobu informacyjnego jest odpowiedzialny za zarządzanie prawami dostępu. Zasoby są chronione przez *bity uprawnień*, które są uwzględnione w trybie obiektu. Bity uprawnień definiują uprawnienia dostępu przydzielane właścicielowi obiektu, grupie obiektu i domyślnej klasie `others`. System operacyjny obsługuje trzy różne typy dostępu (odczyt, zapis, wykonywanie), które można przydzielać oddzielnie.

W przypadku plików, katalogów, potoków nazwanych i urządzeń (plików specjalnych), dostęp jest autoryzowany w następujący sposób:

- Dla każdej pozycji kontroli dostępu (ACE) na liście ACL, lista identyfikatorów jest porównywana do identyfikatorów procesu. Jeśli są zgodne, proces otrzymuje uprawnienia i ograniczenia zdefiniowane dla tej pozycji. Dla każdej zgodnej pozycji na liście ACL obliczane są sumy logiczne uprawnień i ograniczeń. Jeśli proces żądający nie jest zgodny z żadną pozycją na liście ACL, otrzymuje on uprawnienia i ograniczenia pozycji domyślnej.
- Jeśli żądany tryb dostępu jest przyznany (uwzględniony w sumie uprawnień) i nie jest zabroniony (uwzględniony w sumie ograniczeń), dostęp jest przyznawany. W przeciwnym razie dostęp jest zabroniony.

Lista identyfikatorów ACL jest zgodna z procesem, jeśli wszystkie identyfikatory na liście są zgodne z odpowiadającymi im typami efektywnych identyfikatorów dla procesu żądającego. Identyfikator o typie użytkownik jest zgodny z efektywnym identyfikatorem użytkownika, a identyfikator o typie grupa jest

zgodny z efektywnym identyfikatorem grupy procesu lub z jednym z identyfikatorów grupy uzupełniającej. Na przykład pozycja ACE z listą identyfikatorów o następującej postaci:

```
USER:fred, GROUP:philosophers, GROUP:software_programmer
```

będzie zgodna z procesem o efektywnym identyfikatorze użytkownika równym *fred* i grupą ustawioną na:

```
philosophers, philanthropists, software_programmer, doc_design
```

ale nie będzie zgodna z procesem o efektywnym identyfikatorze użytkownika równym *fred* i grupą ustawioną na:

```
philosophers, iconoclasts, hardware_developer, graphic_design
```

Należy zwrócić uwagę, że pozycja ACE z listą identyfikatorów o następującej postaci będzie zgodna z oboma procesami:

```
USER:fred, GROUP:philosophers
```

Innymi słowy, lista identyfikatorów w pozycji ACE jest zbiorem warunków, które muszą być spełnione, aby określone prawo dostępu zostało przyznane.

Wszystkie sprawdzenia uprawnień dostępu dla tych obiektów są wykonywane na poziomie wywołania systemowego podczas pierwszego dostępu do obiektu. Ponieważ dostęp do obiektów komunikacji międzyprocesorowej systemu System V (SVIPC) jest bezstanowy, sprawdzenia są wykonywane przy każdym dostępie. W przypadku obiektów z nazwami systemu plików konieczne jest tłumaczenie nazwy rzeczywistego obiektu. Nazwy są tłumaczone względnie (do katalogu roboczego procesu) lub bezwzględnie (do katalogu głównego procesu). Wszystkie tłumaczenia nazw rozpoczynają się od przeszukania tych dwóch katalogów.

Mechanizm indywidualnej kontroli dostępu umożliwia efektywną kontrolę dostępu do zasobów informacyjnych i zapewnia oddzielne zabezpieczenie poufności i integralności danych. Mechanizmy kontroli dostępu na poziomie użytkownika są efektywne zależnie od tego, jak zostaną ustawione przez użytkowników. Wszyscy użytkownicy muszą rozumieć sposób przydzielania i odbierania uprawnień oraz sposób ich ustawiania.

Autoryzacja dostępu dla list ACL typu NFS4

Dowolny użytkownik, który ma uprawnienie `WRITE_ACL`, może sterować prawami dostępu. Właściciel zasobu informacyjnego zawsze ma uprawnienie `WRITE_ACL`. Dla plików i katalogów z listami ACL typu NFS4, dostęp jest autoryzowany następująco:

- Lista pozycji ACE jest przetwarzana kolejno i zostaną przetworzone tylko te pozycje ACE, które mają wartość "who" (np. tożsamość) zgodną z wartością requestera. Wiarygodność requestera nie jest sprawdzana podczas przetwarzania pozycji ACE z wartością specjalną 'who' równą EVERYONE@.
- Każda pozycja ACE jest przetwarzana, dopóki wszystkie bity dostępu requestera nie zostaną dopuszczone. Po dopuszczeniu bit nie jest już brany pod uwagę podczas przetwarzania następnych pozycji ACE.
- Jeśli jakiś bit odpowiadający dostępowi requestera nie zostanie dopuszczony, nastąpi odmowa dostępu i pozostałe pozycje ACE nie będą przetwarzane.
- Jeśli żaden z bitów dostępu requestera nie zostanie dopuszczony i nie ma już żadnych pozycji ACE do przetworzenia, nastąpi odmowa dostępu.

Jeśli nastąpi odmowa żądanego dostępu na podstawie pozycji ACE oraz żądającym użytkownikiem jest administrator lub użytkownik root, ogólnie dostęp będzie możliwy. Należy zwrócić uwagę, że właściciel obiektu ma zawsze uprawnienia `READ_ACL`, `WRITE_ACL`, `READ_ATTRIBUTES` i `WRITE_ATTRIBUTES`. Więcej informacji na temat algorytmów autoryzacji dostępu zawiera sekcja “Lista kontroli dostępu typu NFS4” na stronie 127.

Rozwiązywanie problemów dotyczących list kontroli dostępu

Poniższe informacje można wykorzystywać podczas rozwiązywania problemów dotyczących list kontroli dostępu (ACL).

Nie powiodło się zastosowanie listy ACL typu NFS4 do obiektu

Podczas rozwiązywania problemów z ustawianiem listy ACL typu NFS4 dla obiektu, takiego jak plik lub katalog, można użyć kodów powrotu lub narzędzia śledzenia. W obu metodach do znalezienia przyczyny problemu używane są komendy **aclput** i **acledit**.

Używanie kodów powrotu do rozwiązywania problemów

Aby wyświetlić kod powrotu, należy użyć komendy `echo $?` po wykonaniu komendy **aclput**. Następująca lista pokazuje kody powrotu oraz ich wyjaśnienia:

22 (EINVAL, zdefiniowany w /usr/include/sys/errno.h)
Przyczyny wystąpienia tego kodu mogą być następujące:

- Niepoprawny format tekstowy w jednym z czterech pól.
- Wielkość wejściowej listy ACL typu NFS4 przekracza 64 KB.
- Lista ACL jest stosowana do pliku, który ma już przynajmniej jedną pozycję ACE z maską ACE ustawioną na `w` (`WRITE_DATA`), ale nie ma pozycji `p` (`APPEND_DATA`) lub ma pozycję `p` (`APPEND_DATA`), ale nie ma pozycji `w` (`WRITE_DATA`).
- Lista ACL została zastosowana do katalogu, który ma już przynajmniej jedną pozycję ACE z maską ACE ustawioną na `w` (`WRITE_DATA`), ale nie ma pozycji `p` (`APPEND_DATA`) lub ma pozycję `p` (`APPEND_DATA`), ale nie ma pozycji `w` (`WRITE_DATA`) i opcja pozycji ACE jest ustawiona na `fi` (`FILE_INHERIT`).
- Istnieje przynajmniej jedna pozycja ACE, dla której **who** (**tożsamość**) ma wartość specjalną OWNER@, i przynajmniej dla jednej maski pozycji ACE ustawionej na `c` (`READ_ACL`), `C` (`WRITE_ACL`), `a` (`READ_ATTRIBUTE`) lub `A` (`WRITE_ATTRIBUTE`) odmówiono dostępu przy użyciu pozycji ACE typu `d`.

124 (ENOTSUP, zdefiniowany w /usr/include/sys/errno.h)
Przyczyny wystąpienia tego kodu mogą być następujące:

- Wartość specjalna who w jednej z pozycji ACE nie jest jedną z trzech wartości: `OWNER@`, `GROUP@` lub `EVERYONE@`.
- Istnieje przynajmniej jedna pozycja ACE z typem ACE `u` (`AUDIT`) lub `l` (`ALARM`).

13 (EACCES, zdefiniowany w /usr/include/sys/errno.h)
Przyczyny wystąpienia tego kodu mogą być następujące:

- Użytkownik nie jest uprawniony do odczytu pliku wejściowego zawierającego pozycje ACE typu NFS4.
- Użytkownik nie jest uprawniony do wyszukania katalogu macierzystego obiektu docelowego, ponieważ nie ma uprawnień `x` (`EXECUTE`) do katalogu macierzystego obiektu docelowego.
- Użytkownik nie jest uprawniony do zapisu lub zmiany listy ACL. Jeśli obiekt jest już skojarzony z listą ACL typu NFS4, użytkownik musi mieć uprawnienie `C` (`WRITE_ACL`) do maski pozycji ACE.

Używanie narzędzia śledzenia do rozwiązywania problemów

Można także utworzyć raport śledzenia w celu znalezienia przyczyny problemu. Następujący scenariusz pokazuje sposób, w jaki należy używać śledzenia do znalezienia przyczyny problemu podczas stosowania listy ACL typu NFS4. W tym przypadku plik `/j2v2/file1` zawiera następującą listę ACL typu NFS4:

```
s:(EVERYONE@):  a       acC
```

Następująca lista ACL jest zawarta w pliku wejściowym `input_acl_file`:

```
s:(EVERYONE@):  a       rwxacC
```

W celu rozwiązania problemu przy użyciu narzędzia śledzenia:

1. Przy użyciu poniższych komend uruchom śledzenie komend **aclput** i **trcrpt**:

   ```
   $ trace -j  478 -o trc.raw
   $->!aclput -i input_acl_file -t NFS4 /j2v2/file1
   $ ->quit
   $ trcrpt trc.raw > trc.rpt
   ```

2. Zanalizuj raport śledzenia. Podczas stosowania listy ACL do pliku lub katalogu, najpierw sprawdzane jest uprawnienie do zapisu lub zmiany listy ACL, a następnie lista ACL jest stosowana. Plik zawiera wiersze podobne do następujących:

   ```
   478 xxx  xxx  ACL ENGINE: chk_access entry: type=NFS4 obj_mode=33587200 size=68 ops=16384 uid=100

   478 xxx  xxx  ACL ENGINE: chk_access exit: type=NFS4 rc=0 ops=16384 priv=0 against=0
   478 xxx  xxx  ACL ENGINE: set_acl entry: type=NFS4 ctl_flg=2 obj_mode=33587200 mode=0 size=48

   478 xxx  xxx  ACL ENGINE: validate_acl: type=NFS4 rc=22 ace_cnt=1 acl_len=48 size=12
   478 xxx  xxx  ACL ENGINE: set_acl exit: type=NFS4 rc=22 obj_mode=33587200 size=68 cmd=536878912
   ```

   Drugi wiersz zawierający `chk_access exit` wskazuje, że jest dozwolony (`rc = 0`) zapis listy ACL. Czwarty wiersz, zawierający parametr `validate_acl`, oraz piąty wiersz, zawierający parametr `set_acl exit`, wskazują, że lista ACL nie została zastosowana pomyślnie (`rc=22` wskazują **EINVAL**). Czwarty wiersz zawierający `validate_acl` wskazuje, że wystąpił problem w pierwszym wierszu pozycji ACE (`ace_cnt=1`). Po sprawdzeniu pierwszej pozycji ACE `s:(EVERYONE@): a rwxacC`) okazuje się, że brak w niej **p** jako maski dostępu. Maska **p** jest wymagana łącznie z **w** podczas stosowania listy ACL.

Rozwiązywanie problemów dotyczących odmowy dostępu

Operacja w systemie plików (na przykład zapis lub odczyt) może się nie powieść na obiekcie skojarzonym z listą ACL typu NFS4. Zwykle zostaje wówczas wyświetlony komunikat o błędzie, lecz komunikat ten nie zawiera informacji wystarczających do określenia problemu. Do znalezienia przyczyny problemu można użyć narzędzia śledzenia. Na przykład, gdy z plikiem `/j2v2/plik2` jest skojarzona następująca lista ACL typu NFS4:

```
s:(EVERYONE@):  a       rwpx
```

Następująca komenda zgłasza błąd "Brak uprawnień":

```
ls -l /j2v2/plik2
```

W celu rozwiązania problemu:

1. Uruchom śledzenie `ls -l /j2v2/plik2` i trcrpt przy użyciu następujących komend:

   ```
   $ trace -j  478 -o trc.raw
   $->!ls -l /j2v2/file2
   $ ->quit
   $ trcrpt trc.raw > trc.rpt
   ```

2. Zanalizuj raport śledzenia. Plik zawiera wiersze podobne do następujących:

   ```
   478  xxx  xxx  ACL ENGINE: chk_access entry: type=NFS4 obj_mode=33587711 size=68 ops=1024 uid=100
   478  xxx  xxx   ACL ENGINE: nfs4_chk_access_self: type=NFS4 aceN=1 aceCnt=1 req=128 deny=0
   478  xxx  xxx   ACL ENGINE: nfs4_mask_privcheck: type=NFS4 deny=128 priv=128
   478  xxx  xxx   ACL ENGINE: chk_access exit: type=NFS4 rc=13 ops=1024 priv=0 against=0
   ```

   Trzeci wiersz wskazuje, że nastąpiła odmowa dostępu dla `access mask = 128` (**0x80**), który jest tylko READ_ATTRIBUTES (patrz plik `/usr/include/sys/acl.h`).

Kontrola - przegląd

Podsystem kontrolujący pozwala na rejestrowanie informacji dotyczących bezpieczeństwa, które mogą być później analizowane przez administratorów systemu w celu wykrycia potencjalnych i rzeczywistych naruszeń systemowych strategii bezpieczeństwa.

Podsystem kontrolujący

Podsystem kontrolujący realizuje funkcje wykrywania, gromadzenia i przetwarzania.

- “Wykrywanie zdarzeń kontrolowanych” na stronie 136
- “Zbieranie informacji o zdarzeniach” na stronie 136
- “Przetwarzanie informacji zapisu kontrolnego” na stronie 137

Wszystkie wymienione powyżej funkcje mogą być skonfigurowane przez administratora systemu.

Wykrywanie zdarzeń kontrolowanych

Wykrywanie zdarzeń jest realizowane przez Zaufaną Bazę Przetwarzania (Trusted Computing Base - TCB) zarówno w jądrze (kod stanu nadzorcy), jak i w programach zaufanych (kod stanu użytkownika). Zdarzeniem kontrolowanym jest każde, mające miejsce w systemie, zdarzenie dotyczące bezpieczeństwa. Zdarzeniem dotyczącym bezpieczeństwa jest każda zmiana stanu zabezpieczeń systemu i usiłowane lub rzeczywiste naruszenie w systemie praw dostępu albo strategii bezpieczeństwa kont bądź też obie te sytuacje. Programy i moduły jądra, które wykryją zdarzenia kontrolowane, są odpowiedzialne za ich zgłoszenie do systemowego programu protokołującego kontroli. Program ten jest uruchamiany jako część jądra, a dostęp do niego można uzyskać za pomocą podprocedury (w przypadku kontroli programów zaufanych) lub za pomocą wywołania procedury jądra (w przypadku kontroli stanu nadzorcy). Zgłoszone informacje zawierają nazwę zdarzenia kontrolowanego, informację o tym, czy zdarzenie zostało pomyślnie wykonane, oraz dodatkowe informacje dotyczące zdarzenia, które są istotne dla kontroli zabezpieczeń.

Proces konfigurowania wykrywania zdarzeń obejmuje włączenie lub wyłączenie wykrywania zdarzeń i wskazanie zdarzeń, które mają być kontrolowane w przypadku poszczególnych użytkowników. Aby aktywować wykrywanie zdarzeń, należy użyć komendy **audit**, która umożliwia włączenie i wyłączenie podsystemu kontrolującego. Informacje o zdarzeniach i użytkownikach badanych przez podsystem kontrolujący zawiera plik `/etc/security/audit/config`.

Zbieranie informacji o zdarzeniach

Zbieranie informacji obejmuje protokołowanie wybranych zdarzeń kontrolowanych. Funkcję tę pełni program protokołujący kontroli jądra, który udostępnia zarówno interfejs wywołań systemowych, jak i wywołań procedur wewnątrz jądra, umożliwiający zapisywanie zdarzeń kontrolowanych.

Program protokołujący kontroli jest odpowiedzialny za utworzenie pełnego rekordu kontroli składającego się z nagłówka kontroli, który zawiera informacje charakterystyczne dla wszystkich zdarzeń (nazwa zdarzenia, użytkownik odpowiedzialny za to zdarzenie, godzina i status powrotu zdarzenia) i z zapisu kontrolnego, który zawiera informacje charakterystyczne dla konkretnego zdarzenia. Program protokołujący kontroli dołącza kolejne rekordy do zapisu kontrolnego jądra. Zapis może odbywać się w jednym lub w obu poniższych trybach:

Tryb binarny (BIN)
Zapis jest wykonywany do zmieniających się plików umożliwiających bezpieczne długoterminowe przechowywanie danych.

Tryb strumieniowy (STREAM)
Zapis jest wykonywany do cyklicznego buforu, który jest synchronicznie odczytywany za pomocą pseudourządzenia kontroli. Odpowiedź w trybie strumieniowym jest natychmiastowa.

Zbieranie informacji można skonfigurować zarówno od strony użytkownika (zapisywanie zdarzeń), jak i od strony zaplecza (przetwarzanie zapisu). Zapisywanie zdarzeń dla poszczególnych użytkowników definiuje

się oddzielnie. Dla każdego użytkownika istnieje zdefiniowany zestaw zdarzeń kontrolowanych, których wystąpienie jest protokołowane w zapisie kontrolnym. Po stronie zaplecza można indywidualnie konfigurować tryby, co umożliwia administratorowi zaimplementowanie przetwarzania zaplecza najbardziej dopasowanego do konkretnego środowiska. Ponadto kontrolę w trybie binarnym można skonfigurować w sposób umożliwiający generowanie alertów w sytuacji, gdy obszar systemu plików przeznaczony na cele kontroli staje się zbyt mały.

Przetwarzanie informacji zapisu kontrolnego

W systemie operacyjnym dostępnych jest wiele opcji umożliwiających przetwarzanie zapisu kontrolnego jądra. Zapis w trybie binarnym można kompresować, filtrować lub formatować go, aby uzyskać odpowiednie dane wyjściowe. Można też wykonywać dowolną poprawną kombinację tych operacji przed ewentualnym archiwizowaniem zapisów kontrolnych. Kompresja jest realizowana za pomocą kodowania Huffmana. Filtrowanie wykonuje się, używając wyboru rekordów kontroli w języku podobnym do standardu SQL (za pomocą komendy **auditselect**). Język ten umożliwia wybiórcze przeglądanie i przechowywanie zapisów kontrolnych. Formatowania rekordów zapisów kontrolnych można użyć w celu sprawdzenia zapisu kontrolnego, tworzenia okresowych raportów dotyczących bezpieczeństwa i drukowania zapisu kontrolnego.

Tryb strumieniowy zapisu kontrolnego można monitorować w czasie rzeczywistym, dzięki czemu możliwe jest ciągłe monitorowanie zagrożeń. Konfigurowanie tych opcji jest wykonywane przez osobne programy, które można wywołać jako procesy demona umożliwiające filtrowanie zapisów w trybie binarnym i strumieniowym. Oczywiście niektóre programy filtrujące są lepiej od innych dopasowane do danego trybu.

Konfigurowanie podsystemu kontrolującego

Podsystem kontrolujący używa globalnej zmiennej stanu, za pomocą której można określić, czy podsystem ten jest włączony. Ponadto każdy proces używa lokalnej zmiennej stanu, która określa, czy podsystem kontrolujący powinien zapisywać informacje dotyczące tego procesu.

Obie wymienione zmienne określają, czy zdarzenia są wykrywane przez programy i moduły bazy TCB. Wyłączenie kontroli realizowanej przez bazę TCB dla konkretnego procesu umożliwia procesowi wykonanie własnej kontroli, a jednocześnie nie jest pomijana strategia systemowa. Jeśli pozwolimy zaufanemu programowi na własną kontrolę, umożliwiamy efektywniejsze zbieranie informacji.

Zbieranie informacji przez podsystem kontrolujący

Zbieranie informacji dotyczy trybów wyboru zdarzeń i zapisu kontrolnego jądra. Zapisywanie jest wykonywane przez procedurę jądra udostępniającą interfejsy do protokołowania informacji, które są używane przez komponenty TCB wykrywające zdarzenia kontrolowane oraz interfejsy konfigurowania używane przez podsystem kontrolujący do sterowania procedurą protokołowania kontroli.

Protokołowanie kontroli

Zdarzenia kontrolowane są protokołowane przez interfejsy stanu użytkownika i stanu nadzorcy. Należący do bazy TCB interfejs stanu użytkownika używa podprocedury **auditlog** lub **auditwrite**, podczas gdy należący do tej bazy interfejs stanu nadzorcy używa zestawu wywołań procedur jądra.

Program protokołujący zdarzenia kontrolowane dodaje do nagłówka kontroli każdego rekordu informacje dotyczące konkretnego zdarzenia. Nagłówek ten identyfikuje użytkownika i proces, których dotyczy kontrola tego zdarzenia, oraz czas wystąpienia zdarzenia. Kod, który wykrył zdarzenie, udostępnia typ zdarzenia i jego kod powrotu lub status oraz opcjonalnie dodatkowe informacje dotyczące konkretnego zdarzenia (zawarte w zapisie zdarzenia). Informacje dotyczące konkretnego zdarzenia zawierają nazwy obiektów (na przykład pliki, do których odmówiono dostępu lub urządzenie tty używane podczas niepomyślnych prób zalogowania się), parametry podprocedur i inne zmodyfikowane informacje.

Zdarzenia są definiowane w sposób symboliczny, a nie numeryczny. Ogranicza to możliwość powstania kolizji nazw bez konieczności używania schematu rejestrowania zdarzeń. Zapisywanie zdarzeń za pomocą numerów jest trudne, ponieważ podprocedury są kontrolowane, a rozszerzalna definicja jądra nie ma

stałych numerów komutowanych obwodów wirtualnych (SVC). Każde rozszerzenie lub ponowne zdefiniowanie interfejsu jądra wymagałoby modyfikacji i protokołowania odwzorowania numerów.

Format rekordu kontroli

Rekordy kontroli składają się ze wspólnego nagłówka, po którym umieszczone są zapisy kontrolne dotyczące konkretnego zdarzenia. Struktury nagłówków są zdefiniowane w pliku `/usr/include/sys/audit.h`. Format informacji w zapisach kontrolnych zależy od charakteru zdarzenia. Jest określony w pliku `/etc/security/audit/events`.

Informacje znajdujące się w nagłówku kontroli są zbierane zazwyczaj przez procedurę protokołowania, dzięki czemu są one dokładne. Informacje znajdujące się w zapisach kontrolnych są natomiast dostarczane przez kod, który wykrył dane zdarzenie. Program protokołujący kontroli nie zna struktury ani semantyki zapisów kontrolnych. Na przykład, jeśli komenda **login** wykryje nieudaną próbę zalogowania się, odnotowuje to konkretne zdarzenie wraz z terminalem, na którym miało ono miejsce, a następnie umieszcza te informacje w zapisie kontrolnym, używając podprocedury **auditlog**. Komponent jądra programu protokołującego kontroli zapisuje w nagłówku informacje dotyczące podmiotów (identyfikatory użytkowników, identyfikatory procesów, czas wystąpienia zdarzenia) i dołącza je do pozostałych informacji. Program wywołujący jedynie udostępnia nagłówkowi nazwę zdarzenia i pola wynikowe.

Konfigurowanie programu protokołującego kontroli

Program protokołujący kontroli jest odpowiedzialny za skonstruowanie pełnego rekordu kontroli. Należy wybrać zdarzenia kontrolowane, które mają być protokołowane.

Wybór zdarzeń kontrolowanych

Typy zdarzeń kontrolowanych:

Kontrola poszczególnych procesów
Aby wybrać zdarzenia procesów, administrator systemu może zdefiniować klasy kontroli. Klasa kontroli jest podzbiorem podstawowych zdarzeń kontrolowanych dostępnych w systemie. Klasy kontroli są wygodnym sposobem logicznego pogrupowania podstawowych zdarzeń kontrolowanych.

Dla każdego użytkownika w systemie administrator systemu definiuje zbiór klas kontroli, który określa podstawowe zdarzenia przeznaczone do protokołowania dla tego użytkownika. Do każdego procesu uruchomionego przez użytkownika przypisywana jest klasa kontroli.

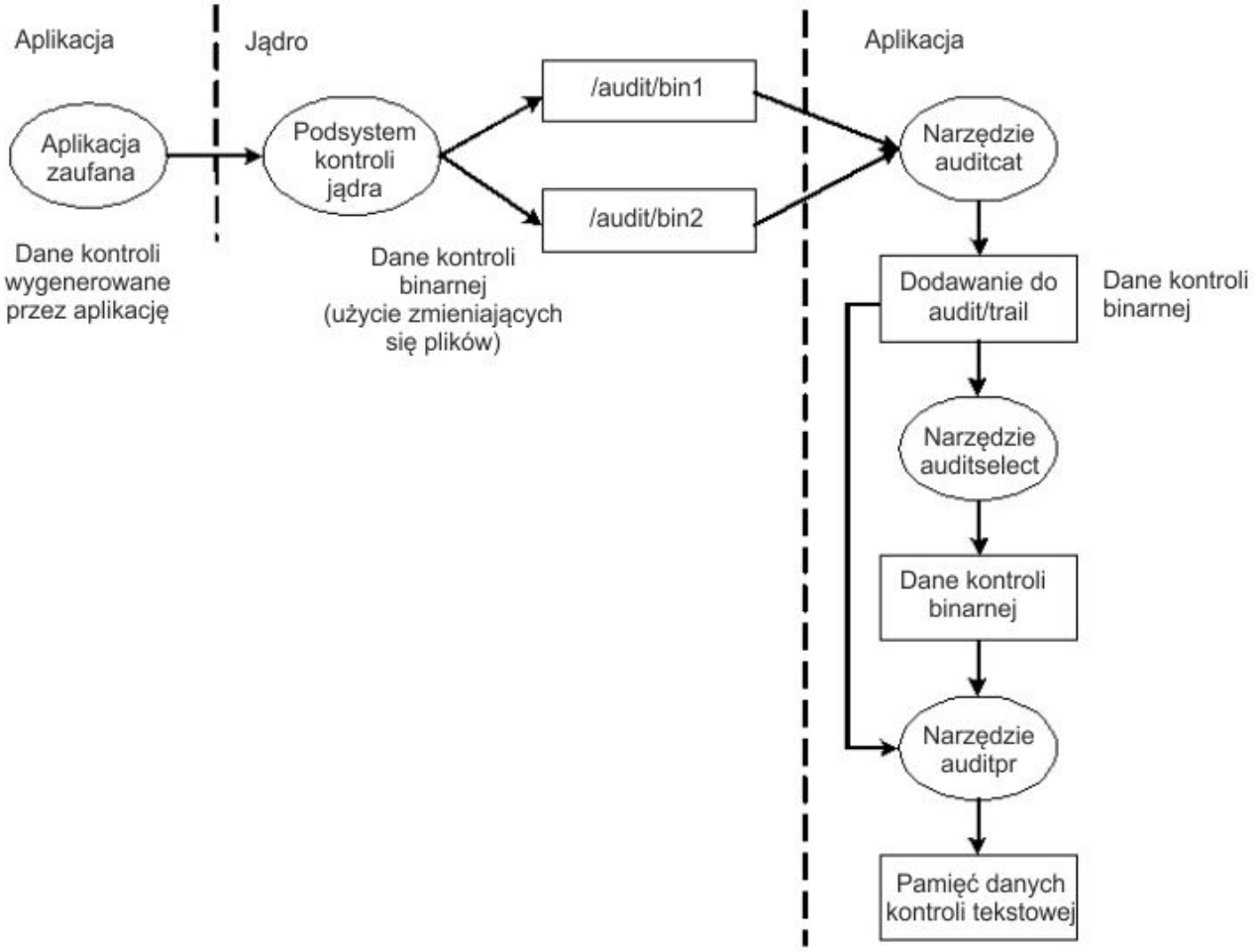
Kontrola poszczególnych obiektów
System operacyjny zapewnia kontrolę dostępu do obiektów za pomocą nazw, tzn. kontrolowane są konkretne obiekty (zwykle są to pliki). Kontrola obiektów za pomocą nazw chroni przed koniecznością kontroli wszystkich dostępów do obiektów i umożliwia kontrolę tylko niektórych wybranych obiektów. Ponadto można określić tryb kontroli, dzięki czemu zapisywane są jedynie dostępy o określonym trybie (odczyt/zapis/wykonanie).

Tryby zapisu kontrolnego jądra

Tryb protokołowania jądra można ustawić na binarny (BIN) lub strumieniowy (STREAM). W ten sposób definiuje się miejsce rejestrowania zapisu kontrolnego jądra. Jeśli używany jest tryb binarny, dla programu protokołującego kontroli jądra należy podać (przed rozpoczęciem kontroli) co najmniej jeden deskryptor pliku, do którego mają być dołączane rekordy.

W trybie binarnym rekordy kontroli są zapisywane do zmieniających się plików. Podczas uruchamiania kontroli do jądra są przekazywane dwa deskryptory plików i ich zalecana maksymalna wielkość binarna. Proces wywołujący przechodzi w tryb zawieszenia i rozpoczyna się zapisywanie rekordów kontroli do pierwszego deskryptora pliku. Gdy wielkość pierwszego pliku binarnego osiągnie maksimum i jeśli drugi deskryptor pliku jest poprawny, następuje przełączenie do drugiego pliku binarnego i reaktywacja procesu wywołującego. Jądro kontynuuje zapis do drugiego pliku binarnego do momentu ponownego wywołania tego jądra wraz z kolejnym poprawnym deskryptorem pliku. Jeśli w tym momencie drugi plik binarny jest pełny, następuje przełączenie do pliku pierwszego, a proces wywołujący jest natychmiast zwracany. W przeciwnym razie proces wywołujący jest zawieszany, a jądro kontynuuje zapisywanie rekordów do

drugiego pliku binarnego do momentu jego zapełnienia. Przetwarzanie jest wykonywane w ten sposób do momentu, kiedy zostanie wyłączone. Poniższy rysunek przedstawia działanie binarnego trybu kontroli.

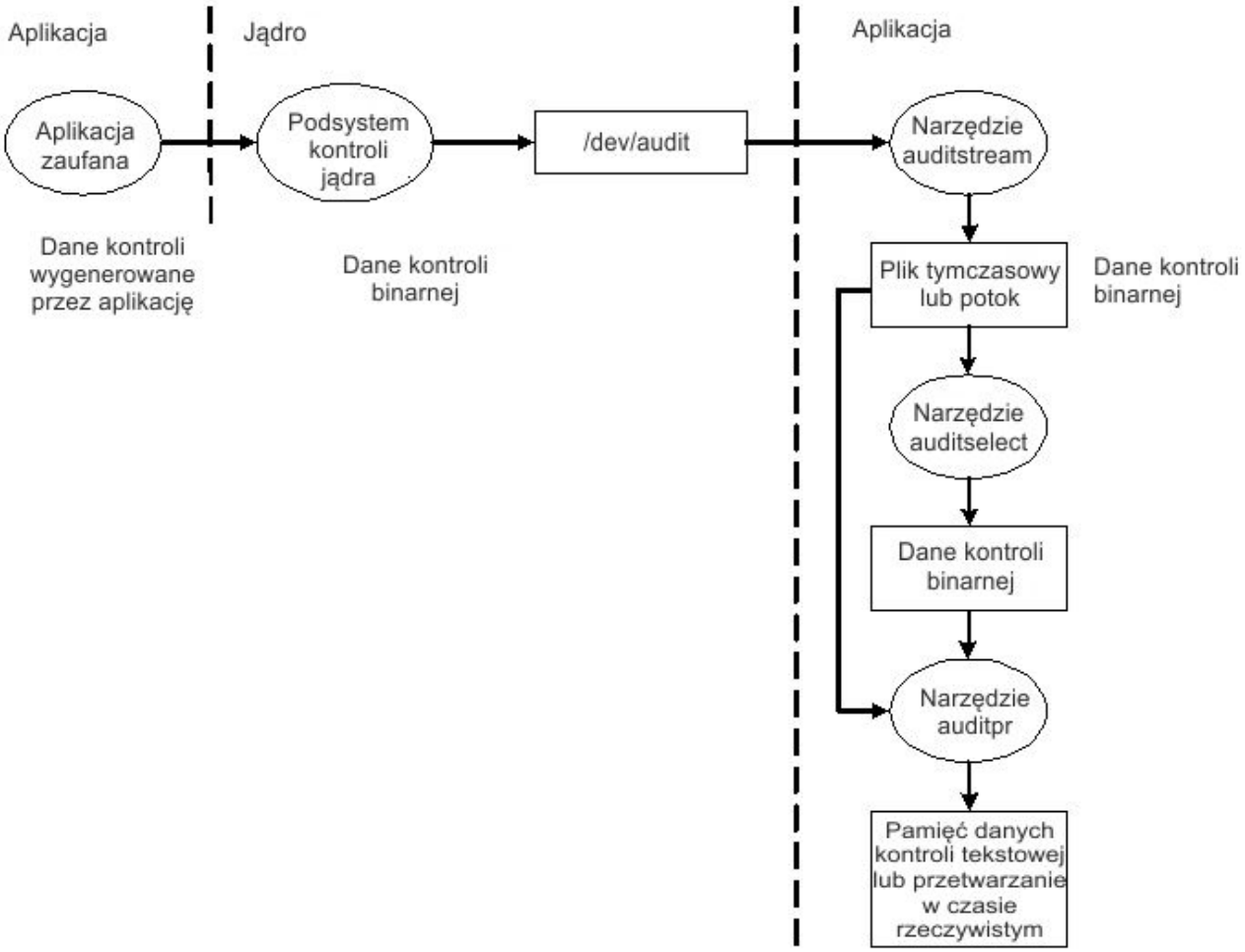


Rysunek 1. Proces trybu kontroli BIN

Mechanizm przełączania plików binarnych zapewnia, że podsystem kontroli zawsze będzie mógł gdzieś zapisywać dane, podczas gdy rekordy kontroli są w międzyczasie przetwarzane. Jeśli podsystem binarny przełącza się do drugiego pliku binarnego, usuwa zawartość pierwszego pliku, umieszczając ją w pliku `trace`. Gdy podsystem z powrotem przełącza się do pierwszego pliku binarnego, jest on już dostępny. Przechowywanie i analiza danych są więc oddzielone od ich generowania. Zwykle do odczytu danych z pliku binarnego, do którego w danej chwili jądro nie zapisuje danych, używany jest program **auditcat**. Aby zapewnić, że w systemie nigdy nie zabraknie pamięci dla zapisu kontrolnego (dane wyjściowe programu **auditcat**), w pliku `/etc/security/audit/config` można podać parametr *freespace*. Gdy w systemie będzie mniej 512-bajtowych bloków, niż podano w tym parametrze, wygenerowany zostanie komunikat syslog.

Jeśli kontrola jest włączona, parametr *binmode* w sekcji `start` w pliku `/etc/security/audit/config` powinien być ustawiony na `panic`. Parametr *freespace* w sekcji `bin` powinien być ustawiony na wartość równą co najmniej 25% miejsca na dysku przeznaczonego na przechowywanie zapisów kontrolnych. Parametry *bytethreshold* i *binsize* powinny być ustawione na 65 536 bajtów.

W trybie strumieniowym (STREAM) jądro zapisuje rekordy do buforu cyklicznego. Po osiągnięciu końca buforu następuje powrót na jego początek. Procesy odczytują informacje za pomocą pseudourządzenia o nazwie `/dev/audit`. Gdy proces otwiera pseudourządzenie, tworzony jest kanał dla tego procesu. Opcjonalnie zdarzenia, które mają być odczytywane w tym kanale, można podać w postaci listy klas kontroli. Poniższy rysunek przedstawia działanie strumieniowego trybu kontroli.



Rysunek 2. Proces trybu kontroli STREAM

Głównym celem trybu strumieniowego jest umożliwienie okresowego odczytu zapisu kontrolnego, co jest wymagane podczas monitorowania zagrożeń w czasie rzeczywistym. Innym zastosowaniem jest utworzenie zapisu, który jest zapisywany natychmiast, co uniemożliwia ewentualne zafałszowanie zapisu kontrolnego. Fałszowanie takiego zapisu jest możliwe, jeśli zapis jest przechowywany na niektórych nośnikach umożliwiających zapis.

Kolejną metodą używania trybu strumieniowego jest zapis strumienia kontroli do programu przechowującego informacje kontroli na zdalnym systemie, co umożliwia centralne przetwarzanie i jednoczesne zabezpieczenie informacji kontroli przed sfałszowaniem na hoście, z którego pochodzą.

Przetwarzanie rekordów kontroli

Do przetwarzania rekordów kontroli zapisywanych w trybie binarnym i strumieniowym można użyć komend **auditselect**, **auditpr** i **auditmerge**. Te programy narzędziowe działają jako filtry, dlatego można ich w prosty sposób używać dla potoków (opcja szczególnie przydatna dla kontroli w trybie strumieniowym).

auditselect
Tego programu można używać do wybrania tylko konkretnych rekordów kontroli za pomocą instrukcji języka podobnego do SQL. Na przykład, aby wybrać tylko zdarzenia **exec()**, które zostały wygenerowane przez użytkownika *afx*, należy wpisać:

```
auditselect -e "login==afx && event==PROC_Execute"
```

auditpr
Ten program narzędziowy jest używany do przekształcania binarnych rekordów kontroli do postaci czytelnej dla użytkownika. Ilość wyświetlanych informacji zależy od opcji podanych w wierszu komend. Aby uzyskać wszystkie dostępne informacje, komendę **auditpr** należy uruchomić w następujący sposób:

```
auditpr -v -hhelrtRpPTc
```

Gdy zostanie podana opcja **-v**, oprócz standardowych informacji kontroli, które jądro dostarcza dla każdego zdarzenia, wyświetlany jest także zapis kontrolny. Zapis ten jest charakterystyczny dla konkretnego zdarzenia (patrz plik `/etc/security/audit/events`).

auditmerge
Ten program narzędziowy jest używany do scalania binarnych zapisów kontrolnych. Jest to szczególnie przydatne w sytuacji, gdy należy połączyć zapisy kontrolne pochodzące z wielu systemów. Komenda **auditmerge** pobiera nazwy zapisów z wiersza komend i wysyła scalony zapis binarny do standardowego wyjścia (standard), tak więc aby zapis ten stał się czytelny dla użytkownika, należy użyć komendy **auditpr**. Na przykład komendy **auditmerge** i **auditptr** można użyć w następujący sposób:

```
auditmerge trail.system1 trail.system2 | auditpr -v -hhelrRtpc
```

Użycie podsystemu kontrolującego do szybkiego sprawdzenia bezpieczeństwa
Do monitorowania pojedynczego podejrzanego programu (bez konieczności konfigurowania podsystemu kontrolującego) można użyć komendy **watch**. Zapisze ona wszystkie lub żądane zdarzenia, które są generowane przez podany program.

Na przykład, aby zapoznać się z wszystkimi zdarzeniami typu **FILE_Open** generowanymi po uruchomieniu polecenia **vi /etc/hosts**, należy wpisać:

```
watch -eFILE_Open -o /tmp/vi.watch vi /etc/hosts
```

Plik `/tmp/vi.watch` zawiera wszystkie zdarzenia **FILE_Open** występujące podczas sesji w edytorze.

Wybór zdarzeń
Przy wyborze zdarzeń trzeba zachować równowagę między zbyt małą lub zbyt dużą ilością szczegółów.

Zestaw zdarzeń kontrolowanych w systemie definiuje zdarzenia, które są rzeczywiście kontrolowane, oraz poziom szczegółowości kontroli. Zdarzenia kontrolowane muszą, jak już wcześniej powiedziano, obejmować występujące w systemie zdarzenia dotyczące bezpieczeństwa. Określając poziom szczegółowości podczas definiowania zdarzeń kontrolowanych, należy zachować równowagę między zawarciem niewystarczającej ilości szczegółów, co powoduje, że administrator może mieć kłopoty ze zrozumieniem zebranych informacji, a zawarciem zbyt dużej ilości szczegółów, co z kolei powoduje, że zebrano nadmierną ilość informacji, które trudno przeanalizować. Podczas definiowania zdarzeń korzysta się z występujących w nich podobieństw. Na potrzeby niniejszego opisu zdefiniujmy *zdarzenie wykryte* jako pojedynczą instancję zdarzenia kontrolowanego (przykładowo dane zdarzenie może zostać wykryte w różnych miejscach). Podstawową zasadą jest określenie wykrytych zdarzeń o podobnych właściwościach bezpieczeństwa jako tego samego zdarzenia kontrolowanego. Poniżej przedstawiono klasyfikację zdarzeń strategii zabezpieczeń:

- zdarzenia dotyczące podmiotów:
  - utworzenie procesu,
  - usunięcie procesu,
  - ustawienie atrybutów bezpieczeństwa podmiotu: identyfikatorów użytkowników i identyfikatorów grup,
  - grupa procesów, terminal sterujący,
- zdarzenia dotyczące obiektów:
  - utworzenie obiektu,

  - usunięcie obiektu,
  - otwarcie obiektu (w tym procesy traktowane jako obiekty),
  - zamknięcie obiektu (w tym procesy traktowane jako obiekty),
  - ustawienie atrybutów bezpieczeństwa obiektu: właściciel, grupa i lista ACL,
- zdarzenia dotyczące importu i eksportu:
  - importowanie i eksportowanie obiektu,
- zdarzenia dotyczące kont:
  - dodanie użytkownika, zmiana atrybutów użytkownika w bazie danych haseł,
  - dodanie grupy, zmiana atrybutów grupy w bazie danych grup,
  - zalogowanie się użytkownika,
  - wylogowanie się użytkownika,
  - zmiana informacji o uwierzytelnianiu użytkownika,
  - konfigurowanie terminalu zaufanej ścieżki,
  - konfigurowanie uwierzytelniania,
  - zarządzanie kontrolą: wybór zdarzeń i zapisów kontrolnych, włączanie i wyłączanie kontroli, definiowanie klas kontroli użytkowników,
- zdarzenia ogólne dotyczące administrowania systemem:
  - użycie uprawnień,
  - konfigurowanie systemu plików,
  - konfigurowanie i definiowanie urządzeń,
  - definiowanie parametrów konfiguracyjnych systemu,
  - normalny IPL systemu i zamykanie systemu,
  - konfigurowanie RAS,
  - konfigurowanie innych elementów systemu,
  - uruchamianie podsystemu kontrolującego,
  - zatrzymywanie podsystemu kontrolującego,
  - kierowanie zapytań do podsystemu kontrolującego,
  - resetowanie podsystemu kontrolującego,
- naruszenia bezpieczeństwa (potencjalne):
  - odmowy dostępu,
  - niepowodzenia dotyczące uprawnień,
  - wykryte przez diagnostykę awarie i błędy systemu,
  - próby zmiany bazy TCB.

Zdarzenia kontrolowane

Zdarzeniem kontrolowanym jest każde zdarzenie dotyczące bezpieczeństwa mające miejsce w systemie. Zdarzeniem dotyczącym bezpieczeństwa może być każda zmiana stanu zabezpieczeń systemu i usiłowane lub rzeczywiste naruszenie w systemie praw dostępu albo strategii bezpieczeństwa kont bądź też obie te sytuacje. Programy i moduły jądra, które wykrywają zdarzenia kontrolowane, zgłaszają je do systemowego programu protokołującego kontroli. Program ten jest uruchamiany jako część jądra, a dostęp do niego można uzyskać za pomocą podprocedury (w przypadku kontroli programów zaufanych) lub za pomocą wywołania procedury jądra (w przypadku kontroli stanu nadzorcy). Informacje zgłoszone w zdarzeniu kontrolowanym zawierają nazwę tego zdarzenia, informację o tym, czy zdarzenie zostało pomyślnie wykonane, oraz dodatkowe informacje dotyczące zdarzenia, które są istotne dla kontroli zabezpieczeń.

Aby kontrolować dane działanie, należy zidentyfikować komendę lub proces inicjujący zdarzenie kontrolowane i umieścić to zdarzenie w pliku `/etc/security/audit/events` w używanym systemie.

Przypisanie użytkownikom zdarzeń kontrolowanych można uprościć, grupując podobne zdarzenia w klasy kontroli. Klasy te są zdefiniowane w pliku `/etc/security/audit/config` w sekcji classes.

W poniższej tabeli podano niektóre często używane zdarzenia kontrolowane, które występują w systemie operacyjnym AIX:

Tabela 11. Zdarzenia kontrolowane

Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
fork	PROC_Create	Określa, że proces został utworzony.
exit	PROC_Delete	Określa, czy proces wywołujący został zakończony.
exec	PROC_Execute	Uruchamia nowy program.
setuidx	PROC_RealUID	Ustawia identyfikator użytkownika procesu.
	PROC_AuditID	
	PROC_SetUserIDs	
setgidx	PROC_RealGID	Ustawia identyfikator grupy procesów.
accessx	FILE_Accessx	Określa dostępność pliku.
statacl	FILE_StatAcl	Pobiera informacje o prawach dostępu do pliku.
revoke	FILE_Revoke	Odbiera dostęp do pliku przez wszystkie procesy.
frevoke	FILE_Frevoke	Odbiera dostęp do pliku przez inne procesy.
usrinfo	PROC_Environ	Zmienia część danych informacji o użytkowniku.
sigaction	PROC_SetSignal	Określa działanie, które ma zostać wykonane, jeśli konkretny sygnał zostanie dostarczany do procesu, który wywołał tę procedurę.
setrlimit	PROC_Limits	Steruje maksymalnym wykorzystaniem zasobów systemu.
nice	PROC_SetPri	Określa użycie funkcji `nice`.
setpri	PROC_Setpri	Ustawia stały priorytet dla procesów.
setpriv	PROC_Privilege	Zmienia jeden lub wiele wektorów uprawnień dla procesów.
settimer	PROC_Settimer	Ustawia wartość bieżącą dla licznika czasu określonego dla całego systemu.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
adjtime	PROC_Adjtime	Zmienia zegar systemowy.
ptrace	PROC_Debug	Śledzi wykonywanie innego procesu.
kill	PROC_Kill	Wysyła sygnał do procesu lub grupy procesów.
setpgid	PROC_setpgid	Ustawia identyfikator grupy procesów.
ld_loadmodule	PROC_Load	Ładuje nowy moduł obiektów do przestrzeni adresowej procesów.
	PROC_LoadError	Wskazuje, że ładowanie obiektu zakończyło się niepowodzeniem.
setgroups	PROC_SetGroups	Zmienia zestaw grup współbieżnych procesów.
sysconfig	PROC_Sysconfig	Przechwytuje działanie w jądrze lub konfiguracji systemu.
audit	AUD_It	Uruchamia i zatrzymuje operację kontroli. Ponadto odpytuje status kontroli.
auditbin	AUD_Bin_Def	Modyfikuje wywołanie systemowe `auditbin`.
auditevents	AUD_Events	Modyfikuje zdarzenia.
auditobj	AUD_Objects	Modyfikuje wywołanie systemowe `auditobj`.
auditproc	AUD_Proc	Uzyskuje lub ustawia stan kontroli procesu.
acct	ACCT_Disable	Wyłącza rozliczanie systemu.
	ACCT_Enable	Włącza rozliczanie systemu.
open i create	FILE_Open	Wywołuje podprocedurę **open**.
read	FILE_Read	Odczytuje dane z deskryptora pliku.
write	FILE_Write	Zapisuje dane w deskryptorze pliku.
close	FILE_Close	Zamyka otwarty deskryptor pliku.
link	FILE_Link	Tworzy nową pozycję katalogu dla obiektu systemu plików.
unlink	FILE_Unlink	Usuwa obiekt systemu plików.
rename	FILE_Rename	Zmienia nazwę obiektu systemu plików.
chown	FILE_Owner	Zmienia prawo własności pliku.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
chmod	FILE_Mode	Zmienia tryb pliku.
fchmod	FILE_Fchmod	Zmienia uprawnienia pliku dla deskryptora pliku.
fchown	FILE_Fchown	Zmienia prawo własności deskryptora pliku.
truncate	FILE_Truncate	Zmienia długość zwykłych plików lub obiektów pamięci współużytkowanej.
symlink	FILE_Symlink	Tworzy dowiązanie symboliczne.
pipe	FILE_Pipe	Tworzy nienazwany potok.
mknod	FILE_Mknod	Tworzy plik specjalny urządzenia lub plik specjalny FIFO (pierwszy przyszedł - pierwszy wyszedł).
fcntl	FILE_Dupfd	Duplikuje deskryptor pliku.
fscntl	FS_Extend	Rozszerza system plików.
mount	FS_Mount	Podłącza system plików do nazwanego katalogu.
umount	FS_Umount	Odłącza podłączony system plików.
chacl	FILE_Acl	Zmienia listę kontroli dostępu (ACL) pliku.
fchacl	FILE_Facl	Zmienia listę ACL deskryptora pliku.
chpriv	FILE_Privilege	Ustawia listę kontroli uprawnień (PCL) dla nazwy ścieżki do pliku.
	FILE_Chpriv	Zmienia listę PCL.
	FILE_Fchpriv	Zmienia listę PCL deskryptora pliku.
chdir	FS_Chdir	Zmienia bieżący katalog roboczy.
fchdir	FS_Fchdir	Zmienia bieżący katalog roboczy za pomocą deskryptora pliku.
chroot	FS_Chroot	Zmienia znaczenie katalogu głównego (/) dla bieżącego procesu.
rmdir	FS_Rmdir	Usuwa obiekt katalogu.
mkdir	FS_Mkdir	Tworzy katalog.
utimes	FILE_Utimes	Wywołuje podprocedurę **utimes**.
stat	FILE_Stat	Wywołuje podprocedurę **stat**.
msgget	MSG_Create	Tworzy kolejkę komunikatów.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
msgrcv	MSG_Read	Odbiera komunikat z kolejki komunikatów.
msgsnd	MSG_Write	Wysyła komunikat do kolejki komunikatów.
msgctl	MSG_Delete	Usuwa kolejkę komunikatów.
	MSG_Owner	Zmienia prawo własności i prawo dostępu kolejki komunikatów.
	MSG_Mode	Sprawdza prawa dostępu kolejki komunikatów.
semget	SEM_Create	Tworzy zestaw semaforów.
semop	SEM_Op	Zwiększa lub zmniejsza jeden lub więcej semaforów.
semctl	SEM_Delete	Usuwa zestaw semaforów.
	SEM_Owner	Zmienia prawo własności i prawa dostępu zestawu semaforów.
	SEM_Mode	Sprawdza prawa dostępu zestawu semaforów.
shmget	SHM_Create	Tworzy nowy segment pamięci współużytkowanej.
shmat	SHM_Open	Wywołuje podprocedurę **shmat** za pomocą opcji **Open**.
shmat	SHM_Detach	Wywołuje podprocedurę **shmat** za pomocą opcji **Detach**.
shmctl	SHM_Close	Zamyka segment pamięci współużytkowanej.
	SHM_Owner	Zmienia prawo własności i prawa dostępu dla segmentu pamięci współużytkowanej.
	SHM_Mode	Sprawdza prawa dostępu segmentu pamięci współużytkowanej.
tcpip user level	TCPIP_connect	Wywołuje podprocedurę **connect**.
	TCPIP_data_out	Wysłano dane.
	TCPIP_data_in	Odebrano dane.
	TCPIP_set_time	Protokołuje próbę zmiany czasu systemowego za pomocą sieci.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
tcpip kernel level	TCP_ksocket	Określa, że gniazdo jest tworzone.
	TCP_ksocketpair	Określa, że tworzona jest para połączonych gniazd.
	TCP_kclose	Określa, że gniazdo jest zamknięte.
	TCP_ksetopt	Określa, że opcje gniazda są ustawione.
	TCP_kbind	Określa, że nazwa jest powiązana z gniazdem.
	TCP_klisten	Nasłuchiwanie na połączenia gniazda.
	TCP_kconnect	Określa, że utworzono połączenie między dwoma gniazdami.
	TCP_kaccept	Akceptuje nowe gniazdo i określa, że zostanie utworzone połączenie z gniazdem.
	TCP_kshutdown	Określa, że wszystkie operacje wysyłania i odbierania gniazda są zakończone.
	TCP_ksend	Określa, że komunikaty są wysyłane z podłączonego gniazda.
	TCP_kreceive	Określa, że komunikaty są odbierane z podłączonego gniazda.
tsm	USER_Login	Loguje użytkownika do systemu.
	PORT_Locked	Wskazuje, że port jest zablokowany z powodu niepoprawnych prób logowania.
	TERM_Logout	Wylogowuje użytkownika z systemu.
rlogind lub telnetd	USER_Exit	Wskazuje, że użytkownik jest wylogowany.
usrck	USER_Check	Sprawdza dokładność definicji użytkownika.
	USRCK_Error	
logout	USER_Logout	Zatrzymuje wszystkie procesy na porcie.
chsec	PORT_Change	Wskazuje zmianę w wartościach atrybutów portu.
chuser	USER_Change	Zmienia atrybuty użytkownika.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
rmuser	USER_Remove	Usuwa użytkownika.
mkuser	USER_Create	Tworzy użytkownika.
setgroups	USER_SetGroups	Ustawia identyfikator grupy uzupełniającej bieżącego procesu.
setsenv	USER_SetEnv	Ustawia zmienną środowiskową.
su	USER_SU	Zmienia identyfikator użytkownika, który jest powiązany z sesją.
grpck	GROUP_User	Usuwa nieistniejących użytkowników z grupy.
	GROUP_Adms	Usuwa nieistniejących użytkowników administracyjnych z grupy.
chgroup	GROUP_Change	Zmienia atrybuty grupy.
mkgroup	GROUP_Create	Tworzy grupę.
rmgroup	GROUP_Remove	Usuwa grupę.
passwd	PASSWORD_Change	Zmienia hasło użytkownika.
pwdadm	PASSWORD_Flags	Zmienia hasło administratora.
pwdck	PASSWORD_Check	Weryfikuje dokładność informacji uwierzytelniania lokalnego.
	PASWORD_Ckerr	
startsrc	SRC_Start	Uruchamia kontroler zasobów systemu.
stopsrc	SRC_Stop	Zatrzymuje kontroler zasobów systemu.
addssys	SRC_Addssys	Dodaje definicję SRC`subsys` do klasy obiektów podsystemu.
chssys	SRC_Chssys	Zmienia definicję podsystemu w klasie obiektów podsystemu.
addserver	SRC_Addserver	Dodaje definicję podserwera do klasy obiektów podserwera.
chserver	SRC_Chserver	Zmienia definicję podserwera w klasie obiektów podserwera.
rmsys	SRC_Delssys	Usuwa definicję podsystemu z klasy obiektów podsystemu.
rmserver	SRC_Delserver	Usuwa definicję podserwera z klasy obiektów typu `Subserver`.
enq	ENQUE_admin	Kolejkuje plik.
qdaemon	ENQUE_exec	Planuje zadania w kolejce.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
sendmail	SENDMAIL_Config	Kieruje pocztę do dostarczania lokalnego lub sieciowego.
	SENDMAIL_ToFile	
at	AT_JobAdd	Usuwa i dodaje komendy, które są zaplanowane do uruchomienia za pomocą komendy **at**.
	At_JobRemove	
cron	CRON_JobRemove	Usuwa i dodaje komendy, które są zaplanowane do uruchomienia za pomocą komendy **cron**.
	CRON_JobAdd	
	CRON_Start	Wskazuje początek zadania **cron**.
	CRON_Finish	Wskazuje koniec zadania **cron**.
nvload	NVRAM_Config	Określa dostęp do nieulotnej pamięci o dostępie bezpośrednim (NVRAM).
cfgmgr	DEV_Configure	Konfiguruje urządzenia.
chdev i mkdev	DEV_Change	Określa zmianę w urządzeniu.
mkdev	DEV_Create	Określa tworzenie urządzenia.
	DEV_Start	Określa uruchomienie urządzenia.
installp	INSTALLP_Inst	Instaluje dostępne produkty oprogramowania w kompatybilnym pakiecie instalacyjnym.
	INSTALLP_Exec	
rmdev	DEV_Stop	Określa zatrzymanie urządzenia.
	DEV_Unconfigure	Określa zdekonfigurowanie urządzenia.
	DEV_Remove	Określa, że urządzenie zostało usunięte.
lchangelv, lextendlv i lreducelv	LVM_ChangeLV	Określa, że wolumin logiczny został zmieniony.
lchangepv, ldeletepv i linstallpv	LVM_ChangeVG	Określa, że grupa woluminów została zmieniona.
lcreatelv	LVM_CreateLV	Określa, że wolumin logiczny został dodany do systemu.
lcreatevg	LVM_CreateVG	Określa, że grupa woluminów została utworzona w systemie.
ldeletepv	LVM_DeleteVG	Określa, że grupa woluminów została usunięta z systemu.
rmlv	LVM_DeleteLV	Określa, że wolumin logiczny został usunięty z systemu.
lvaryoffvg	LVM_VaryoffVG	Dezaktywuje grupę woluminów.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
lvaryonvg	LVM_VaryonVG	Aktywuje grupę woluminów.
Operacje na woluminach logicznych	LVM_AddLV	Dodaje wolumin logiczny do istniejącej grupy woluminów.
	LVM_KDeleteLV	Usuwa wolumin logiczny z istniejącej grupy woluminów.
	LVM_ExtendLV	Zwiększa wielkość woluminu logicznego, dodając zwolnione partycje fizyczne z grupy woluminów.
	LVM_ReduceLV	Zmniejsza wielkość woluminu logicznego.
	LVM_KChangeLV	Zmienia istniejący wolumin logiczny.
	LVM_AvoidLV	Nie zezwala woluminowi logicznemu na wykonanie konkretnych operacji.
Operacje na woluminach fizycznych	LVM_MissingPV	Dodaje brakujący wolumin fizyczny do istniejącej grupy woluminów.
	LVM_AddPV	Dodaje wolumin fizyczny do istniejącej grupy woluminów.
	LVM_AddMissPV	Dodaje brakujący wolumin fizyczny do istniejącej grupy woluminów.
	LVM_DeletePV	Kasuje wolumin fizyczny z istniejącej grupy woluminów.
	LVM_RemovePV	Usuwa wolumin fizyczny z istniejącej grupy woluminów.
	LVM_AddVGSA	Dodaje obszar statusu grupy woluminów (VGSA) do istniejącego woluminu fizycznego.
	LVM_DeleteVGSA	Usuwa obszar VGSA z istniejącego woluminu fizycznego.

Tabela 11. Zdarzenia kontrolowane (kontynuacja)		
Wywołanie użytkownika lub systemowe	**Zdarzenie kontrolowane**	**Opis**
Operacje na grupach woluminów	LVM_SetupVG	Konfiguruje grupę woluminów przez zdefiniowanie woluminów logicznych i podanie informacji o obszarze VGSA oraz pamięci podręcznej spójności zapisu lustrzanego (MWCC).
	LVM_DefineVG	Definiuje grupę woluminów dla jądra.
	LVM_KDeleteVG	Usuwa grupę woluminów z jądra.
Operacje tworzenia i odtwarzania kopii zapasowych	BACKUP_Export	Przechwytuje postęp operacji tworzenia kopii zapasowej.
	RESTORE_Import	Przechwytuje postęp operacji odtwarzania.
shell	USER_Shell	Przechwytuje informacje `tty` użytkownika.
reboot	USER_Reboot	Przechwytuje zdarzenie restartu systemu.
	PROC_Reboot	Przechwytuje zdarzenie restartu procesu. Podprocedura **reboot** restartuje system lub powtarza operację ładowania programu startowego (IPL) w systemie.

Konfigurowanie kontroli
Niniejsza procedura ilustruje sposób konfigurowania podsystemu kontrolującego. Więcej szczegółowych informacji zawierają pliki konfiguracyjne, o których wspomniano w poniższych krokach.

1. Z listy znajdującej się w pliku `/etc/security/audit/events` wybierz działania w systemie (zdarzenia), które mają być kontrolowane. Jeśli do aplikacji lub rozszerzeń jądra zostały dodane nowe zdarzenia kontrolowane, należy zmodyfikować ten plik, dodając te nowe zdarzenia:
   - Zdarzenie dodaje się do tego pliku, jeśli kod umożliwiający protokołowanie tego zdarzenia dodano do aplikacji (za pomocą podprocedury **auditwrite** lub **auditlog**) lub do rozszerzenia jądra (za pomocą usług jądra **audit_svcstart**, **audit_svcbcopy** i **audit_svcfinis**).
   - W pliku `/etc/security/audit/events` należy umieścić instrukcje formatujące dla nowych zdarzeń kontrolowanych. Te specyfikacje umożliwiają komendzie **auditpr** zarejestrowanie zapisu kontrolnego podczas formatowania rekordów kontroli.
2. Pogrupuj wybrane zdarzenia kontrolowane w zestawy podobnych pozycji nazywane *klasami kontroli*. Klasy kontroli zdefiniuj w sekcji classes pliku `/etc/security/audit/config`.
3. Poszczególnym użytkownikom przypisz klasy kontroli, a plikom (obiektom), które chcesz kontrolować, przypisz zdarzenia kontrolowane:
   - Aby poszczególnym użytkownikom przypisać klasy kontroli, dodaj wiersz w pliku `/etc/security/audit/config` do sekcji każdego użytkownika. Aby użytkownikowi przypisać klasy kontroli, użyj komendy **chuser**,
   - Aby obiektowi (danym lub plikowi wykonywalnemu) przypisać zdarzenia kontrolowane, dodaj sekcję dotyczącą tego obiektu do pliku `/etc/security/audit/objects`,
   - Możesz także podać domyślne klasy kontroli dla nowych użytkowników, modyfikując plik `/usr/lib/security/mkuser.default`. W tym pliku znajdują się atrybuty użytkowników, które zostaną użyte

podczas generowania identyfikatorów nowych użytkowników. Przykładowo dla wszystkich identyfikatorów nowych użytkowników użyj klasy kontroli `general`:

```
user:
    auditclasses = general
    pgrp = staff
    groups = staff
    shell = /usr/bin/ksh
    home = /home/$USER
```

Aby podać wszystkie zdarzenia kontrolowane, użyj klasy ALL. Spowoduje to, nawet w średnio obciążonym systemie, wygenerowanie ogromnej ilości danych. Zwykle praktyczniejszym rozwiązaniem jest ograniczenie liczby zapisywanych zdarzeń.

4. W pliku `/etc/security/audit/config` skonfiguruj typ zbierania informacji, wybierając zbieranie do pliku, zbieranie do strumienia lub obie te metody. Zadbaj, używając dla danych kontroli oddzielnego systemu plików, aby nie współzawodniczyły o miejsce z innymi danymi. Dzięki temu dla danych kontroli będzie zapewniona wystarczająca ilość miejsca. Skonfiguruj typ zbierania danych:
   - Aby skonfigurować zbieranie danych do pliku binarnego:
     a. Włącz tryb zbierania danych do pliku binarnego, ustawiając `binmode = on` w sekcji start,
     b. Zmodyfikuj sekcję binmode, konfigurując pliki binarne oraz zapisy, a następnie podaj ścieżkę do pliku zawierającego komendy postprocesora do przetwarzania w trybie binarnym. Plikiem domyślnym komend postprocesora jest `/etc/security/audit/bincmds`,
     c. Zadbaj o to, aby pliki binarne kontroli miały wystarczającą wielkość i ustaw parametr *freespace*, tak aby zbliżające się zapełnienie systemu plików było sygnalizowane alertem,
     d. Do pliku `/etc/security/audit/bincmds` dodaj komendy powłoki przetwarzające pliki binarne kontroli w potoku kontroli,
   - Aby skonfigurować kolekcję strumieni:
     a. Włącz tryb zbierania danych do strumienia, ustawiając `streammode = on` w sekcji start,
     b. Zmodyfikuj sekcję streammode, podając ścieżkę do pliku zawierającego komendy przetwarzania trybu strumieniowego. Plikiem domyślnym, który zawiera te informacje, jest `/etc/security/audit/streamcmds`,
     c. Do pliku `/etc/security/audit/streamcmds` włącz komendy powłoki przetwarzające rekordy strumieniowe w potoku kontroli.
5. Po wprowadzeniu niezbędnych zmian do plików konfiguracyjnych możesz użyć komendy **audit start**, aby włączyć podsystem kontrolujący. Spowoduje to wygenerowanie zdarzenia **AUD_It** o wartości 1.
6. Aby zobaczyć, które zdarzenia i obiekty są kontrolowane, użyj komendy **audit query**. Spowoduje to wygenerowanie zdarzenia **AUD_It** o wartości 2.
7. Aby ponownie dezaktywować podsystem kontrolujący, użyj komendy **audit shutdown**. Spowoduje to wygenerowanie zdarzenia **AUD_It** o wartości 4.

Generowanie protokołu kontroli ogólnej

Poniżej przedstawiono przykłady generowania ogólnego protokołu kontroli.

W tym przykładzie przyjęto, że administrator systemu chce użyć podsystemu kontrolującego do monitorowania dużego systemu serwerowego, z którego korzysta wielu użytkowników. Brak tu bezpośredniej ingerencji w identyfikatory, a wszystkie rekordy kontroli będą ręcznie badane pod kątem występowania w nich nieregularności. Zapisywanych jest tylko kilka podstawowych zdarzeń kontrolowanych, aby zarządzanie generowanymi danymi było wykonalne.

Zdarzenia kontrolowane, które zostały wybrane do wykrywania:

FILE_Write
Ponieważ potrzebne są informacje o zapisach do plików konfiguracyjnych, to zdarzenie będzie używane dla wszystkich plików znajdujących się w katalogu `/etc` i jego podkatalogach.

PROC_SetUserIDs
Wszystkie zmiany identyfikatorów użytkowników

AUD_Bin_Def
Konfigurowanie pliku binarnego kontroli

USER_SU
Komenda **su**

PASSWORD_Change
Komenda **passwd**

AUD_Lost_Rec
Powiadamianie w razie utraty rekordów

CRON_JobAdd
Nowe zdania cron

AT_JobAdd
Nowe zadania at

USER_Login
Wszystkie logowania się

PORT_Locked
Wszystkie blokady występujące na terminalach spowodowane zbyt dużą liczbą nieudanych prób

Poniżej został przedstawiony przykład generowania protokołu kontroli ogólnej:

1. Skonfiguruj listę newralgicznych plików, dla których mają być monitorowane wprowadzane zmiany (takich jak wszystkie pliki znajdujące się w katalogu `/etc`), i skonfiguruj je w pliku `objects` pod kątem zdarzeń **FILE_Write**:

```
find /etc -type f | awk '{printf("%s:\n\tw = FILE_Write\n\n",$1)}' >> /etc/security/audit/
objects
```

2. Użyj komendy **auditcat**, aby skonfigurować kontrolę w trybie binarnym. Zawartość pliku `/etc/security/audit/bincmds` jest zbliżona do następującej:

```
/usr/sbin/auditcat -p -o $trail $bin
```

3. Zmodyfikuj plik `/etc/security/audit/config`, dodając klasę dla interesujących Cię zdarzeń. Podaj wszystkich istniejących użytkowników i określ dla nich klasę `custom`.

```
start:
        binmode = on
        streammode = off

bin:
        cmds = /etc/security/audit/bincmds
        trail = /audit/trail
        bin1 = /audit/bin1
        bin2 = /audit/bin2
        binsize = 100000
        freespace = 100000

classes:
        custom = FILE_Write,PROC_SetUser,AUD_Bin_Def,AUD_Lost_Rec,USER_SU, \
                 PASSWORD_Change,CRON_JobAdd,AT_JobAdd,USER_Login,PORT_Locked

users:
        root = custom
        afx = custom
        ...
```

4. Do pliku `/usr/lib/security/mkuser.default` dodaj klasę kontroli `custom`, dzięki czemu z nowymi identyfikatorami będzie automatycznie powiązane odpowiednie wywołanie kontroli:

```
user:
    auditclasses = custom
    pgrp = staff
    groups = staff
```

```
    shell = /usr/bin/ksh
    home = /home/$USER
```

5. Za pomocą programu SMIT lub komendy **crfs** utwórz nowy system plików o nazwie `/audit`. Powinien on być wystarczająco duży, aby pomieścić dwa pliki binarne i duży zapis kontrolny.
6. Uruchom komendę **audit start** i przejrzyj plik `/audit`. Powinien on zawierać na początku dwa pliki binarne i jeden pusty plik `trail`. Po pewnym czasie korzystania z systemu w pliku `trail` powinny pojawić się rekordy kontroli. Plik ten można odczytać za pomocą komendy:

```
auditpr  -hhelpPRtTc -v | more
```

W powyższym przykładzie użyto tylko kilku zdarzeń. Aby zobaczyć wszystkie zdarzenia, nazwy klasy ALL należy użyć dla wszystkich użytkowników. Spowoduje to wygenerowanie dużych ilości danych. Do klasy `custom` można dodać wszystkie zdarzenia powiązane ze zmianami dotyczącymi użytkowników i uprawnień.

Monitorowanie dostępu do newralgicznych plików w czasie rzeczywistym
Opisane czynności można wykonać w celu monitorowania dostępu do newralgicznych plików w czasie rzeczywistym.

Wykonaj następujące czynności:

1. Skonfiguruj listę newralgicznych plików, dla których mają być monitorowane wprowadzane zmiany (są to na przykład wszystkie pliki znajdujące się w katalogu `/etc`), i skonfiguruj je w pliku `objects` pod kątem zdarzeń **FILE_Write**:

```
find /etc -type f | awk '{printf("%s:\n\tw = FILE_Write\n\n",$1)}' >> /etc/security/audit/
objects
```

2. Skonfiguruj kontrolę strumienia, tak aby wyświetlane były wszystkie zapisy do plików. (W tym przykładzie wszystkie zapisy do plików wyświetlane są na konsoli, ale w środowisku produkcyjnym można wykorzystać program backend wysyłający te zdarzenia do systemu wykrywania włamań). Zawartość pliku `/etc/security/audit/streamcmds` jest zbliżona do następującej:

```
/usr/sbin/auditstream | /usr/sbin/auditselect -e "event == FILE_Write" |
auditpr  -hhelpPRtTc -v > /dev/console &
```

3. W pliku `/etc/security/audit/config` skonfiguruj kontrolę w trybie strumieniowym, dodaj klasę obejmującą zdarzenia zapisu do plików i skonfiguruj wszystkich użytkowników, którzy powinni być kontrolowani za pomocą tej klasy:

```
start:
        binmode = off
        streammode = on

stream:
        cmds = /etc/security/audit/streamcmds

classes:
        filemon = FILE_write

users:
        root = filemon
        afx = filemon
        ...
```

4. Uruchom komendę **audit start**. Wszystkie zdarzenia typu **FILE_Write** są wyświetlane na konsoli.

Wybór zdarzeń kontrolowanych
Kontrola ma na celu wykrywanie działań, które mogą stanowić zagrożenie bezpieczeństwa systemu.

Jeśli wymienione poniżej działania są wykonywane przez nieuprawnionego użytkownika, naruszają one bezpieczeństwo systemu, powinny być więc kontrolowane:

- wykonywanie działań w bazie TCB,
- uwierzytelnianie użytkowników,

- uzyskiwanie dostępu do systemu,
- zmiana konfiguracji systemu,
- próby obejścia systemu kontrolującego,
- inicjowanie systemu,
- instalowanie programów,
- modyfikowanie kont,
- przesyłanie informacji do i z systemu.

W systemie kontrolującym nie ma domyślnego zestawu zdarzeń, które mają być kontrolowane. Administrator powinien sam wybrać zdarzenia lub klasy zdarzeń stosownie do potrzeb.

Aby kontrolować dane działanie, należy zidentyfikować komendę lub proces inicjujący zdarzenie kontrolowane i umieścić to zdarzenie w pliku `/etc/security/audit/events` w używanym systemie. Następnie zdarzenie to należy dodać albo do odpowiedniej klasy w pliku `/etc/security/audit/config` , albo do sekcji obiektów w pliku `/etc/security/audit/objects`. Listę zdarzeń kontrolowanych i instrukcje dotyczące formatowania zapisu zawiera plik `/etc/security/audit/events` znajdujący się w używanym systemie. Opis zapisywania i używania formatów zdarzeń kontrolowanych zawiera pomoc dla komendy **auditpr**.

Po wybraniu zdarzeń do kontrolowania należy połączyć podobne zdarzenia w klasy kontroli. Klasy kontroli przypisuje się następnie użytkownikom.

Wybór klas kontroli

Przypisanie użytkownikom zdarzeń kontrolowanych można uprościć, grupując podobne zdarzenia w klasy kontroli. Klasy te są zdefiniowane w pliku `/etc/security/audit/config` w sekcji classes.

Do najczęściej stosowanych klas kontroli należą:

general
Klasa ta obejmuje zdarzenia zmieniające stan systemu i uwierzytelnianie użytkowników. Kontroluje próby obejścia kontroli dostępu do systemu.

objects
Dostęp do zapisu do plików konfiguracyjnych zabezpieczeń.

kernel
Zdarzenia w tej klasie są generowane przez funkcje zarządzania procesami jądra.

Przykład sekcji pliku `/etc/security/audit/config`:

```
classes:
    general = USER_SU,PASSWORD_Change,FILE_Unlink,FILE_Link,FILE_Rename
    system = USER_Change,GROUP_Change,USER_Create,GROUP_Create
    init = USER_Login,USER_Logout
```

Wybór metody zbierania danych kontroli

Wybór metody zbierania danych jest podyktowany sposobem wykorzystania tych danych. Jeśli potrzebne jest długoterminowe przechowywanie dużych ilości danych, należy wybrać zbieranie danych do pliku binarnego. Jeśli dane mają być przetwarzane zaraz po ich zebraniu, należy wybrać zbieranie do strumienia. Jeśli potrzebne jest zarówno długoterminowe przechowywanie, jak i natychmiastowe przetwarzanie, należy wybrać obie metody. Poniżej podano opis każdej z tych metod:

Zbieranie do pliku binarnego
Umożliwia długotrwałe przechowywanie dużych ilości zapisów kontrolnych. Rekordy kontroli są zapisywane do pliku, który jest tymczasowym pojemnikiem. Po jego zapełnieniu dane są przetwarzane przez demon **auditbin**, podczas gdy podsystem kontrolujący zapisuje dane do drugiego pliku binarnego, a rekordy są zapisywane do pliku zapisów kontrolnych w celu ich przechowywania.

Zbieranie do strumienia
Umożliwia przetwarzanie danych kontroli zaraz po ich zebraniu. Rekordy kontroli są zapisywane do cyklicznego buforu w jądrze, a odtwarzane za pomocą pseudourządzenia `/dev/audit`. Rekordy kontroli można wyświetlać, drukować (w celu uzyskania papierowej wersji zapisu kontroli) lub - za pomocą komendy **auditcat** - przekształcać na rekordy binarne.

Kontrola partycji WPAR
W środowisku partycji WPAR dostępne są trzy typy kontroli: globalna, systemowa i kontrola z poziomu globalnego.

Kontrolę partycji WPAR można włączyć globalnie, wewnątrz partycji WPAR lub używając tych dwóch sposobów jednocześnie. Konfiguracja kontroli dla systemowej i globalnej kontroli WPAR jest podobna do konfiguracji w środowisku innymi niż partycji WPAR. Globalną kontrolę partycji WPAR można zainicjować dla partycji WPAR systemu i aplikacji.

Uwaga: Kontroli partycji WPAR aplikacji nie można zainicjować wewnątrz partycji WPAR, ale można ją zainicjować za pomocą globalnej kontroli partycji WPAR.

Globalna kontrola partycji WPAR pomaga administratorom systemu globalnego kontrolować partycje WPAR z systemu globalnego. Administrator systemu globalnego może sterować poziomem kontroli wszystkich partycji WPAR z jednego miejsca, określając klasy przeznaczone do kontroli dla każdej partycji WPAR w pliku globalnym `/etc/security/audit/config`.

Dodając sekcję WPARS do pliku `/etc/security/audit/config`, administrator systemu globalnego może udostępnić listę klas podlegających kontroli dla partycji WPAR. Na przykład:

```
WPARS:
<nazwa_partycji_wpar> = <klasa kontroli>, ... <klasa kontroli>
```

W podanym przykładzie <nazwa_partycji_wpar> musi być nazwą systemową partycji WPAR, a każdy parametr klasa_kontroli powinien być zdefiniowany w sekcji klas (classes).

Aby skonfigurować kontrolę partycji WPAR testwpar z klasami general, tcpip, i lvm, do pliku `/etc/security/audit/config` dodaj następującą sekcję:

```
WPARS:
testwpar = general,tcpip,lvm
```

Administrator systemu globalnego może uruchamiać i zatrzymywać kontrolę na partycji WPAR, używając komendy **audit** i podając nazwę partycji WPAR w następujący sposób:

```
audit start -@ <nazwa_wpar1> -@ <nazwa_wpar2> ...
audit shutdown -@ <nazwa_wpar1> -@ <nazwa_wpar2> ...
```

Możesz kontrolować obiekty WPAR ze środowiska globalnego, określając bezwzględne ścieżki do obiektów, które mają być kontrolowane. Na przykład, aby zdefiniować zdarzenia kontrolowane dla pliku `/wpars/wpar1/etc/security/passwd`, do pliku `/etc/security/audit/objects` w systemie AIX obsługującym partycję WPAR dodaj następującą sekcję:

```
/wpars/wpar1/etc/security/passwd:
     r = "WPAR1_PASSWD_RD"
     w = "WPAR1_PASSWD_WR"
```

Ta poprzedzająca sekcja jest analizowana podczas uruchamiania kontroli (-@ <wpar1>) w celu włączenia kontroli obiektu dla obiektu `/etc/security/passwd` partycji wpar1. Atrybuty te generują zdarzenie kontrolowane WPAR1_PASSWD_RD przy każdym odczycie pliku `/wpars/wpar1/etc/security/passwd`. Ponadto atrybuty te generują zdarzenie kontrolowane WPAR1_PASSWD_WR przy każdym otwarciu tego pliku do zapisu.

Uwaga: Przed włączeniem kontroli WPAR ze środowiska globalnego należy włączyć kontrolę dla środowiska globalnego.

Do wygenerowania raportu kontroli wyświetlającego nazwę partycji WPAR można użyć komendy **auditpr**. Na przykład:

```
auditpr -v < /audit/trail
```

Kontrola w środowisku NFS

Podsystem kontrolujący systemu AIX obsługuje kontrolę podłączonych systemów plików. Konfiguracja podłączonego systemu plików na kliencie jest podobna do konfiguracji lokalnego systemu plików. Operacje kontroli wykonywane na podłączonych obiektach podlegających kontroli są podobne do operacji na obiektach lokalnych, zgodnie z opisem w sekcji dotyczącej przeglądu kontroli. Działanie kontroli na kliencie i serwerze dla podłączonych systemów plików opisano w dalszej części tej sekcji.

Kontrola na kliencie NFS

Wszystkie wykonywane przez klienta operacje na obiektach podlegających kontroli w podłączonych systemach plików są rejestrowane na kliencie. Zakłada się, że na tych obiektach nie są wykonywane żadne inne operacje, ani przez serwer NFS, ani przez inne klienty NFS lub na kliencie należy włączyć kontrolę dla pełnej ścieżki.

Więcej informacji na ten temat zawiera opis komendy **audit**. Jeśli nie włączono kontroli dla pełnej ścieżki i plik jest modyfikowany przez serwer lub inne klienty, kolejne operacje kontroli mogą być nieprzewidywalne. Działanie to można naprawić, restartując kontrolę na kliencie. Jeśli system plików jest podłączony na wielu klientach, zaleca się kontrolowanie operacji na serwerze, dzięki czemu można uzyskać dokładny protokół zdarzeń, lub włączenie kontroli dla pełnej ścieżki na kliencie.

Uwaga: Konfiguracja podsystemu kontroli nie obsługuje używania systemu plików protokołu kontroli zdarzeń jako podłączonego systemu plików NFS.

Kontrola na serwerze NFS

Wszystkie operacje wykonywane przez klienta i serwer na podłączonym systemie plików są protokołowane na serwerze NFS.

Ograniczenia po stronie serwera

- Jeśli jakiekolwiek operacje wykonane przez klienta NFS nie zostaną wysłane na serwer, z powodu buforowania NFS lub architektury właściwej systemowi NFS, operacje te nie będą kontrolowane przez serwer.

  Na przykład: Po podłączeniu systemu plików tylko pierwsza operacja odczytu wykonywana na pliku jest kontrolowana przez serwer. Kolejne operacje odczytu nie są protokołowane na serwerze. Reguła ta dotyczy operacji odczytu plików, dowiązań i katalogów.
- Operacje wykonywane przez klienta są rejestrowane na serwerze jako **nfsd**, a nazwą użytkownika jest **root**.

Przykład

System plików o nazwie *system_plików* został podłączony na kliencie za pomocą komendy **mount server:/system_plików /mnt**. Jeśli plik o nazwie *A* w systemie plików *system_plików* ma być kontrolowany przez serwer, to `/system_plików/A` należy skonfigurować w plikach konfiguracyjnych kontroli.

Jeśli użytkownik zdecyduje się na kontrolę pliku *A* w systemie plików *system_plików* na kliencie, to należy skonfigurować kontrolę `/mnt/A` na tym kliencie.

Jeśli plik *A* został skonfigurowany na potrzeby kontroli zarówno na serwerze, jak i na kliencie, operacje wykonywane przez serwer i klienta na tym pliku *A* są kontrolowane i rejestrowane na serwerze, a operacje wykonywane przez klienta są rejestrowane na tym kliencie.

Każda operacja wykonywana przez tego klienta na pliku *A* jest protokołowana na serwerze jako demon **nfsd**, a nie jako nazwa operacji lub komendy.

Protokół LDAP (Lightweight Directory Access Protocol)

Protokół LDAP (Lightweight Directory Access Protocol) definiuje standardową metodę dostępu do informacji i ich aktualizacji w katalogu (bazie danych) lokalnym lub zdalnym w przypadku modelu klient/serwer.

Protokół jest zoptymalizowany pod kątem czytania, przeglądania i wyszukiwania katalogów. Został on początkowo zaprojektowany jako niewymagający protokół dla X.500 Directory Access Protocol. Metoda LDAP jest używana przez klaster hostów w celu umożliwienia scentralizowanego uwierzytelniania oraz dostępu do informacji o użytkownikach i grupach. Ta funkcja jest przeznaczona do użycia w środowisku klastrowym w celu przechowywania informacji o uwierzytelnianiu, użytkownikach i grupach, wspólnych w obrębie klastra.

Obiekty w protokole LDAP są zapisane w hierarchicznej strukturze, znanej jako drzewo informacji katalogu (Directory Information Tree - DIT). Dobry katalog jest uruchamiany ze strukturalnym układem drzewa DIT. Drzewo DIT powinno być starannie zaprojektowane przed zaimplementowaniem protokołu LDAP jako narzędzia uwierzytelniania.

Moduł ładowalny uwierzytelniania LDAP

Wykorzystanie podsystemu zabezpieczeń przez protokół LDAP zostało zaimplementowane jako moduł ładowalny uwierzytelniania LDAP. Jest on koncepcyjnie podobny do innych modułów ładowalnych, takich jak NIS, DCE i KRB5. Moduły ładowalne są zdefiniowane w pliku `/usr/lib/security/methods.cfg`.

Moduł ładowalny protokołu LDAP udostępnia uwierzytelnianie użytkowników oraz scentralizowane zarządzanie grupami i użytkownikami. Użytkownik zdefiniowany na serwerze LDAP może być skonfigurowany, tak aby logował się do klienta LDAP nawet wtedy, gdy użytkownik nie jest zalogowany lokalnie.

Moduł ładowalny protokołu LDAP w systemie AIX jest w pełni zintegrowany z systemem operacyjnym AIX. Po włączeniu modułu ładowalnego uwierzytelniania LDAP w celu udostępniania informacji o użytkownikach i grupach, funkcje API wysokiego poziomu, komendy i narzędzia do zarządzania systemem pracują bez zmian. Dla większości komend wysokiego poziomu wprowadzono opcję **-R**, umożliwiającą pracę przez różne moduły ładowalne. Na przykład, aby utworzyć użytkownika LDAP o nazwie *jan*, na kliencie należy wprowadzić komendę:

```
mkuser -R LDAP jan
```

Uwaga: Mimo że infrastruktura LDAP może obsługiwać nieograniczoną liczbę użytkowników w grupie, dla pojedynczej grupy, na której testowano różne operacje, utworzono prawie 25 000 użytkowników. Niektóre historyczne interfejsy POSIX mogą nie zwracać pełnych informacji dla grupy. W celu sprawdzenia tego typu ograniczeń, należy sprawdzić dokumentację funkcji API.

Uwierzytelnianie w oparciu o protokół LDAP

Istnieją pewne ograniczenia różnych jednostek będących częścią procesu uwierzytelniania w oparciu o protokół LDAP w systemie AIX.

Należy zauważyć, że sama infrastruktura LDAP nie określa żadnych ograniczeń zawartości bazy danych. Jednakże ta sekcja dokumentuje wyniki w oparciu o ograniczone konfiguracje testowe. Dla uwierzytelniania w oparciu o protokół LDAP w systemie operacyjnym AIX przetestowano następujące wartości graniczne:

Całkowita liczba użytkowników: w pojedynczym systemie utworzono prawie 500 000 użytkowników, a jednoczesne uwierzytelnianie przetestowano dla setek użytkowników.

Całkowita liczba grup: w pojedynczym systemie utworzono i przetestowano prawie 500 grup.

Maksymalna liczba użytkowników na grupę: w pojedynczej grupie utworzono prawie 25 000 użytkowników, dla których przetestowano różne operacje na grupie.

Niektóre historyczne interfejsy POSIX mogą nie zwracać pełnych informacji dla grupy. W celu sprawdzenia tego typu ograniczeń, należy sprawdzić dokumentację funkcji API. Co więcej, powyższe wartości określone zostały dla wykonanych testów. Nie wykluczają one możliwości skonfigurowania systemów z dużo większą liczbą użytkowników i grup, jeśli tylko dostępne są wymagane zasoby.

Konfigurowanie serwera IBM Security Directory Server
Aby skonfigurować system jako serwer informacji o bezpieczeństwie LDAP udostępniający informacje o uwierzytelnianiu, użytkownikach i grupach za pomocą LDAP, należy najpierw zainstalować pakiety serwera i klienta LDAP.

Jeśli wymagana jest obsługa protokołu SSL (Secure Sockets Layer) lub TLS (Transport Layer Security), należy również zainstalować pakiet Global Security Kit w wersji 8 (GSKitV8) dla serwera IBM Security Directory Server w wersji 6.4. Administrator systemu musi utworzyć bazę danych kluczy, korzystając z komendy zarządzania kluczami GSKit. Można użyć komendy **gsk8capicmd** lub **gsk8capicmd_64**, która jest dostępna w pakiecie GSKitV8. Więcej informacji na temat konfigurowania obsługi protokołu SSL dla serwera LDAP zawiera sekcja Bezpieczna komunikacja przy użyciu SSL.

Przed skonfigurowaniem klienta należy skonfigurować serwer LDAP. Aby zainstalować i skonfigurować serwer LDAP, wykonaj poniższe działania.

1. Zainstaluj zestawy plików powiązane z pakietem GSKit jako użytkownik root.
   a. Podłącz dysk DVD z pakietem rozszerzeń systemu AIX 7.2.
   b. Zmień katalog na położenie zestawu plików GSKit.

      ```
      cd <punkt_podłączenia>/installp/ppc
      ```

2. Uruchom komendę **installp**, aby zainstalować wszystkie pakiety GSKit.
   - Aby zainstalować 64-bitowe pakiety GSKit, wprowadź następujące komendy:

     ```
     installp -acXgYd . GSKit8.gskcrypt64.ppc.rte
     installp -acXgYd . GSKit8.gskssl64.ppc.rte
     ```

   - Aby zainstalować 32-bitowe pakiety GSKit, wprowadź następujące komendy:

     ```
     installp -acXgYd . GSKit8.gskcrypt32.ppc.rte
     installp -acXgYd . GSKit8.gskssl32.ppc.rte
     ```

     Uwaga: W celu zainstalowania zestawów plików GSKit z dysku DVD można także użyć programu SMIT lub SMITTY.
3. Zainstaluj bazę danych IBM Db2 w wersji 10.5.
   a. Podłącz drugi wolumin (wolumin 2 z 2) dysku DVD systemu AIX 7.2.
   b. Przejdź do katalogu bazy danych IBM Db2 w wersji 10.5.

      ```
      cd <punkt_podłączenia>/ismp/ppc/db2_10_05*
      ```

   c. Otwórz plik `setupaix.bin`, aby zainstalować serwer Db2 w folderze `/opt/IBM/db2/V10.5` i dodać go do bazy danych VPD (Vital Product Database). Dodanie serwera Db2 do bazy VPD umożliwia komendzie **lslpp** wyświetlenie serwera Db2 na liście. Jeśli nie jest dostępny graficzny interfejs użytkownika (GUI), można użyć komendy `db2_install` w celu zainstalowania serwera Db2.

      ```
      ./db2_install
      Wybierz domyślny folder instalacyjny: /opt/IBM/db2/V10.5
       lub podaj folder niestandardowy w tym samym systemie.
      Wybierz opcję SERVER jako produkt Db2, który ma zostać zainstalowany.
      Wybierz wartość NIE dla opcji Db2 pureScale Feature.
      ```

   d. Zastosuj licencję dla bazy danych IBM Db2 w wersji 10.5. Użytkownik musi znajdować się w ścieżce `<punkt_podłączenia>/ismp/ppc/db2_10_05*` i wykonać następującą komendę:

      ```
      <folder_instalacyjny_db2>/adm/db2licm -a ./db2/license/db2ese_t.lic
      ```

4. Zainstaluj klienta *idsldap* i zestawy plików serwera jako użytkownik root.
   a. Podłącz drugi wolumin (wolumin 2 z 2) dysku DVD systemu AIX 7.2.

b. Uruchom komendę **idsLicense**.

```
cd <punkt_podłączenia>/license
./idsLicense
```

5. Jeśli zgadzasz się na warunki umowy licencyjnej na oprogramowanie, wprowadź cyfrę 1 z poniższej listy dostępnych opcji:

```
1: zaakceptowanie umowy licencyjnej.
2: odrzucenie umowy licencyjnej i zakończenie instalacji.
3: wydrukowanie umowy licencyjnej.
4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
99: powrót do poprzedniego ekranu.
```

Po zaakceptowaniu warunków umowy licencyjnej na oprogramowanie w katalogu instalacyjnym serwera IBM Security Directory Server tworzony jest plik LAPID i folder licencji. W folderze licencji znajdują się pliki licencji serwera IBM Security Directory Server we wszystkich obsługiwanych językach.

6. Określ pakiety klienta serwera IBM Security Directory Server *idsldap*, które należy zainstalować.
   - Dla działania klienta i serwera LDAP bez obsługi SSL należy zainstalować następujące zestawy plików:
     - idsldap.license64
     - idsldap.cltbase64
     - idsldap.clt32bit64
     - idsldap.clt64bit64
     - idsldap.cltjava64
     - idsldap.msg64.en_US
     - idsldap.srvbase64bit64
     - idsldap.srv64bit64
     - idsldap.srvproxy64bit64
   - Dla działania klienta i serwera LDAP z obsługą SSL należy zainstalować następujące zestawy plików:
     - idsldap.license64
     - idsldap.cltbase64
     - idsldap.clt32bit64
     - idsldap.clt64bit64
     - idsldap.clt_max_crypto32bit64
     - idsldap.clt_max_crypto64bit64
     - idsldap.cltjava64
     - idsldap.msg64.en_US
     - idsldap.srvbase64bit64
     - idsldap.srv64bit64
     - idsldap.srvproxy64bit64
     - idsldap.srv_max_cryptobase64bit64

       Uwaga: Funkcjonalność SSL wymaga zainstalowania zestawów plików GSKitv8.
   - Aby uzyskać narzędzie Web Administration Tool serwera IBM Security Directory Server, należy zainstalować następujące zestawy plików:
     - idsldap.webadmin64
     - idsldap.webadmin_max_crypto64 (włączona obsługa SSL)

Podczas instalacji programu IBM Security Directory Server Web Administration Tool w folderze `/opt/IBM/ldap/V6.4/idstools/` znajduje się tylko plik `IDSWebApp.war`. Niezbędne jest posiadanie obsługiwanej wersji serwera WebSphere Application Server, w którym można wdrożyć plik WAR. Więcej informacji na temat wdrażania programu Web Administration Tool można znaleźć w sekcji Ręczne wdrażanie programu Web Administration Tool.

7. Uruchom następujące komendy, aby zainstalować pakiety klienta serwera IBM Directory Server *idsldap*.
   - Aby zainstalować jeden lub więcej pakietów klienta IBM Security Directory Server *idsldap*, uruchom następujące komendy:

     ```
     cd <punkt_podłączenia>/installp/ppc/
     installp -acXgYd . <nazwy_pakietów>
     ```

   - Aby zainstalować wszystkie pakiety produktu IBM Security Directory Server z bieżącej ścieżki, uruchom następującą komendę:

     ```
     installp -acXgYd . idsldap
     ```

8. Sprawdź, czy instalacja serwera IBM Security Directory Server zakończyła się pomyślnie, korzystając z podsumowania instalacji wygenerowanej przez system.

   Uwaga: Do zainstalowania zidentyfikowanych zestawów plików i pakietów z dysku DVD można także użyć programu SMIT lub SMITTY.

9. Aby skonfigurować serwer, należy uruchomić komendę **mksecldap**, zastępując wartości odpowiednio do używanego środowiska:

   ```
   mksecldap -s -a cn=admin -p hasloadmin -S rfc2307aix
   ```

Komenda **mksecldap** tworzy serwer LDAP i jego bazę danych zaplecza o nazwie *ldapdb2*, zapełnia ten serwer informacjami o użytkownikach i grupach z hosta lokalnego, a także ustawia nazwę wyróżniającą (DN) i hasło administratora serwera LDAP. Opcjonalnie za pomocą tej komendy można także skonfigurować warstwę SSL dla komunikacji klient/serwer. Komenda **mksecldap** dodaje także pozycję do pliku `/etc/inittab`, służącą do uruchamiania serwera LDAP podczas każdego restartu. Więcej informacji na temat komendy **mksecldap** zawiera temat **mksecldap**.

Użytkownicy i grupy systemu AIX są zapisywani na serwerze LDAP za pomocą jednego z następujących schematów:

Schemat AIX
Zawiera klasy obiektów `aixAccount` i `aixAccessGroup`. Ten schemat udostępnia pełny zestaw atrybutów dla użytkowników i grup systemu AIX.

Schemat RFC 2307
Zawiera klasy obiektów `posixAccount`, `shadowAccount` i `posixGroup` i jest używany w produktach katalogowych wielu dostawców. Schemat RFC 2307 definiuje tylko niewielki podzestaw atrybutów używanych w systemie AIX.

Schemat RFC2307AIX
Zawiera klasy obiektów `posixAccount`, `shadowAccount` i `posixGroup` oraz dodatkowo `aixAuxAccount` i `aixAuxGroup`. Klasy obiektów `aixAuxAccount` i `aixAuxGroup` udostępniają atrybuty używane przez system AIX, które nie są zdefiniowane w schemacie RFC 2307.

Dla użytkowników i grup zaleca się użycie schematu RFC2307AIX. Schemat RFC2037AIX jest w pełni zgodny ze schematem RFC 2307, a ponadto zawiera atrybuty do obsługi dodatkowej funkcjonalności zarządzania użytkownikami systemu AIX. Serwer IBM Tivoli Directory Server z konfiguracją schematu RFC2307AIX obsługuje nie tylko klientów LDAP w systemie AIX, ale także innych klientów LDAP w systemach UNIX i Linux zgodnych ze schematem RFC 2307.

Wszystkie informacje o użytkownikach i grupach są zapisywane we wspólnym drzewie w systemie AIX (przyrostek). Domyślnym przyrostkiem jest "cn=aixdata". Komenda **mksecldap** akceptuje przyrostek dostarczony przez użytkownika podany za pomocą opcji *-d*. Nazwa poddrzewa tworzonego dla

użytkownika, grupy, identyfikatora i tak dalej, znajduje się w pliku konfiguracyjnym `sectoldif.cfg`. Więcej informacji można znaleźć w pliku `sectoldif.cfg`.

Drzewo systemu AIX jest chronione przy użyciu listy ACL (Access Control List). Domyślna lista ACL nadaje uprawnienia administratora tylko jednostce określonej w opcji komendy *-a* jako administrator. Tożsamości serwera proxy można nadać dodatkowe uprawnienia, używając opcji komendy *-x* i *-X*. Użycie tej opcji spowoduje utworzenie tożsamości serwera proxy i skonfigurowanie uprawnień dostępu zgodnie z definicją zawartą w pliku `/etc/security/ldap/proxy.ldif.template`. Utworzenie tożsamości serwera proxy umożliwia klientom LDAP łączenie się z serwerem bez konieczności używania tożsamości administratora i ograniczania uprawnień administratora na serwerze LDAP.

Komendę **mksecldap** można uruchamiać na serwerze LDAP, który został skonfigurowany do innych celów, na przykład dla informacji o wyszukiwaniu ID użytkownika. W tym przykładzie komenda **mksecldap** dodaje drzewo systemu AIX i wypełnia istniejący serwer LDAP informacjami o zabezpieczeniach systemu AIX. To drzewo jest chronione listą ACL niezależnie od innych istniejących drzew.

Uwaga: Przed uruchomieniem komendy **mksecldap** i umieszczeniem tego serwera na serwerze informacji o bezpieczeństwie AIX należy utworzyć kopię zapasową istniejącego serwera informacji o bezpieczeństwie LDAP.

Po pomyślnym skonfigurowaniu serwera informacji o bezpieczeństwie LDAP ten sam host można skonfigurować jako klienta, aby zarządzać użytkownikami i grupami LDAP i umożliwić użytkownikom LDAP logowanie się na tym serwerze.

Jeśli serwer informacji o bezpieczeństwie LDAP nie zostanie pomyślnie skonfigurowany, można wycofać konfigurację, uruchamiając komendę **mksecldap** z opcją *-U*. Spowoduje ona odtworzenie pliku `ibmslapd.conf` lub `slapd.conf` albo `slapd32.conf` do stanu sprzed konfiguracji. Po każdej nieudanej próbie wykonania konfiguracji, a przed ponownym uruchomieniem komendy **mksecldap**, należy uruchomić komendę **mksecldap** z opcją *-U*. W przeciwnym razie w pliku konfiguracyjnym mogą pozostać resztki informacji konfiguracyjnych, co może doprowadzić do kolejnej nieudanej próby konfiguracji. Opcja wycofywania, jako środek ostrożności zapewniający bezpieczeństwo, nie wprowadza żadnych zmian w bazie danych (znajdujących się w niej danych), ponieważ baza ta mogła istnieć przed uruchomieniem komendy **mksecldap**. Jeśli baza danych została utworzona za pomocą komendy **mksecldap**, należy ją usunąć ręcznie. Jeśli komenda **mksecldap** dodała dane do wcześniej istniejącej bazy danych, należy zdecydować, jakie kroki należy podjąć w celu przywrócenia normalnego stanu po niepomyślnej próbie konfiguracji.

Pojęcia pokrewne

Zarządzanie użytkownikami LDAP
Użytkownikami i grupami na serwerze informacji o bezpieczeństwie LDAP można zarządzać z dowolnego klienta LDAP za pomocą komend wysokiego poziomu.

Konfigurowanie klienta LDAP

Aby skonfigurować klienta w celu używania protokołu LDAP do uwierzytelniania i uzyskiwania informacji o użytkownikach i grupach, należy upewnić się, że każdy klient ma zainstalowany pakiet klienta LDAP. Więcej informacji na temat instalowania pakietu klienta LDAP można znaleźć w krokach od “3” na stronie 163 do “7” na stronie 164. Jeśli wymagane jest użycie protokołu SSL (Secure Sockets Layer) lub TLS (Transport Layer Security), musi być zainstalowany pakiet GSKit. Należy utworzyć klucz i dodać do niego certyfikat klucza SSL serwera LDAP. Patrz kroki od “1” na stronie 163 do “2” na stronie 163.

Podobnie jak podczas konfigurowania serwera LDAP, do skonfigurowania klienta LDAP można użyć komendy **mksecldap**. Aby dany klient miał kontakt z serwerem informacji o bezpieczeństwie LDAP, podczas konfigurowania należy podać nazwę tego serwera. Aby klient uzyskał dostęp do drzewa AIX na serwerze, wymagana jest także nazwa wyróżniająca i hasło powiązania serwera. Komenda **mksecldap** zapisuje na serwerze nazwę domeny powiązania serwera, hasło, nazwę serwera i nazwę domeny drzewa AIX na serwerze, a w pliku `/etc/security/ldap/ldap.cfg` - ścieżkę klucza i hasło SSL oraz inne atrybuty konfiguracji.

Komenda **mksecldap** zapisuje hasło powiązania i hasło klucza SSL (w przypadku konfigurowania SSL) w pliku `/etc/security/ldap/ldap.cfg` w formacie szyfrowanym. Zaszyfrowane hasła są specyficzne dla danego systemu i mogą być używane przez demon **secldapclntd** tylko w systemie, w którym zostały

wygenerowane. Demon **secldapcIntd** może korzystać z hasła w postaci jawnego tekstu lub z hasła zaszyfrowanego z pliku `/etc/security/ldap/ldap.cfg`.

Podczas konfigurowania klienta w komendzie **mksecldap** można podać wiele serwerów. W takiej sytuacji klient kontaktuje się z serwerami w podanej kolejności i ustanawia połączenie z pierwszym serwerem, z którym jest to możliwe. Jeśli pojawi się błąd połączenia między klientem a serwerem, wykonywane jest żądanie ponownego połączenia przy użyciu tej samej logiki. Model eksploatacji bezpieczeństwa LDAP nie obsługuje odwołań. Ważne jest, aby serwery replikacji były zsynchronizowane.

Klient komunikuje się z serwerem informacji o bezpieczeństwie LDAP za pomocą demona istniejącego na kliencie (**secldapcIntd**). Jeśli moduł ładowalny LDAP jest włączony na tym kliencie, komendy wysokiego poziomu dla klientów zdefiniowanych w protokole LDAP są kierowane do demona przez bibliotekę API. Demon obsługuje pamięć podręczną żądanych pozycji protokołu LDAP. Jeśli odpowiedź na żądanie nie zostanie znaleziona w pamięci podręcznej, demon odpytuje serwer, aktualizuje pamięć podręczną i zwraca informację z powrotem do programu wywołującego.

Podczas konfigurowania klienta dla komendy **mksecldap** można podać inne opcje strojenia, takie jak ustawienie liczby wątków używanych przez demon, wielkość pozycji pamięci podręcznej i limit czasu wygaśnięcia tej pamięci. Opcje te są przeznaczone tylko dla doświadczonych użytkowników. W większości środowisk wystarczają wartości domyślne.

Podczas końcowych kroków konfigurowania klienta komenda **mksecldap** uruchamia demon po stronie klienta i dodaje pozycję do pliku `/etc/inittab`, dzięki czemu demon ten jest uruchamiany podczas każdego restartu. Aby stwierdzić, czy konfigurowanie zostało wykonane pomyślnie, należy sprawdzić proces demona **secldapcIntd** za pomocą komendy **ls-secldapclntd**. Przy założeniu, że serwer informacji o zabezpieczeniach LDAP jest skonfigurowany i uruchomiony, demon będzie działał, jeśli jego konfiguracja została pomyślnie wykonana.

Informacje o zabezpieczeniach serwera LDAP muszą być skonfigurowane przed skonfigurowaniem klienta. Konfiguracja klienta zależy od zmigrowanych danych na serwerze. Wykonaj poniższe kroki, aby zainstalować i skonfigurować klienta:

1. Zainstaluj zestawy plików powiązane z pakietem GSKit jako użytkownik root.
   a. Podłącz dysk DVD z pakietem rozszerzeń systemu AIX 7.2.
   b. Zmień katalog na położenie zestawu plików GSKit.

   ```
   cd <punkt_podłączenia>/installp/ppc
   ```

2. Uruchom komendę **installp**, aby zainstalować pakiety GSKit.
   - Aby zainstalować 64-bitowe pakiety GSKit, wprowadź następujące komendy:

     ```
     installp -acXgYd . GSKit8.gskcrypt64.ppc.rte
     installp -acXgYd . GSKit8.gskssl64.ppc.rte
     ```

   - Aby zainstalować 32-bitowe pakiety GSKit, wprowadź następujące komendy:

     ```
     installp -acXgYd . GSKit8.gskcrypt32.ppc.rte
     installp -acXgYd . GSKit8.gskssl32.ppc.rte
     ```

     Uwaga: W celu zainstalowania zestawów plików GSKit z dysku DVD można także użyć programu SMIT lub SMITTY.

3. Zainstaluj klienty *idsldap* jako użytkownik root.
   a. Podłącz drugi wolumin (wolumin 2 z 2) dysku DVD systemu AIX 7.2.
   b. Uruchom komendę **idsLicense**.

   ```
   cd <punkt_podłączenia>/license
   ./idsLicense
   ```

4. Jeśli zgadzasz się na warunki umowy licencyjnej na oprogramowanie, wprowadź cyfrę 1 z poniższej listy dostępnych opcji:

```
1: zaakceptowanie umowy licencyjnej.
2: odrzucenie umowy licencyjnej i zakończenie instalacji.
3: wydrukowanie umowy licencyjnej.
4: wyświetlenie warunków firm innych niż IBM znajdujących się w umowie licencyjnej.
99: powrót do poprzedniego ekranu.
```

   Po zaakceptowaniu warunków umowy licencyjnej na oprogramowanie w katalogu instalacyjnym serwera IBM Security Directory Server tworzony jest plik LAPID i folder licencji. W folderze licencji znajdują się pliki licencji serwera IBM Security Directory Server we wszystkich obsługiwanych językach.
5. Określ pakiety klienta serwera IBM Security Directory Server *idsldap*, które należy zainstalować.
   - Dla działania klienta LDAP bez obsługi SSL należy zainstalować następujące zestawy plików:
     - idsldap.license64
     - idsldap.cltbase64
     - idsldap.clt32bit64
     - idsldap.clt64bit64
   - Dla działania klienta LDAP z obsługą SSL należy zainstalować następujące zestawy plików:
     - idsldap.license64
     - idsldap.cltbase64
     - idsldap.clt32bit64
     - idsldap.clt64bit64
     - idsldap.clt_max_crypto32bit64
     - idsldap.clt_max_crypto64bit64

     Uwaga: Funkcjonalność SSL wymaga zainstalowania zestawów plików GSKitv8.
6. Zainstaluj pakiety klienta produktu IBM Security Directory Server *idsldap*.
   - Aby zainstalować jeden lub więcej pakietów klienta IBM Security Directory Server *idsldap*, uruchom następujące komendy:

```
cd <punkt_podłączenia>/installp/ppc/
installp -acXgYd . <nazwy_pakietów>
```

     Uwaga: Do zainstalowania zidentyfikowanych zestawów plików i pakietów z dysku DVD można także użyć programu SMIT lub SMITTY.
7. Sprawdź, czy instalacja serwera IBM Security Directory Server zakończyła się pomyślnie, korzystając z podsumowania instalacji wygenerowanej przez system.
8. Aby skonfigurować klienta LDAP, uruchom następującą komendę, zastępując wartości odpowiednio do używanego środowiska:

```
# mksecldap -c -h server1.ibm.com -a cn=admindn -p adminpwd -d cn=basedn
```

Informacje pokrewne

Komenda mksecldap

Komenda secldapclntd

Włączanie obsługi grup sieciowych LDAP dla klienta

Grup sieciowych można używać jako części protokołu NIS-LDAP (metody tłumaczenia nazw).

Aby włączyć obsługę grup sieciowych LDAP dla klienta:

1. Zainstaluj i skonfiguruj zarządzanie grupami użytkowników oparte na protokole LDAP zgodnie z opisem w sekcji ldap_client_setup.dita.

Jeśli konfigurowanie grupy sieciowej nie jest zakończone, każdy użytkownik zdefiniowany przy użyciu protokołu LDAP będzie pokazany w systemie. Na przykład, jeśli *nguser* jest użytkownikiem grupy sieciowej należącym do grupy sieciowej *mygroup*, która jest już zdefiniowana na serwerze LDAP, komenda `lsuser -R LDAP nguser` pokaże użytkownika.

2. Aby włączyć funkcję grupy sieciowej, definicja modułu dla LDAP w pliku `/usr/lib/security/methods.cfg` musi zawierać atrybut options z wartością netgroup. Należy zmienić plik `/usr/lib/security/methods.cfg`, dodając w sekcji LDAP wiersz `options = netgroup`. Spowoduje to oznaczenie modułu ładowalnego LDAP jako moduł obsługujący grupy sieciowe. Na przykład:

   ```
   LDAP:
         program = /usr/lib/security/LDAP
         program_64 =/usr/lib/security/LDAP64
         options = netgroup
   ```

   Teraz komendy `lsuser -R LDAP nguser` lub `lsuser nguser` lub `lsuser -R LDAP -a ALL` nie pokażą żadnych użytkowników. Serwer LDAP jest teraz widziany przez klienta tylko jako baza danych grup sieciowych, a żadna grupa sieciowa nie została jeszcze temu klientowi udostępniona.

3. Zmień plik `/etc/passwd`, dodając wiersz dla grupy sieciowej, która powinna mieć dostęp do systemu. Jeśli na przykład *mygroup* jest grupą sieciową na serwerze LDAP zawierającą wymaganego użytkownika, dodaj wiersz:

   ```
   +@mygroup
   ```

4. Zmień plik `/etc/group`, dodając wiersz `+:`, aby włączyć wyszukiwania NIS dla grup:

   ```
   +:
   ```

   Teraz uruchomienie komendy `lsuser nguser` zwróci użytkownika, ponieważ użytkownik *nguser* należy do grupy sieciowej *mygroup*.

   Komenda `lsuser -R LDAP nguser` nie znajdzie użytkownika, ale znajdzie go komenda `lsuser -R compat nguser`, ponieważ jest on teraz traktowany jako użytkownik **compat**.

5. Aby użytkownicy grupy sieciowej byli uwierzytelniani w systemie, mechanizm uwierzytelniania systemu AIX musi znać odpowiednią metodę. Jeśli domyślna sekcja w pliku `/etc/security/user` zawiera pozycję `SYSTEM = compat`, to w systemie mogą uwierzytelniać się wszyscy użytkownicy grupy sieciowej dodanej do pliku `/etc/passwd`. Inna możliwość to indywidualne konfigurowanie użytkowników przez ręczne dodanie sekcji do pliku `/etc/security/user` dla odpowiednich użytkowników. Przykładowa sekcja dla użytkownika *nguser*:

   ```
   nguser:
           SYSTEM = compat
           registry = compat
   ```

   Użytkownicy grupy sieciowej w dozwolonych grupach mogą teraz uwierzytelniać się w systemie.

   Włączenie opcji grup sieciowych aktywuje także następujące warunki:

   - Użytkownicy zdefiniowani w pliku `/etc/security/user` jako członkowie rejestru LDAP (z parametrami `registry=LDAP` i `SYSTEM="LDAP"`) nie mogą uwierzytelniać się jako użytkownicy LDAP. Są teraz użytkownikami **nis_ldap** i wymagają rodzimej przynależności do grupy sieciowej NIS.
   - Znaczenie rejestru compat zostało rozwinięte w celu włączenia modułów korzystających z grupy sieciowej. Na przykład, jeśli moduł LDAP ma włączoną obsługę grupy sieciowej, compat obejmuje rejestry plików, NIS oraz LDAP. Użytkownicy pobrani z tych modułów mają wartość rejestru compat.

Informacje pokrewne

- Dokument exports File for NFS
- Dokument .rhosts File Format for TCP/IP
- Dokument hosts.equiv File Format for TCP/IP

Obsługiwane serwery LDAP
Zarządzanie grupami i użytkownikami oparte na LDAP w AIX obsługuje serwery IBM Tivoli Directory Server, serwery inne niż IBM ze schematem zgodnym z RFC 2307 i serwery Microsoft Active Directory.

IBM Tivoli Directory Server

Zaleca się skonfigurowanie zarządzania grupami/użytkownikami AIX za pomocą serwerów IBM Tivoli Directory Server. Więcej informacji na temat konfigurowania serwera IBM Tivoli Directory Server pod kątem zarządzania użytkownikami i grupami zawiera sekcja Konfigurowanie serwera informacji o bezpieczeństwie IBM Tivoli Directory Server.

Serwery katalogów inne niż IBM

System AIX obsługuje wiele serwerów katalogów, których użytkownicy i grupy są zdefiniowane za pomocą schematu RFC 2307. Gdy system AIX jest skonfigurowany jako klient LDAP dla takich serwerów, to używa on tych serwerów w ten sam sposób, jak serwera IBM Tivoli Directory Server ze schematem RFC 2037. Serwery te muszą obsługiwać protokół LDAP w wersji 3.

Ponieważ schemat RFC 2307 definiuje tylko podzbiór atrybutów użytkowników i grup, których system AIX może używać, niektóre funkcje zarządzania użytkownikami i grupami systemu AIX nie mogą być realizowane, jeśli system AIX jest skonfigurowany pod kątem użycia takiego serwera LDAP (na przykład wymuszanie resetowania haseł użytkowników, historia haseł, limit zasobów dla użytkownika, kontrola logowania w niektórych systemach za pomocą atrybutów AIX: `hostsallowedlogin` i `hostsdeniedlogin` itd.).

System AIX nie obsługuje serwerów katalogów niezgodnych z RFC 2307. Jednak system AIX można skonfigurować do pracy z takimi serwerami niezgodnymi z RFC 2307, których użytkownicy i grupy są zdefiniowane ze wszystkimi wymaganymi atrybutami UNIX. Minimalnym zestawem atrybutów użytkowników i grup wymaganym przez system AIX jest zestaw zdefiniowany w RFC 2307. Obsługa takich serwerów katalogów wymaga konfiguracji ręcznej. System AIX udostępnia do tego celu mechanizm odwzorowania schematu. Więcej informacji na temat formatu i użycia pliku schematu zawiera sekcja Format pliku odwzorowania atrybutów LDAP.

Microsoft Active Directory

System AIX obsługuje Microsoft Active Directory (AD) jako serwer LDAP do zarządzania użytkownikami i grupami. Serwer Active Directory musi mieć zainstalowany schemat obsługi UNIX. Schemat obsługi UNIX produktu Active Directory pochodzi z pakietu Microsoft Service For UNIX (SFU). Każda wersja SFU zawiera nieco inne definicje schematu użytkowników i grup w porównaniu do wersji poprzednich. System AIX obsługuje produkt Active Directory działający w systemach Windows 2000 i 2003 ze schematem SFU w wersji 3.0 i 3.5 oraz produkt Active Directory działający w systemie Windows 2003 R2 z wbudowanym schematem UNIX.

Z powodu różnicy w zarządzaniu użytkownikami i grupami w systemach UNIX i systemach Windows, nie wszystkie komendy systemu AIX mogą działać dla użytkowników LDAP, jeśli serwerem jest Active Directory. Przykładowymi komendami, które nie działają, są **mkuser** i **mkgroup**. Większość komend zarządzania użytkownikami i grupami jednak działa, w zależności od praw dostępu nadanych tożsamości, której system AIX używa do połączenia z Active Directory. Dotyczy to komend: **lsuser**, **chuser**, **rmuser**, **lsgroup**, **chgroup**, **rmgroup**, **id**, **groups**, **passwd** i **chpasswd**.

System AIX obsługuje dwa mechanizmy uwierzytelniania użytkowników na serwerach Windows: uwierzytelnianie LDAP i uwierzytelnianie Kerberos. W każdym z tych mechanizmów system AIX obsługuje identyfikację użytkowników za pomocą protokołu LDAP w Active Directory, przy czym nie jest wymagane odpowiednie konto użytkownika w systemie AIX.

Konfigurowanie systemu operacyjnego AIX do pracy z Active Directory przez LDAP
System AIX obsługuje Microsoft Active Directory (AD) jako serwer LDAP do zarządzania użytkownikami i grupami. Serwer Active Directory musi mieć zainstalowany schemat obsługi UNIX.

Administrator może użyć komendy **mksecldap** do skonfigurowania systemu AIX na serwerze Active Directory w taki sam sposób, jak serwer IBM Tivoli Directory Server. Komenda **mksecldap** ukrywa

wszystkie szczegóły konfigurowania w celu uproszczenia procesu. Przed uruchomieniem komendy **mksecldap** w celu skonfigurowania systemu AIX na serwerze Active Directory:

1. Na serwerze Active Directory musi być zainstalowany schemat obsługi UNIX.
2. Serwer Active Directory musi zawierać użytkowników obsługujących system UNIX.

Więcej informacji na temat instalowania schematu UNIX w Active Directory i włączania użytkowników Active Directory do obsługi systemu UNIX zawiera odpowiednia dokumentacja Microsoft.

Schemat Active Directory często zawiera wiele definicji atrybutów dla tego samego atrybutu systemu UNIX (na przykład istnieje wiele definicji haseł użytkowników i członków grupy). Chociaż system AIX obsługuje większość z nich, wybierając definicje, które mają być używane, należy zachować rozwagę i przeprowadzić staranne planowanie. Zaleca się, aby w celu uniknięcia konfliktów systemy AIX i systemy inne niż AIX współużytkujące ten sam katalog Active Directory używały tej samej definicji.

Wybór atrybutu hasła Active Directory
AIX obsługuje dwa mechanizmy uwierzytelniania: **unix_auth** i **ldap_auth**.

W przypadku **unix_auth** hasło w Microsoft Active Directory (AD) musi być w postaci zaszyfrowanej. Podczas uwierzytelniania zaszyfrowane hasło jest pobierane z Active Directory i porównywane z zaszyfrowaną postacią hasła wprowadzonego przez użytkownika. Uwierzytelnianie jest pomyślne, gdy są one zgodne. W trybie **ldap_auth** system AIX uwierzytelnia użytkownika za pomocą operacji połączenia LDAP z serwerem z tożsamością danego użytkownika i z podanym hasłem. Użytkownik jest uwierzytelniany, jeśli operacja połączenia powiedzie się. Active Directory obsługuje wiele atrybutów hasła użytkownika. Różne tryby uwierzytelniania AIX wymagają różnych atrybutów hasła użytkownika Active Directory.

Tryb unix_auth

Dla trybu **unix_auth** można użyć następujących atrybutów haseł Active Directory:

- **userPassword**
- **unixUserPassword**
- **msSFU30Password**

Zarządzanie hasłami w systemie AIX może być trudne z powodu istnienia wielu atrybutów haseł w Active Directory. Stwierdzenie, które atrybuty zarządzania hasłami powinny być używane przez klientów UNIX może nie być łatwe. Dzięki możliwości odwzorowania atrybutów LDAP w systemie AIX umożliwia dostosowanie zarządzania hasłami stosowanie do potrzeb.

Domyślnie system AIX używa atrybutu **msSFU30Password** dla Active Directory w systemach Windows 2000 i 2003 oraz atrybutu **userPassword** w systemie Windows 2003 R2. Jeśli używane jest inne hasło, należy zmodyfikować plik `/etc/security/ldap/sfu30user.map` (lub plik `/etc/security/ldap/sfur2user.map`, jeśli Active Directory działa w systemie Windows 2003 R2). Należy znaleźć wiersz rozpoczynający się słowem **spassword** i zmienić trzecie pole tego wiersza na żądaną nazwę atrybutu hasła Active Directory. Więcej informacji na ten temat zawiera sekcja Format pliku odwzorowania atrybutów LDAP. Po wprowadzeniu zmiany należy uruchomić komendę **mksecldap**, aby skonfigurować klienta LDAP AIX. Jeśli klient LDAP AIX jest już skonfigurowany, należy uruchomić komendę **restart-secldapclntd**, aby restartować demon **secldapclntd** w celu uwzględnienia tej zmiany.

W trybie **unix_auth** hasło może być niezsynchronizowane między systemami Windows i UNIX, w wyniku czego będą istniały różne hasła dla każdego systemu. Dzieje się tak wtedy, gdy zmieniane jest hasło z systemu AIX na hasło w systemie Windows, ponieważ system Windows używa atrybutu hasła **uncodepwd**. Komenda **passwd** w systemie AIX może zresetować hasło systemu UNIX, tak aby było takie samo, jak hasło Windows, ale system AIX nie obsługuje automatycznej zmiany hasła Windows po zmianie hasła UNIX w systemie AIX.

Tryb ldap_auth

W Active Directory występuje także atrybut hasła **unicodepwd**. Atrybut ten jest używany przez systemy Windows do uwierzytelniania użytkowników Windows. Podczas wykonywania operacji połączenia z Active

Directory należy użyć hasła **unicodePwd**. Żadne spośród haseł podanych dla trybu **unix_auth** nie będzie działało dla operacji połączenia. Jeśli opcja **ldap_auth** zostanie podana w wierszu komend, komenda **mksecldap** odwzoruje ten atrybut hasła na atrybut **unicodePwd** Active Directory w konfiguracji klienta bez konieczności ręcznego wykonywania jakichkolwiek kroków.

Dzięki odwzorowaniu haseł AIX za pomocą atrybutu **unicodePwd** użytkownicy zdefiniowani w Active Directory mogą zalogować się w systemach Windows i AIX, używając tego samego hasła. Zresetowanie hasła w systemie AIX lub Windows obowiązuje zarówno w systemie AIX, jak i w systemie Windows.

Wybór atrybutów członków grupy Active Directory
Opracowana przez firmę Microsoft usługa Service for UNIX definiuje atrybuty członka grupy: **memberUid**, **msSFU30MemberUid** i **msSFU30PosixMember**.

Atrybuty **memberUid** i **msSFU30MemeberUid** akceptują nazwy kont użytkowników, a atrybut **msSFU30PosixMember** akceptuje tylko pełną nazwę wyróżniającą. Na przykład dla konta użytkownika *foo* (o nazwisku *bar*) zdefiniowanego w Active Directory:

- **memberUid: foo**
- **msSFU30MemberUid: foo**
- **msSFU30PosixMember: CN=foo bar,CN=Users,DC=austin,DC=ibm,DC=com**

System operacyjny AIX obsługuje wszystkie te atrybuty. Aby określić atrybut, który ma być używany, należy skontaktować się z administratorem Active Directory. Domyślnie komenda **mksecldap** konfiguruje system operacyjny AIX, tak aby używał atrybutu **msSFU30PosixMember** dla Active Directory w systemach Windows 2000 i 2003, a także atrybutu **uidMember** dla Active Directory w systemach Windows 2003 R2. Taki wybór wynika z tego, że Active Directory wybiera atrybut podczas dodawania użytkownika do grupy z systemu Windows. Strategia biznesowa może wymagać użycia atrybutu członka grupy innego niż domyślny w celu zapewnienia obsługi wielu platform.

Jeśli potrzebny jest inny atrybut członka grupy, można zmienić odwzorowanie, edytując plik odwzorowania grupy. Plikiem odwzorowania grupy dla Active Directory jest `/etc/security/ldap/sfu30group.map` w systemach Windows 2000 i 2003 oraz `/etc/security/ldap/sfur2group.map` w systemie Windows 2003 R2. Należy znaleźć wiersz rozpoczynający się słowem **users** i zastąpić trzecie pole żądaną nazwą atrybutu dla członków grupy. Więcej informacji na ten temat zawiera sekcja Format pliku odwzorowania atrybutów LDAP. Po wprowadzeniu zmiany należy uruchomić komendę **mksecldap**, aby skonfigurować klienta LDAP systemu AIX lub jeśli system AIX jest już skonfigurowany, należy uruchomić komendę **restart-secldapclntd**, aby restartować demon **secldapclntd** w celu uwzględnienia tej zmiany.

Wiele jednostek organizacyjnych
Serwer Active Directory może mieć zdefiniowanych wiele jednostek organizacyjnych, z których każda zawiera zestaw użytkowników.

Większość użytkowników Windows Active Directory jest zdefiniowana w poddrzewie **cn=users,...**, ale niektórzy mogą być zdefiniowani w innym miejscu. W przypadku takiego serwera Active Directory można użyć opcji wielu podstawowych nazw wyróżniających systemu AIX. Więcej informacji na ten temat zawiera sekcja Obsługa wielu podstawowych nazw wyróżniających.

Uwierzytelnianie Kerberos dla serwerów Windows
Oprócz mechanizmów uwierzytelniania LDAP system operacyjny AIX obsługuje także uwierzytelnianie użytkowników za pomocą protokołu Kerberos dla serwerów Windows.

System operacyjny AIX obsługuje uwierzytelnianie Kerberos dla identyfikatorów KDC i LDAP Windows dla Windows Active Directory przez utworzenie złożonego modułu ładowalnego KRB5ALDAP. Ponieważ informacje o identyfikatorach użytkowników są pobierane z Microsoft Active Directory, nie trzeba tworzyć odpowiadających im kont użytkowników w systemie AIX.

Zarządzanie użytkownikami LDAP
Użytkownikami i grupami na serwerze informacji o bezpieczeństwie LDAP można zarządzać z dowolnego klienta LDAP za pomocą komend wysokiego poziomu.

Użytkownikami i grupami na serwerze informacji o zabezpieczeniach LDAP można zarządzać przy użyciu protokołu LDAP i innych modułów ładowalnych uwierzytelniania, takich jak DCE, NIS i KRB5 przy użyciu komend wysokiego poziomu i opcji *-R*. Więcej informacji na temat opcji *-R* można znaleźć w każdej z komend zarządzania użytkownikami lub grupami.

Aby umożliwić uwierzytelnianie użytkownika za pomocą protokołu LDAP, należy uruchomić komendę **chuser**, zmieniającą wartość atrybutu *SYSTEM* użytkownika na LDAP. Po zmianie wartości atrybutu *SYSTEM* stosownie do zdefiniowanej składni, użytkownik może być uwierzytelniany za pomocą więcej niż jednego modułu ładowalnego, takich jak na przykład compat i LDAP. Więcej informacji na temat ustawiania metod uwierzytelniania użytkowników zawiera sekcja “Uwierzytelnianie użytkowników” na stronie 73 oraz składnia atrybutu *SYSTEM*, która jest zdefiniowana w pliku `/etc/security/user`.

Dla użytkownika można ustawić uwierzytelnianie LDAP podczas konfigurowania klienta przez uruchomienie komendy **mksecldap** z opcją *-u* w jednej z następujących postaci:

- ```
  mksecldap -c -u użytkownik1,użytkownik2,...
  ```

  Gdzie: *użytkownik1, użytkownik2,...* jest listą użytkowników. Użytkownicy podani na liście mogą być użytkownikami zdefiniowanymi lokalnie lub zdalnie za pomocą protokołu LDAP. Atrybut *SYSTEM* jest ustawiany na LDAP w sekcjach wszystkich wymienionych użytkowników w pliku `/etc/security/user`. Tacy użytkownicy są uwierzytelniani tylko za pomocą protokołu LDAP. Użytkownicy podani na tej liście muszą istnieć na serwerze LDAP, w przeciwnym razie nie mogą się zalogować z hosta. Aby zmodyfikować atrybut *SYSTEM* i umożliwić uwierzytelnianie za pomocą wielu metod, na przykład lokalnie lub przez LDAP, należy uruchomić komendę **chuser**.

- ```
  mksecldap -c -u ALL
  ```

  Powoduje ona ustawienie atrybutu *SYSTEM* na LDAP w sekcjach wszystkich lokalnie zdefiniowanych użytkowników w pliku `/etc/security/user`. Wszyscy ci użytkownicy są uwierzytelniani tylko za pomocą protokołu LDAP. Lokalnie zdefiniowani użytkownicy muszą istnieć na serwerze informacji o bezpieczeństwie LDAP, w przeciwnym razie nie mogą się zalogować z hosta. Użytkownik zdefiniowany na serwerze LDAP, ale niezdefiniowany lokalnie nie może się zalogować z tego hosta. Aby umożliwić użytkownikowi zdefiniowanemu zdalnie za pomocą protokołu LDAP zalogowanie się z tego hosta, należy uruchomić komendę **chuser**, która ustawi dla tego użytkownika atrybut *SYSTEM* na wartość LDAP.

Alternatywnie można włączyć wszystkich użytkowników LDAP bez względu na to, czy są oni zdefiniowani lokalnie, czy też nie, w celu uwierzytelnienia ich za pomocą LDAP na lokalnym hoście, modyfikując sekcję "default" w pliku `/etc/security/user`, tak aby używana była wartość "LDAP". Dla wszystkich użytkowników, którzy nie mają zdefiniowanej wartości dla atrybutu *SYSTEM*, należy użyć wartości zdefiniowanej w sekcji "default". Na przykład, jeśli w sekcji "default" znajduje się `"SYSTEM = "compat""`, zmiana wartości na `"SYSTEM = "compat OR LDAP""` umożliwia uwierzytelnianie wszystkich użytkowników LDAP za pomocą AIX lub LDAP. Zmiana sekcji default na `"SYSTEM = "LDAP""` umożliwia uwierzytelnianie wyłącznie za pomocą LDAP. Użytkowników, dla których zdefiniowano wartość atrybutu *SYSTEM*, ta sekcja default nie dotyczy.

Zadania pokrewne

Konfigurowanie klienta LDAP

Aby skonfigurować klienta w celu używania protokołu LDAP do uwierzytelniania i uzyskiwania informacji o użytkownikach i grupach, należy upewnić się, że każdy klient ma zainstalowany pakiet klienta LDAP. Więcej informacji na temat instalowania pakietu klienta LDAP można znaleźć w krokach od “3” na stronie 163 do “7” na stronie 164. Jeśli wymagane jest użycie protokołu SSL (Secure Sockets Layer) lub TLS (Transport Layer Security), musi być zainstalowany pakiet GSKit. Należy utworzyć klucz i dodać do niego certyfikat klucza SSL serwera LDAP. Patrz kroki od “1” na stronie 163 do “2” na stronie 163.

Konfigurowanie serwera IBM Security Directory Server

Aby skonfigurować system jako serwer informacji o bezpieczeństwie LDAP udostępniający informacje o uwierzytelnianiu, użytkownikach i grupach za pomocą LDAP, należy najpierw zainstalować pakiety serwera i klienta LDAP.

Obsługa wielu podstawowych nazw wyróżniających
W systemie AIX obsługiwanych jest wiele podstawowych nazw wyróżniających. W pliku `/etc/security/ldap/ldap.cfg` można podać do 10 podstawowych nazw wyróżniających dla każdej jednostki.

Podstawowe nazwy wyróżniające są uszeregowane pod względem ważności w pliku `/etc/security/ldap/ldap.cfg`. Operacja wykonywana przez komendy AIX w przypadku wielu podstawowych nazw wyróżniających jest realizowana zgodnie z priorytetem podstawowej nazwy wyróżniającej. Obowiązują tu następujące zasady:

- Operacja zapytania (na przykład wykonywana przez komendę **lsuser**) jest wykonywana na podstawowych nazwach wyróżniających zgodnie z ich priorytetem do momentu znalezienia zgodnego konta. Jeśli w wyniku przeszukania wszystkich podstawowych nazw wyróżniających nie zostanie znalezione zgodne konto, zostanie zwrócona informacja o niepowodzeniu. Zapytanie o WSZYSTKO powoduje zwrócenie wszystkich kont z każdej podstawowej nazwy wyróżniającej.
- Operacja modyfikacji (na przykład wykonywana przez komendę **chuser**) jest realizowana do znalezienia pierwszego zgodnego konta.
- Operacja usuwania (na przykład wykonywana przez komendę **rmuser**) jest realizowana do znalezienia pierwszego zgodnego konta.
- Operacja tworzenia (na przykład wykonywana przez komendę **mkuser**) jest realizowana tylko do pierwszej podstawowej nazwy wyróżniającej. System AIX nie obsługuje tworzenia kont w innych podstawowych nazwach wyróżniających.

Za utrzymanie bezkolizyjnej bazy danych kont odpowiada administrator serwera katalogów. Jeśli istnieje wiele definicji tego samego konta, z których każda znajduje się w innym poddrzewie, tylko pierwsze konto jest widoczne dla systemu AIX. Operacja wyszukiwania zwraca tylko pierwsze zgodne konto. Podobnie operacja modyfikacji lub usuwania jest wykonywana tylko dla pierwszego zgodnego konta.

Komenda **mksecldap** używana do konfigurowania klienta LDAP znajdzie podstawową nazwę wyróżniającą dla każdej pozycji i zapisze ją w pliku `/etc/security/ldap/ldap.cfg`. Gdy dla jednostki na serwerze LDAP dostępnych jest wiele podstawowych nazw wyróżniających, komenda **mksecldap** losowo używa jednej z nich. Aby system AIX działał z wieloma podstawowymi nazwami wyróżniającymi, należy zmienić plik `/etc/security/ldap/ldap.cfg` po pomyślnym zakończeniu komendy **mksecldap**. Należy znaleźć odpowiednią definicję podstawowej nazwy wyróżniającej i dodać kolejną potrzebną podstawową nazwę wyróżniającą. System AIX obsługuje do 10 podstawowych nazw wyróżniających dla każdej jednostki. Dodatkowe podstawowe nazwy wyróżniające są ignorowane.

System AIX obsługuje także zdefiniowany przez użytkownika filtr i zasięg wyszukiwania dla każdej podstawowej nazwy wyróżniającej. Podstawowa nazwa wyróżniająca może mieć własny filtr i zasięg różne od filtru i zasięgu podstawowych nazw wyróżniających na poziomie węzła. Do zdefiniowania zestawu kont widocznych dla systemu AIX można użyć filtrów.

Dla systemu AIX widoczne są tylko te konta, które spełniają kryteria filtru.

Konfigurowanie warstwy SSL na serwerze LDAP
Aby skonfigurować protokół Secure Sockets Layer (SSL) na serwerze LDAP, należy zainstalować zestawy plików szyfrowania LDAP i zestawy plików **GSKit**, aby włączyć obsługę szyfrowania serwera. Powyższe zestawy plików znajdują się w pakiecie rozszerzenia systemu AIX.

Wykonaj poniższe kroki, aby włączyć obsługę protokołu SSL dla uwierzytelniania serwera katalogów IBM.

1. Zainstaluj pakiet GSKitv8 dla serwera IBM Security Directory Server w wersji 6.4. Więcej informacji na temat instalowania pakietu GSKitv8 dla serwera IBM Security Directory Server w wersji 6.4 można znaleźć w sekcji “Konfigurowanie serwera IBM Security Directory Server” na stronie 159.
2. Wygeneruj klucz prywatny i certyfikat serwera IBM Directory Server, korzystając z odpowiedniego programu narzędziowego GSKit do zarządzania kluczami. Konieczne jest użycie komendy **gsk8capicmd** lub **gsk8capicmd_64** dla serwera IBM Security Directory Server w wersji 6.4 lub nowszej.

   Uwaga: Certyfikat serwera może zostać podpisany przez komercyjny ośrodek certyfikacji (CA), taki jak VeriSign. Alternatywnie, narzędzie do zarządzania kluczami GSKit może samodzielnie podpisać

certyfikat serwera. Certyfikat publiczny (lub certyfikat samopodpisany) ośrodka CA należy także wysłać do pliku bazy danych kluczy aplikacji klienta.

3. Zapisz plik bazy danych kluczy serwera oraz powiązany plik ukrytych haseł na serwerze. Domyślna ścieżka dla katalogu bazy danych kluczy `/usr/ldap/etc` jest typowa.
4. Uruchom następującą komendę, w której `klucze.kdb` jest bazą danych kluczy, a *hasło* jest hasłem do bazy danych kluczy:

```
# mksecldap -s -a cn=admin -p pwd -S rfc2307aix -k /usr/ldap/etc/klucze.kdb -w hasło
```

Konfigurowanie warstwy SSL na kliencie LDAP
Aby użyć protokołu SSL w kliencie LDAP, należy zainstalować zestawy plików `idsldap.clt_max_crypto32bit64` i `idsldap.clt_max_crypto64bit64` z drugiego woluminu dysku DVD AIX wraz z zestawami plików pakietu Global Security Kit (GSKit) z dysku DVD pakietu rozszerzeń systemu AIX®.

Wykonaj poniższe kroki po skonfigurowaniu protokołu SSL na serwerze LDAP.

1. Uruchom komendę **gsk8capicmd** lub **gsk8capicmd_64**, aby wygenerować bazę danych kluczy na każdym kliencie. Więcej informacji na temat generowania bazy danych kluczy na każdym kliencie można znaleźć w sekcji *On the C-based LDAP client system* w serwisie WWW The gskcapicmd tool.
2. Skopiuj certyfikat serwera do każdego klienta. Jeśli serwer SSL korzysta z certyfikatu samopodpisanego, należy najpierw wyodrębnić certyfikat.
3. W każdym systemie klienckim uruchom komendę **gsk8capicmd** lub **gsk8capicmd_64**, aby dodać certyfikat serwera do bazy danych kluczy.
4. Aby włączyć obsługę SSL dla każdego klienta, uruchom następującą komendę:

```
# mksecldap -c -h nazwa serwera -a nazwa wyr admin -p hasło -k /usr/ldap/etc/klucze.kdb -p
hasło
```

   Pełna ścieżka do bazy danych kluczy to `/usr/ldap/etc/mykey.kdb`, a hasło do klucza to *hasło*. Jeśli hasło do bazy danych kluczy nie zostanie wpisane w wierszu komend, zostanie użyty plik ukrytych haseł z tego samego katalogu. Plik ukrytych haseł musi mieć taką samą nazwę, jak baza danych kluczy z rozszerzeniem `.sth`, na przykład `klucze.sth`).

Kontrola dostępu do hosta LDAP
System AIX umożliwia kontrolę dostępu (przez logowanie) do hosta na poziomie użytkowników. Administratorzy mogą skonfigurować użytkowników LDAP, tak aby mogli oni logować się do systemu AIX, ustawiając atrybut **SYSTEM** tych użytkowników na LDAP.

Atrybut **SYSTEM** jest zdefiniowany w pliku `/etc/security/user`. Aby ustawić wartość tego argumentu, można użyć komendy **chuser**. Na przykład:

```
# chuser -R LDAP SYSTEM=LDAP registry=LDAP foo
```

Uwaga: Gdy stosowany jest ten typ kontroli, nie należy ustawiać domyślnego atrybutu **SYSTEM** na LDAP, ponieważ umożliwiłoby to logowanie się do systemu wszystkim użytkownikom LDAP.

Wykonanie powyższej komendy powoduje ustawienie atrybutu LDAP, umożliwiające użytkownikowi *foo* zalogowanie się w tym systemie. Komenda ta ustawia także rejestr LDAP, co umożliwia procesowi logowania zaprotokołowanie liczby prób logowania się użytkownika *foo* w LDAP i wykonywanie zadań zarządzania użytkownikiem w LDAP.

Administrator musi wykonać takie konfigurowanie na każdym z klientów, aby włączyć logowanie niektórych użytkowników.

W systemie AIX dostępna jest opcja ograniczenia logowania użytkownika LDAP tylko do niektórych klientów LDAP. Opcja ta umożliwia scentralizowane zarządzanie kontrolą dostępu do hosta. Administratorzy mogą określić dwie listy kontroli dostępu do hosta dla konta użytkownika: listę dozwolonego dostępu i listę odmowy dostępu. Te dwa atrybuty użytkownika są zapisane na serwerze LDAP wraz z kontem użytkownika. Użytkownik może uzyskać dostęp do systemów lub sieci, które znajdują

się na liście dozwolonego dostępu i nie może uzyskać dostępu do systemów lub sieci, które znajdują się na liście odmowy dostępu. Jeśli dany system został podany na obu listach, użytkownik nie może uzyskać dostępu do systemu. Istnieją dwa sposoby podania list dostępu dla użytkownika: za pomocą komendy **mkuser** podczas tworzenia użytkownika lub za pomocą komendy **chuser**, gdy użytkownik już istnieje. W celu zapewnienia zgodności z wcześniejszymi wersjami, jeśli zarówno lista dozwolonego dostępu, jak i lista odmowy dostępu nie istnieją dla użytkownika, użytkownik ten domyślnie może zalogować się na dowolnym kliencie LDAP.

Przykłady konfigurowania list dozwolonego dostępu i list odmowy dostępu dla użytkowników:

```
# mkuser -R LDAP hostsallowedlogin=host1,host2 foo
```

Wykonanie tej komendy powoduje utworzenie użytkownika *foo*, który może zalogować się tylko do hostów `host1` i `host2`.

```
# mkuser -R LDAP hostsdeniedlogin=host2 foo
```

Wykonanie tej komendy powoduje utworzenie użytkownika *foo*, który może logować się do wszystkich klientów LDAP oprócz hosta `host2`.

```
# chuser -R LDAP hostsallowedlogin=192.9.200.1 foo
```

Wykonanie tej komendy powoduje nadanie użytkownikowi *foo* uprawnień do logowania się na kliencie o adresie `192.9.200.1`.

```
# chuser -R LDAP hostsallowedlogin=192.9.200/24 hostsdeniedlogin=192.9.200.1 foo
```

Wykonanie tej komendy powoduje nadanie użytkownikowi *foo* uprawnień do logowania się na wszystkich klientach w ramach podsieci `192.9.200/24`, oprócz klienta o adresie `192.9.200.1`.

Więcej informacji na ten temat zawiera pomoc do komendy **chuser**.

Bezpieczna komunikacja przy użyciu warstwy SSL
W zależności od typu uwierzytelniania używanego pomiędzy klientem LDAP a serwerem, hasło jest wysyłane w postaci zaszyfrowanej (unix_auth) lub w postaci jawnego tekstu (ldap_auth). Warstwa SSL (Secure Socket Layer) jest używana do zabezpieczania danych, kiedy przez sieć lub w pewnych wypadkach przez Internet przesyłane są hasła, nawet zaszyfrowane. System AIX udostępnia pakiet dla warstwy SSL, który zapewnia bezpieczną komunikację pomiędzy serwerem katalogów a klientami.

Więcej informacji na ten temat zawierają sekcje:

- “Konfigurowanie warstwy SSL na kliencie LDAP” na stronie 171
- “Konfigurowanie warstwy SSL na serwerze LDAP” na stronie 170

Użycie trybu tylko uwierzytelniania LDAPA
Moduł LDAP jest w pełni funkcjonalnym modułem obsługującym zarówno uwierzytelniania użytkowników, jak i identyfikację użytkowników. Moduł LDAPA udostępnia tryb tylko uwierzytelniania. Moduł LDAPA jest podobny do modułu LDAP, ale można wskazać użycie trybu tylko uwierzytelniania.

W trybie tylko uwierzytelniania modułu LDAPA należy używać w połączeniu z innym modułem bazy danych, aby utworzyć złożony moduł w miejsce modułu autonomicznego. Moduł LDAPA wykonuje uwierzytelnianie użytkowników, podczas gdy drugi moduł wykonuje identyfikację. Taki połączony moduł jest nazywany modułem złożonym. Dla tego modułu złożonego należy zdefiniować użytkowników zarówno na serwerze LDAP, jak i na serwerze bazy danych.

W module LDAPA informacje o grupie pochodzą z serwera bazy danych. Na przykład w przypadku plików LDAPA informacje o grupie pochodzą z lokalnego pliku `/etc/group`. Jeśli niektórzy użytkownicy LDAP należą tylko do grup LDAP, przed skonfigurowaniem modułu plików LDAPA należy utworzyć odpowiednie grupy LDAP na serwerze bazy danych. Tworząc taką grupę, unikniesz sytuacji, gdy użytkownik plików LDAPA nie może rozstrzygnąć ustawień grupy, ponieważ to ustawienie grupy nie istnieje na serwerze bazy danych.

Uwaga: Moduł LDAPA nie obsługuje tworzenia i usuwania użytkowników. Aby utworzyć użytkownika plików LDAPA, administrator systemu musi utworzyć użytkownika LDAP, korzystając z modułu LDAP, a następnie utworzyć lokalnie tego samego użytkownika. Następnie przekształca tego użytkownika w użytkownika plików LDAPA, ustawiając SYSTEM i rejestr tego użytkownika na `LDAPAfiles` za pomocą komendy **chuser**.

Aby za pomocą modułu LDAPA skonfigurować LDAP w trybie tylko uwierzytelniania, użyj komendy **mksecldap** z opcją `-i <moduł_bazy_danych>`. Ta komenda tworzy moduł LDAPA z ustawieniem `options = authonly` i złożony moduł ładowalny LDAPA *<moduł_bazy_danych>*.

Na przykład, aby skonfigurować LDAP w trybie tylko uwierzytelniania i użyć plików lokalnych dla modułu bazy danych, użyj następującego przykładu:

```
mksecldap -c –h <serwer ldap> -a <dn_powiązania> -p <hasło powiązania> -i pliki
```

Plik `/usr/lib/security/methods.cfg` zostanie zaktualizowany w następujący sposób:

```
LDAPA:
        program = /usr/lib/security/LDAP
        program_64 =/usr/lib/security/LDAP64
        options = authonly

LDAP:
        program = /usr/lib/security/LDAP
        program_64 =/usr/lib/security/LDAP64

LDAPAfiles:
        options = db=BUILTIN,auth=LDAPA
```

Ustawienie `options = authonly` w sekcji LDAPA wskazuje ustawienie trybu tylko uwierzytelniania dla modułu LDAPA. Sekcja `LDAPAfiles` definiuje złożony moduł ładowalny.

Moduł LDAP jest zachowywany do rozstrzygania danych innych niż użytkownika/grupy, takich jak RBAC. Moduł LDAP może być nadal używany jako autonomiczny moduł uwierzytelniania niezależnie od modułu LDAPA.

Informacje pokrewne
Komenda mksecldap

Atrybuty obsługiwane przez LDAPA
Moduł LDAPA w trybie tylko uwierzytelniania obsługuje ograniczoną liczbę atrybutów strategii haseł systemu AIX. Pozostałe atrybuty systemu AIX są spełniane przez moduł bazy danych.

Moduł LDAPA w trybie tylko uwierzytelniania obsługuje następujące atrybuty:

- maxage
- minage
- minlen
- lastupdate
- flags
- maxrepeats
- minalpha
- mindiff
- minother
- pwdwarntime
- pwdchecks
- histsize
- histexpire
- time_last_login

- time_last_unsuccessful_login
- tty_last_login
- tty_last_unsuccessful_login
- host_last_login
- host_last_unsuccessful_login
- unsuccessful_login_count
- account_locked
- loginretries
- logintimes

Nie wszystkie serwery LDAP obsługują te atrybuty. Gdy serwer LDAP nie obsługuje wszystkich podanych atrybutów, obsługiwanymi atrybutami są tylko te atrybuty, które są wspólne dla tej listy i pliku odwzorowań użytkownik-atrybut. Plik ten znajduje się w katalogu `/etc/security/ldap`.

W przypadku serwera zgodnego z RFC2307 bez obsługi schematu AIX obsługiwane są następujące atrybuty AIX:

- maxage
- minage
- lastupdate
- pwdwarntime
- lastupdate

Łączenie z wykorzystaniem protokołu Kerberos
Oprócz prostego łączenia za pomocą nazwy wyróżniającej oraz hasła łączenia, demon **secldapclntd** obsługuje także łączenie za pomocą referencji protokołu Kerberos V.

Klucze łączenia podmiotu Kerberos przechowywane są w pliku keytab i, aby można było użyć łączenia z wykorzystaniem protokołu Kerberos, muszą być dostępne dla demona **secldapclntd**. Gdy łączenie Kerberos jest włączone, demon **secldapclntd** przeprowadza uwierzytelnianie na serwerze LDAP za pomocą protokołu Kerberos, korzystając z nazwy użytkownika Kerberos oraz pliku keytab podanych w pliku konfiguracyjnym klienta `/etc/security/ldap/ldap.cfg`. Korzystanie z łączenia Kerberos powoduje, że demon **secldapclntd** ignoruje nazwę wyróżniającą oraz hasło łączenia podane w pliku `/etc/security/ldap/ldap.cfg`.

Gdy uwierzytelnianie za pomocą protokołu Kerberos powiedzie się, demon **secldapclntd** zapisuje referencje łączenia w katalogu `/etc/security/ldap/krb5cc_secldapclntd` . Zapisane referencje wykorzystywane są do późniejszego ponownego łączenia. Jeśli w momencie, gdy demon **secldapclntd** spróbuje ponownie połączyć się z serwerem LDAP, referencje będą starsze niż jedna godzina, demon **secldapclntd** reinicjuje proces odnowienia referencji.

Aby system klienta LDAP skonfigurować w celu korzystania z łączenia Kerberos, należy skorzystać z komendy **mksecldap** oraz nazwy wyróżniającej i hasła łączenia. Jeśli konfigurowanie powiedzie się, należy dokonać edycji pliku `/etc/security/ldap/ldap.cfg` podając poprawne wartości dla atrybutów związanych z protokołem Kerberos. Demon **secldapclntd** korzysta z łączenia Kerberos podczas restartu. Po pomyślnym skonfigurowaniu nazwa wyróżniająca oraz hasło łączenia nie są już używane. Mogą zostać bezpiecznie usunięte z pliku `/etc/security/ldap/ldap.cfg` lub pozostawione jako komentarz.

Tworzenie nazwy użytkownika Kerberos
W celu obsługi łączenia Kerberos, w centrum dystrybucji kluczy (KDC) należy utworzyć przynajmniej dwa podmioty Kerberos, które używane będą przez serwer i klienta IDS. Pierwszy podmiot Kerberos jest podmiotem serwera LDAP, natomiast drugi - podmiotem używanym przez systemy klienta w celu łączenia się z serwerem.

Wszystkie klucze podmiotu Kerberos muszą być umieszczone w pliku keytab, tak aby mogły być użyte do uruchomienia procesu serwera lub procesu demona klienta.

Poniższy przykład opiera się na usłudze uwierzytelniania sieciowego IBM. Jeśli oprogramowanie protokołu Kerberos zostało zainstalowane z innych źródeł, używane komendy mogą się różnić od tych pokazanych w przykładzie.

- Jako użytkownik root, na serwerze KDC uruchom narzędzie kadmin.

```
#/usr/krb5/sbin/kadmin.local
kadmin.local:
```

- Dla serwera LDAP utwórz nazwę użytkownika Kerberos ldap/*nazwa_hosta*. *Nazwa_hosta* jest pełną nazwą hosta DNS, na którym uruchomiony zostanie serwer LDAP.

```
kadmin.local: addprinc ldap/plankton.austin.ibm.com
OSTRZEŻENIE: nie określono żadnej strategii dla "ldap/
plankton.austin.ibm.com@ud3a.austin.ibm.com":
Wpisz ponownie hasło podmiotu kerberos "ldap/plankton.austin.ibm.com@ud3a.austin.ibm.com":
Podmiot kerberos "ldap/plankton.austin.ibm.com@ud3a.austin.ibm.com" został utworzony.
kadmin.local:
```

- Dla utworzonego podmiotu Kerberos serwera utwórz plik keytab. Ten klucz zostanie użyty przez serwer LDAP podczas startu. Aby utworzyć plik keytab nazwany `slapd_krb5.keytab` wpisz:

```
kadmin.local: ktadd -k /etc/security/slapd_krb5.keytab ldap/plankton.austin.ibm.com
Pozycja podmiotu kerberos ldap/plankton.austin.ibm.com o kvno 2,
typie szyfrowania Triple DES tryb cbc z HMAC/sha1 została dodana do tablicy kluczy
WRFILE:/etc/security/slapd_krb5.keytab.
Pozycja podmiotu kerberos ldap/plankton.austin.ibm.com o kvno 2,
typie szyfrowania ArcFour z HMAC/md5 została dodana do tablicy kluczy
WRFILE:/etc/security/slapd_krb5.keytab.
Pozycja podmiotu kerberos ldap/plankton.austin.ibm.com o kvno 2,
typie szyfrowania AES-256 tryb CTS z 96-bit SHA-1 HMAC została dodana do tablicy kluczy
WRFILE:/etc/security/slapd_krb5.keytab.
Pozycja podmiotu kerberos ldap/plankton.austin.ibm.com o kvno 2,
typie szyfrowania DES tryb cbc z RSA-MD5 została dodana do tablicy kluczy
WRFILE:/etc/security/slapd_krb5.keytab.
kadmin.local:
```

- Dla administratora IDS utwórz użytkownika Kerberos o nazwie ldapadmin.

```
kadmin.local: addprinc ldapadmin
OSTRZEŻENIE: nie określono żadnej strategii dla ldapadmin@ud3a.austin.ibm.com;
domyślną wartością będzie brak strategii.
Strategia może zostać nadpisana przez ograniczenia listy ACL.
Wpisz hasło podmiotu kerberos "ldapadmin@ud3a.austin.ibm.com":
Wpisz ponownie hasło podmiotu kerberos "ldapadmin@ud3a.austin.ibm.com":
Podmiot kerberos "ldapadmin@ud3a.austin.ibm.com" został utworzony.
kadmin.local:
```

- Dla podmiotu Kerberos łączenia utwórz plik keytab `kdapadmin.keytab`. Ten klucz może być użyty przez demon klienta **secldapclntd**.

```
kadmin.local: ktadd -k /etc/security/ldapadmin.keytab ldapadmin
Pozycja podmiotu kerberos ldapadmin o kvno 2, typie szyfrowania
Triple DES tryb cbc z HMCA/sha1 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapadmin.keytab.
Pozycja podmiotu kerberos ldapadmin o kvno 2, typie szyfrowania
ArcFour z HMAC/md5 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapadmin.keytab.
Pozycja podmiotu kerberos ldapadmin o kvno 2, typie szyfrowania
AES-256 tryb CTS z 96-bit SHA-1 HMAC została dodana do tablicy kluczy
WRFILE:/etc/security/ldapadmin.keytab.
Pozycja podmiotu kerberos ldapadmin o kvno 2, typie szyfrowania
DES tryb cbc z RSA-MD5 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapadmin.keytab.
kadmin.local
```

- Dla klientów, w celu łączenia z serwerem LDAP utwórz użytkownika Kerberos o nazwie ldapproxy.

```
kadmin.local: addprinc ldapproxy
OSTRZEŻENIE: nie określono żadnej strategii dla ldapproxy @ud3a.austin.ibm.com;
domyślną wartością będzie brak strategii.
Strategia może zostać nadpisana przez ograniczenia listy ACL.
```

```
Wpisz hasło podmiotu kerberos "ldapproxy@ud3a.austin.ibm.com":
Wpisz ponownie hasło podmiotu kerberos "ldapproxy@ud3a.austin.ibm.com":
Podmiot kerberos "ldapproxy@ud3a.austin.ibm.com" został utworzony.
kadmin.local:
```

- Dla podmiotu Kerberos łączenia **ldapproxy** utwórz plik keytab o nazwie *ldapproxy.keytab*. Ten klucz może być użyty przez demon klienta **secldapclntd**.

```
kadmin.local: ktadd -k /etc/security/ldapproxy.keytab ldapproxy
Pozycja podmiotu kerberos ldapproxy o kvno 2, typie szyfrowania
Triple DES tryb cbc z HMAC/sh1 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapproxy.keytab.
Pozycja podmiotu kerberos ldapproxy o kvno 2, typie szyfrowania
ArcFour z HMAC/md5 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapproxy.keytab.
Pozycja podmiotu kerberos ldapproxy o kvno 2, typie szyfrowania
AES-256 tryb CTS z 96-bit SHA-1 HMAC została dodana do tablicy kluczy
WRFILE:/etc/security/ldapproxy.keytab.
Pozycja podmiotu kerberos ldapproxy o kvno 2,
typie szyfrowania DES tryb cbc z RSA-MD5 została dodana do tablicy kluczy
WRFILE:/etc/security/ldapproxy.keytab.
kadmin.local:
```

Włączanie łączenia Kerberos serwera IDS
Poniższa procedura włącza możliwość łączenia serwera IDS przy użyciu wiązania Kerberos.

Przedstawiony poniżej przykład prezentuje sposób konfigurowania serwera IDS do łączenia Kerberos.

Zaprezentowany przykład został przetestowany z serwerem IDS v5.1:

1. Zainstaluj zestaw plików `krb5.client`.
2. Upewnij się, że plik `/etc/krb5/krb5.conf` istnieje i został prawidłowo skonfigurowany. Jeśli trzeba go skonfigurować, uruchom komendę **/usr/sbin/config.krb5**.

```
# config.krb5 -r ud3a.austin.ibm.com -d austin.ibm.com -c KDC -s alyssa.austin.ibm.com
Initializing configuration...
Creating /etc/krb5/krb5_cfg_type...
Creating /etc/krb5/krb5.conf...
The command completed successfully.
# cat /etc/krb5/krb5.conf
[libdefaults]
     default_realm = ud3a.austin.ibm.com
     default_keytab_name = FILE:/etc/krb5/krb5.keytab
     default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-md5 des-cbc-crc
     defaut_tgs_enctypes = des3-cbc-sha11 arcfour-hmac aes256-cts des-cbc-md5 des-cbc-crc
[realms]
  ud3a.austin.ibm.com = {
     kdc = alyssa.austin.ibm.com:88
     admin_server = alyssa.austin.ibm.com:749
     default_domain = austin.ibm.com
  }

[domain_realm]
     .austin.ibm.com = ud3a.austin.ibm.com
     alyssa.austin.ibm.com = ud3a.austin.ibm.com

[logging]
     kdc = FILE:/var/krb5/log/krb5
     admin_server = FILE:/var/krb5/log/kadmin.log
     default = FILE:/var/krb5/log/krb5lib.log
```

3. Pobierz plik keytab nazwy użytkownika Kerberos ldap:/*nazwa_hosta* i umieść go w katalogu `/usr/ldap/etc`. Na przykład: `/usr/ldap/etc/slapd_krb5.keytab`.
4. Ustaw uprawnienia, aby umożliwić procesowi serwera dostęp do pliku.

```
# chown ldap:ldap/usr/ldap/etc/slapd_krb5.keytab
#
```

5. Aby włączyć serwer IDS w celu obsługi łączenia Kerberos, zmień plik `/etc/ibmslapd.conf` i dołącz następujące pozycje:

```
dn: cn=Kerberos, cn-Configuration
cn: Kerberos
ibm-slapdKrbAdminDN: ldapadmin
```

```
ibm-slapdKrbEnable: true
ibm-slapdKrbIdentityMap: true
ibm-slapdKrbKeyTab: /usr/ldap/etc/slapd_krb5.keytab
ibm-slapdKrbRealm: ud3a.austin.ibm.com
objectclass: ibm-slapdKerberos
objectclass: ibm-slapdconfigEntry
objectclass: top
```

6. Odwzoruj nazwę użytkownika Kerberos ldapproxy na nazwę wyróżniającą łączenia o nazwie cn-proxyuser,cn=aixdata.
   a) Jeśli na serwerze IDS istnieje nazwa wyróżniająca łączenia, utwórz plik `ldapproxy.ldif` o następującej zawartości:

   ```
   dn: cn=proxyuser,cn=aixdata
   changetype: modify
   add: objectclass
   objectclass: ibm-securityidentities
   -
   add:altsecurityidentities
   altsecurityidentities: Kerberos:ldapproxy@ud3a.austin.ibm.com
   ```

   LUB

   b) Jeśli pozycja nazwy wyróżniającej łączenia nie została jeszcze dodana do serwera, utwórz plik `proxyuser.ldif` o następującej zawartości:

   Uwaga: Wartość *proxyuserpwd* (hasło użytkownika proxy) należy zastąpić własnym hasłem.

   ```
   dn: cn=proxyuser,cn=mytest
   cn: proxyuser
   sn: proxyuser
   userpassword: proxyuserpwd
   objectclass: person
   objectclass: top
   objectclass: ibm-securityidentities
   altsecurityidentities: Kerberos:ldapproxy@ud3a.austin.ibm.com
   ```

   Za pomocą komendy **ldapmodify** dodaj do serwera IDS pozycję nazwy wyróżniającej łączenia.

   ```
   # ldapmodify -D cn-admin -w adminPwd -f /tmp/proxyuser.ldif modifying entry
   cn=proxyuser,cn=mytest
   #
   ```

7. Zrestartuj serwer IDS.

Włączanie łączenia Kerberos klienta LDAP systemu AIX
System klienta LDAP systemu AIX można skonfigurować do korzystania z protokołu Kerberos podczas początkowego łączenia z serwerem LDAP.

Serwer IDS musi być skonfigurowany dla hosta w taki sposób, aby był klientem dla samego siebie.

Zaprezentowany przykład został przetestowany z serwerem IDS v 5.1:

1. Zainstaluj zestaw plików `krb5.client`.
2. Upewnij się, że plik `/etc/krb.conf` i został prawidłowo skonfigurowany. Jeśli nie został prawidłowo skonfigurowany, uruchom komendę **/usr/sbin/config.krb5** , aby go skonfigurować.
3. Pobierz plik keytab podmiotu Kerberos łączenia i umieść go w katalogu `/etc/security/ldap`.
4. Uprawnienia ustaw na 600.
5. Za pomocą komendy **mksecldap**, używając nazwy wyróżniającej i hasła łączenia, skonfiguruj klienta. Upewnij się, że komendy systemu AIX działają dla użytkowników LDAP.
6. Aby ustawić atrybuty związane z protokołem Kerberos, dokonaj edycji pliku `/etc/security/ldap/ldap.cfg`. W przedstawionym poniżej przykładzie podmiotem Kerberos łączenia jest `ldapproxy`, a plikiem keytab `ldapproxy.keytab`. Jeśli serwer IDS ma mieć uprawnienia administratora, wartość *ldapproxy* należy zastąpić wartością *ldapadmin*, a plik *ldapproxy.keytab* plikiem *ldapadmin.keytab*.

   ```
   useKRB5:yes
   krbprincipal:ldapproxy
   ```

```
krbkeypath:/etc/security/ldap/ldapproxy.keytab
krbcmddir:/usr/krb5/bin/
```

Teraz nazwę wyróżniającą i hasło łączenia można usunąć z pliku `ldap.cfg` lub przekształcić w komentarz, ponieważ demon **secldapclntd** korzysta teraz z łączenia Kerberos.

7. Zrestartuj demon **secldapclntd**.
8. Plik `/etc/security/ldap/ldap.cfg` można teraz przenieść do innych systemów klienckich.

Kontrola serwera informacji o bezpieczeństwie LDAP

Produkt SecureWay Directory w wersji 3.2 (i nowszych) udostępnia domyślną funkcję protokołowania kontroli serwera. Po jej włączeniu ta domyślna wtyczka kontroli rejestruje działania serwera LDAP w pliku dziennika. Więcej informacji na temat tej domyślnej wtyczki kontroli zawiera dokumentacja dotycząca protokołu LDAP w *Packaging Guide for LPP Installation*.

Funkcja kontroli serwera informacji o bezpieczeństwie LDAP dostępna w systemie operacyjnym AIX jest nazywana *wtyczką kontroli zabezpieczeń LDAP*. Jest ona niezależna od domyślnej usługi kontroli produktu SecureWay Directory, dlatego można włączyć jeden lub oba z tych podsystemów kontroli. Wtyczka kontroli systemu AIX zapisuje tylko te zdarzenia, które aktualizują lub odpytują informacje o zabezpieczeniach AIX dotyczące serwera LDAP. Moduł ten działa w ramach kontroli systemu AIX.

W pliku `/etc/security/audit/event` znajdują się następujące zdarzenia kontrolowane, umożliwiające dostosowanie protokołu LDAP:

- `LDAP_Bind`
- `LDAP_Unbind`
- `LDAP_Add`
- `LDAP_Delete`
- `LDAP_Modify`
- `LDAP_Modifydn`
- `LDAP_Search`

W pliku `/etc/security/audit/config` tworzona jest także definicja klasy kontroli `ldapserver` zawierająca wszystkie powyższe zdarzenia.

Aby kontrolować serwer informacji o bezpieczeństwie LDAP, do sekcji poszczególnych użytkowników w pliku `/etc/security/audit/config` należy dodać wiersz:

```
ldap = ldapserver
```

Ponieważ wtyczka kontroli serwera informacji o bezpieczeństwie LDAP została zaimplementowana w ramach kontroli systemu AIX, jest ona częścią podsystemu kontrolującego systemu AIX. Kontrolę serwera informacji o bezpieczeństwie LDAP można włączać i wyłączać za pomocą komend kontroli systemu, takich jak **audit start** i **audit shutdown**. Wszystkie rekordy kontroli są dodawane do zapisów kontrolnych systemu, które można przeglądać za pomocą komendy **auditpr**. Więcej informacji na ten temat zawiera sekcja “Kontrola - przegląd” na stronie 136.

Komendy LDAP

Istnieje kilka komend LDAP.

Komenda lsldap

Komendy **lsldap** można używać do wyświetlania jednostek usługi nazw ze skonfigurowanego serwera LDAP. Jednostki te to aliasy, automatyczne podłączanie, parametry startowe, ethers, grupy, hosty, grupy sieciowe, sieci, hasła, protokoły, rpc i usługi.

Komenda mksecldap

Komendy **mksecldap** można używać do skonfigurowania serwerów i klientów oprogramowania IBM SecureWay Directory pod kątem uwierzytelniania bezpieczeństwa i zarządzania danymi. Komendę tę należy uruchomić na serwerze i wszystkich klientach.

Demon secldapclntd

Demon **secldapclntd** akceptuje żądania z modułu ładowalnego LDAP, przekazuje je do serwera informacji o bezpieczeństwie (Security Information Server) LDAP, a następnie przesyła wynik uzyskany z serwera z powrotem do modułu ładowalnego.

Komendy zarządzania LDAP
Do zarządzania protokołem LDAP wykorzystywanych jest kilka komend.

Komenda start-secldapclntd

Komenda **start-secldapclntd** uruchamia demon **secldapclntd**, jeśli nie jest on jeszcze uruchomiony.

Komenda stop-secldapclntd

Komenda **stop-secldapclntd** przerywa uruchomiony proces demona **secldapclntd**.

Komenda restart-secldapclntd

Skrypt **restart-secldapclntd** zatrzymuje demon **secldapclntd**, jeśli jest on uruchomiony i restartuje go. Jeśli demon ten nie jest uruchomiony, uruchamia go.

Komenda ls-secldapclntd

Komenda **ls-secldapclntd** wyświetla status demona **secldapclntd**.

Komenda flush-secldapclntd

Komenda **flush-secldapclntd** czyści pamięć podręczną dla procesu demona **secldapclntd**.

Komenda sectoldif

Komenda **sectoldif** odczytuje zdefiniowanych lokalnie użytkowników i grupy, a następnie wysyła wynik odczytu do standardowego wyjścia w formacie **ldif**.

Format pliku odwzorowań dla atrybutów LDAP
Te pliki odwzorowań są używane przez moduł `/usr/lib/security/LDAP` i demon **secldapclntd** do tłumaczeń nazw atrybutów systemu AIX na nazwy atrybutów LDAP i odwrotnie.

Każda pozycja w pliku odwzorowania reprezentuje tłumaczenie atrybutu. Pozycja składa się z czterech pól oddzielonych spacjami:

```
nazwa_atrybutu_AIX typ_atrybutu_AIX nazwa_atrybutu_LDAP typ_wartości_LDAP
```

Poniżej podano opisy tych pól:

nazwa_atrybutu_AIX
Nazwa atrybutu AIX.

typ_atrybutu_AIX
Typ atrybutu AIX. Poprawne wartości to: SEC_CHAR, SEC_INT, SEC_LIST i SEC_BOOL.

nazwa_atrybutu_LDAP
Nazwa atrybutu LDAP.

typ_wartości_LDAP
Typ wartości LDAP. Poprawne wartości to **s** w przypadku wartości pojedynczej i **m** w przypadku wartości wielokrotnej.

LDAP i KRB5LDAP na pojedynczym kliencie
Jeśli LDAP jest częścią złożonego modułu, takiego jak KRB5LDAP, dozwolone są wyłącznie operacje odczytu, a operacje zapisu są niedozwolone. Jednak, wprowadzając podane poniżej zmiany w konfiguracji w pliku **/usr/lib/security/methods.cfg**, zarówno LDAP, jak i złożone moduły ładowania, takie jak KRB5LDAP, zostaną dostosowane w pojedynczym pliku. Wykonaj następujące kroki:

1. Skonfiguruj klienta LDAP i klienty KRB5LDAP w zwykły sposób.
2. Zmodyfikuj plik **/usr/lib/security/methods.cfg** w następujący sposób:

```
LXAP:   program = /usr/lib/security/LDAP program_64
        =/usr/lib/security/
LDAP64

LDAP:   program = /usr/lib/security/LDAP program_64
        =/usr/lib/security/
LDAP64

NIS:    program = /usr/lib/security/NIS program_64 =
        /usr/lib/security/
NIS_64

DCE:    program = /usr/lib/security/
DCE


KRB5:   program = /usr/lib/security/
KRB5


KRB5LXAP: options =
db=LXAP,auth=KRB5
```

3. Zmodyfikuj plik **/etc/security/user** w sekcji domyślnej w następujący sposób:

```
        SYSTEM = "KRB5LXAP OR LDAP OR compat"
```

Użytkowników LDAP można przetworzyć w zwykły sposób. W poniższych przykładach przedstawiono przetwarzanie użytkowników KRB5LDAP:

```
mkuser -R KRB5LXAP <nazwa_użytkownika>
rmuser -R KRB5LXAP <nazwa_użytkownika>
lsuser -R KRB5LXAP <nazwa_użytkownika>
passwd -R KRB5LXAP <nazwa_użytkownika>
```

System EFS (Encrypted File System)

System EFS umożliwia poszczególnym użytkownikom w systemie szyfrowanie danych znajdujących się w systemie plików J2 za pomocą ich własnych plików kluczy.

Każdy klucz jest powiązany z użytkownikiem. Klucze są przechowywane w pliku kluczy chronionym kryptograficznie i po pomyślnym zalogowaniu się użytkownika jego klucze są ładowane do jądra i wiązane z uprawnieniami procesów. Następnie, jeśli proces potrzebuje otworzyć plik chroniony EFS, te referencje są sprawdzane i jeśli zostanie znaleziony klucz pasujący do zabezpieczenia pliku, proces może deszyfrować klucz pliku i następnie zawartość pliku. Obsługiwane jest również zarządzanie kluczami na podstawie grup.

Uwaga: System EFS stanowi część kompletnej strategii bezpieczeństwa. Został zaprojektowany przy założeniu stosowania solidnych praktyk w zakresie bezpieczeństwa oraz ich kontroli.

Łatwość używania systemu EFS
Zarządzanie kluczami, szyfrowanie i deszyfrowanie plików systemu EFS to operacje zwykle niewidoczne dla użytkownika.

System EFS stanowi część podstawowego systemu operacyjnego AIX. Aby włączyć system EFS, użytkownik root (lub dowolny inny użytkownik z autoryzacją RBAC **aix.security.efs**, więcej informacji na ten temat można znaleźć w sekcji Obsada EFS) musi użyć komendy **efsenable** w celu aktywacji systemu EFS i utworzenia środowiska EFS. Jest to operacja jednorazowa w danym systemie. Po włączeniu systemu EFS, gdy użytkownik rozpocznie sesję, jego klucze i pliki kluczy są tworzone bezobsługowo i chronione lub szyfrowane za pomocą jego hasła logowania. Klucze użytkowników są następnie używane bezobsługowo przez system plików J2 przy szyfrowaniu i deszyfrowaniu plików EFS. Każdy plik EFS jest chroniony własnym unikalnym kluczem pliku, a ten klucz pliku jest chroniony lub szyfrowany kluczem grupy lub właściciela pliku w zależności od uprawnień do tego pliku.

Domyślnie w systemie plików J2 mechanizm EFS jest wyłączony. Po jego włączeniu system plików J2 w sposób niewidoczny dla użytkownika zarządza szyfrowaniem i deszyfrowaniem w jądrze, obsługując żądania odczytu i zapisu. Komendy administrowania użytkownikami i grupami (takie jak **mkgroup**, **chuser** oraz **chgroup**) zarządzają plikami kluczy użytkowników i grup w niezauważalny dla nich sposób.

Do zarządzania kluczami i szyfrowaniem plików udostępniono użytkownikom następujące komendy EFS:

efskeymgr
Zarządza i administruje kluczami.

efsmgr
Zarządza szyfrowaniem systemu plików/katalogów/plików.

Obsada systemu EFS (Encrypted File System)
Są trzy typy użytkowników mogących zarządzać kluczami EFS i ich używać:

Pełny lub ograniczony dostęp użytkownika root
Dostęp użytkownika root do kluczy może być nieograniczony lub ograniczony. W obu tych trybach użytkownik root nie może wykonać po prostu komendy **su**, aby uzyskać prawa danego użytkownika wraz z dostępem do jego pliku kluczy i zaszyfrowanych plików.

W jednym trybie użytkownik root może zresetować hasło do pliku kluczy użytkownika i może uzyskać dostęp do kluczy użytkownika znajdujących się w tym pliku kluczy. Tryb ten zapewnia większą elastyczność administrowania systemem.

W innym trybie użytkownik root może zresetować hasło logowania użytkownika, ale nie może zresetować jego hasła do pliku kluczy. Użytkownik root nie może zastąpić użytkownika (używając komendy **su**) i odziedziczyć otwartego pliku kluczy. Wprawdzie użytkownik root może tworzyć i usuwać użytkowników i grupy, wraz z powiązanymi plikami kluczy, jednak nie ma dostępu do kluczy w tych plikach. Ten tryb zapewnia wyższy stopień ochrony przed atakami złośliwego użytkownika root.

Są dwa tryby zarządzania plikami kluczy i używania ich, Root Admin i Root Guard. Udostępniany jest również klucz administrowania EFS.

Klucz administrowania EFS umożliwia dostęp do pozostałych haseł do wszystkich plików kluczy w trybie Root Admin. Klucz ten znajduje się w specjalnym pliku kluczy **efs_admin**. Dostęp do specjalnego pliku kluczy **efs_admin** jest nadawany tylko autoryzowanym użytkownikom (użytkownik root i grupa security podczas instalacji lub autoryzacji RBAC **aix.security.efs**).

Gdy plik kluczy jest w trybie Root Guard, nie można uzyskać zawartych w nim kluczy bez podania poprawnego hasła pliku kluczy. Stanowi to dobre zabezpieczenie przeciwko złośliwemu użytkownikowi root, jednak zarazem powoduje problemy, gdy użytkownik zapomni swojego hasła, ponieważ nie ma możliwości ponownego wygenerowania hasła bez utraty kluczy znajdujących się w pliku kluczy, a w wyniku tego użytkownik traci dostęp do swoich danych. W tym trybie pliku kluczy niektóre operacje nie mogą być wykonywane natychmiast i są wpisywane do harmonogramu jako operacje oczekujące. Operacje takie są generowane na przykład przy dodawaniu grupowego klucza dostępu do pliku kluczy użytkownika albo odrzucaniu tego klucza lub przy ponownym generowaniu klucza prywatnego. Są one zarządzane przez właściciela pliku kluczy.

Klucz administrowania efs_admin
Plik kluczy efs_admin zawiera specjalny klucz, otwierający dowolny plik kluczy użytkownika lub grupy w trybie administrowania użytkownika root (tryb domyślny).

Hasło do otworzenia tego specjalnego pliku kluczy jest zapisywane w plikach kluczy użytkownika root i grupy security podczas aktywowania systemu EFS. Hasło to można następnie podać innym grupom i użytkownikom albo usunąć komendą **efskeymgr**. Klucz w połączeniu z autoryzacją **aix.security.efs** kontroli RBAC umożliwia użytkownikowi administrowanie systemem EFS (to znaczy dostęp do plików kluczy w trybie administrowania użytkownika root).

Zagadnienia związane z kontrolą RBAC i komendą efs_admin

W systemach z włączoną kontrolą dostępu na podstawie ról komenda **efs_admin** jest chroniona autoryzacją **aix.security.efs**.

Plik kluczy użytkownika

W większości operacji zarządzanie plikiem kluczy użytkownika odbywa się automatycznie. Do zaawansowanego korzystania z mechanizmu EFS i zadań związanych z konserwacją służy komenda **efskeymgr**. Użytkownicy mogą tworzyć szyfrowane pliki i katalogi komendą **efsmgr**. Zarządzanie plikiem kluczy jest zintegrowane z większością komend administrowania użytkownikami. Jeśli użytkownik jest dodawany do grupy, automatycznie uzyskuje dostęp do pliku kluczy tej grupy.

Właściciel pliku z dostępem EFS do pliku używa komendy **efsmgr** w celu nadania dostępu EFS innym użytkownikom i grupom (podobnie jak w listach ACL w systemie UNIX). Użytkownicy mogą zmienić swoje hasła. nie wpływając na oddzielne procesy uruchomione z tym samym identyfikatorem UID z otwartym plikiem kluczy.

Plik kluczy systemu EFS (Encrypted File System)

Pliki kluczy są chronione hasłem. Użytkownicy mogą wybrać alternatywne hasło pliku kluczy, różniące się od hasła logowania. W takim przypadku plik kluczy nie jest otwierany i dostępny podczas standardowego logowania się użytkownika. Użytkownik musi samodzielnie załadować plik kluczy komendą **efskey**, aby podać hasło do tego pliku.

Formatem pliku kluczy jest **PKCS # 12**. Pliki kluczy są przechowywane w następujących plikach.

plik kluczy użytkownika
/var/efs/users//keystore

plik kluczy grupy
/var/efs/groups//keystore

plik kluczy użytkownika efsadmin
/var/efs/efs_admin/keystore

Jeśli użytkownik ustawi takie samo hasło logowania i hasło pliku kluczy, jego plik kluczy będzie otwierany i dostępny w momencie logowania.

Użytkownik może użyć komendy systemu EFS **efskeymgr**, aby wybrać typ algorytmu szyfrowania i długość klucza.

Dostęp do pliku kluczy jest dziedziczony przez wszystkie procesy potomne.

Obsługiwane jest również zarządzanie kluczami na poziomie grupy. Jeśli plik kluczy grupy jest w trybie guard, tylko członek grupy może dodać klucze grupy do plików kluczy członków lub je stamtąd usunąć. Plik kluczy użytkownika zawiera klucz prywatny użytkownika oraz hasło otwierające pliki kluczy grup użytkownika, zawierające klucze prywatne grupy.

Uwaga: Plik kluczy systemu EFS jest otwierany automatycznie podczas standardowego logowania w systemie AIX pod warunkiem, że hasło pliku kluczy użytkownika jest zgodne z jego hasłem logowania. Można tak skonfigurować domyślnie w trakcie początkowego tworzenia pliku kluczy użytkownika. Metody logowania się inne niż standardowe logowanie do systemu AIX, na przykład ładowalne moduły uwierzytelniania i moduły PAM mogą nie otwierać automatycznie pliku kluczy.

Szyfrowanie i dziedziczenie

Mechanizm EFS jest opcją J2. Opcja **efs** systemu plików musi być ustawiona na **yes** (patrz komendy **mkfs** i **chfs**).

Mechanizm EFS w systemie plików J2 automatycznie szyfruje i deszyfruje dane użytkownika. Jeśli jednak użytkownik ma prawo odczytu pliku z aktywowanym systemem EFS, a nie ma odpowiedniego klucza, nie może odczytać tego pliku w zwykły sposób. Jeśli nie ma poprawnego klucza, nie może deszyfrować danych.

Wszystkie funkcje szyfrujące pochodzą z usług jądra CLiC oraz bibliotek użytkownika CLiC.

Domyślnie w systemie plików J2 mechanizm EFS jest wyłączony. Należy go włączyć przed aktywacją dziedziczenia EFS systemu plików lub przed szyfrowaniem EFS danych użytkownika. Plik jest tworzony w postaci zaszyfrowanej albo jawnie, komendą **efsmgr**, albo niejawnie, przez dziedziczenie EFS. Dziedziczenie EFS można aktywować albo na poziomie systemu plików, albo na poziomie katalogu, albo jednocześnie na obydwu poziomach.

Komenda **ls** wyświetla zaszyfrowane pliki, poprzedzając je literą **e**.

Komendy **cp** i **mv** mogą obsługiwać metadane i dane szyfrowane płynnie między EFS a EFS i EFS a systemem bez EFS.

Komendy **backup**, **restore** i **tar** oraz komendy pokrewne mogą tworzyć kopie zapasowe szyfrowanych danych i je odtwarzać wraz z metadanymi EFS służącymi do szyfrowania i deszyfrowania.

Tworzenie i odtwarzanie kopii zapasowej
Istotną sprawą jest poprawne zarządzanie archiwizacją lub tworzeniem kopii zapasowych plików kluczy powiązanych z archiwizowanymi plikami EFS. Należy ponadto zająć się hasłami powiązanymi z tymi plikami kluczy. Niepowodzenie wykonania dowolnego z powyższych zadań może spowodować utratę danych.

Podczas tworzenia kopii zapasowej z plików szyfrowanych EFS można użyć opcji –Z komendy **backup**, aby utworzyć kopię zapasową zaszyfrowanej postaci pliku wraz z metadanymi szyfrującymi pliku. Zarówno dane pliku, jak i metadane, są chronione silnym szyfrowaniem. Takie rozwiązanie jest korzystniejsze z punktu widzenia bezpieczeństwa od chronienia silnym szyfrowaniem kopii zapasowych plików. Konieczne jest utworzenie kopii zapasowej pliku kluczy właściciela i grupy pliku powiązanego z owym plikiem, którego kopia zapasowa jest tworzona. Pliki kluczy są następujące:

pliki kluczy użytkowników
/var/efs/users/*nazwa_użytkownika*/*

plik kluczy grupy
/var/efs/groups//keystore

plik kluczy użytkownika efsadmin
/var/efs/efs_admin/keystore

Aby odtworzyć kopię zapasową EFS (utworzoną przy użyciu komendy **backup** z opcją –Z), należy użyć komendy **restore**. Użycie komendy restore powoduje także odtworzenie metadanych szyfrowania. Podczas procesu odtwarzania nie ma potrzeby odtwarzania kopii zapasowych plików kluczy, jeśli użytkownik nie zmienił kluczy we własnym pliku kluczy. Gdy użytkownik zmienia hasło otwierające plik kluczy, klucz wewnątrz tego pliku kluczy nie jest zmieniany. Aby zmienić klucze wewnątrz pliku kluczy, należy użyć komendy **efskeymgr**.

Jeśli wewnętrzny klucz pliku kluczy użytkownika nie został zmieniony, użytkownik może natychmiast otworzyć i deszyfrować odtworzony plik, korzystając ze swojego bieżącego pliku kluczy. Jednak jeśli wewnętrzny klucz w pliku kluczy użytkownika został zmieniony, użytkownik musi otworzyć plik kluczy, którego kopia zapasowa została utworzona wraz z kopią zapasową pliku. Do otworzenia tego pliku kluczy służy komenda **efskeymgr –o**. Komenda **efskeymgr** poprosi użytkownika o hasło do otworzenia pliku kluczy. Jest to to samo hasło, które było użyte w połączeniu z plikiem kluczy w momencie tworzenia kopii zapasowej.

Na przykład załóżmy, że plik kluczy użytkownika Robert był chroniony hasłem **foo** (hasło ‘foo’ nie jest bezpieczne i zostało użyte w niniejszym przykładzie tylko dla uproszczenia) a kopia zapasowa zaszyfrowanych plików Roberta wraz z jego plikiem kluczy została wykonana w styczniu. W naszym przykładzie Robert używa również hasła **foo** jako hasła do logowania się w systemie AIX. W lutym Robert zmienił swoje hasło na **bar**, co spowodowało również zmianę jego hasła dostępu do pliku kluczy na **bar**.

Jeśli w marcu pliki EFS Roberta zostaną odtworzone, będzie mógł je otworzyć i przeglądać korzystając z aktualnego pliku kluczy i hasła, ponieważ nie zmienił klucza wewnętrznego pliku kluczy.

Jeśli jednak zaszła konieczność zmiany klucza wewnętrznego pliku kluczy Roberta (komendą **efskeymgr**), wtedy domyślnie stary klucz wewnętrzny pliku kluczy staje się nieaktualny i pozostawiony w pliku kluczy Roberta. W momencie, gdy użytkownik chce uzyskać dostęp do pliku, system EFS automatycznie rozpozna, że odtworzony plik używa starego klucza wewnętrznego, a następnie użyje nieaktualnego klucza, aby go deszyfrować. W tej samej sesji dostępu system EFS przekształci plik, aby używał nowego klucza wewnętrznego. Operacja ta nie ma istotnego wpływu na wydajność procesu, ponieważ obsługa odbywa się na poziomie pliku kluczy i zaszyfrowanych metadanych pliku i nie jest konieczne ponowne szyfrowanie danych pliku.

Jeśli nieaktualny klucz wewnętrzny zostanie usunięty komendą **efskeymgr**, należy odtworzyć stary plik kluczy ze starym kluczem wewnętrznym i użyć go razem z plikami szyfrowanymi tym kluczem wewnętrznym.

Rodzi to pytanie o sposób bezpiecznego konserwowania starych haseł i ich archiwizowania. Istnieją metody i narzędzia do realizacji tego zadania. Ogólnie ujmując, metody te wymagają posiadania pliku zawierającego listę wszystkich starych haseł, a następnie szyfrowania tego pliku i ochrony za pomocą bieżącego pliku haseł, które jest chronione bieżącymi hasłami. Jednak środowiska informatyczne i strategie bezpieczeństwa w różnych organizacjach różnią się między sobą, dlatego należy zastanowić się nad konkretnymi potrzebami związanymi z bezpieczeństwem w danej organizacji, aby zastosować strategie bezpieczeństwa i zwyczaje najlepiej pasujące w danym środowisku.

Wewnętrzny mechanizm EFS J2
Każdy plik z aktywowanym mechanizmem EFS w systemie plików J2 jest powiązany ze specjalnym atrybutem rozszerzonym zawierającym metadane EFS służące do sprawdzania poprawności uprawnienia szyfrowania i informacje służące do szyfrowania i deszyfrowania plików (klucze, algorytm szyfrowania itp.).

Zawartość atrybutu rozszerzonego jest osłonięta przed systemem plików J2. Zarówno referencje użytkownika, jak i metadane EFS, są niezbędne do określenia autoryzacji szyfrowania (kontroli dostępu) dla każdego pliku z aktywowanym mechanizmem EFS.

Uwaga: Należy zwrócić baczną uwagę na sytuacje, w których może nastąpić utrata pliku lub danych (na przykład usunięcie atrybutu rozszerzonego pliku).

Dziedziczenie ochrony EFS
Po włączeniu mechanizmu EFS dla katalogu każdy nowo tworzony element bezpośrednio potomny, jeśli nie zostanie wymuszone inaczej, ma automatycznie włączany mechanizm EFS. Atrybuty EFS katalogu macierzystego mają pierwszeństwo przed atrybutami EFS systemu plików.

Zasięg dziedziczenia katalogu to dokładnie jeden poziom. Każdy nowo tworzony element potomny dziedziczy również atrybuty EFS elementu macierzystego, jeśli jego katalog macierzysty ma włączony mechanizm EFS. Istniejące elementy potomne utrzymują swój istniejący stan: szyfrowany lub nieszyfrowany. Logiczny łańcuch dziedziczenia zostaje przerwany, jeśli element macierzysty zmieni swoje atrybuty EFS. Te zmiany nie są propagowane w dół do istniejących elementów potomnych katalogu i muszą być oddzielnie zastosowane do tych katalogów.

Uwagi dotyczące partycji zarządzania obciążeniem
Przed włączeniem lub rozpoczęciem korzystania z systemu EFS na partycji zarządzania obciążeniem konieczne jest włączenie komendą **efsenable** mechanizmu EFS w systemie globalnym. Operację taką należy przeprowadzić raz. Ponadto wszystkie systemy plików, w tym systemy plików z włączonym mechanizmem EFS, muszą być tworzone z systemu globalnego.

Konfigurowanie systemu EFS (Encrypted File System)

Na wstępie należy wykonać następujące działania.

Kolejne etapy należy wykonać dokładnie tak, jak to opisano.

1. Zainstaluj zestaw plików **clic.rte**. W tym zestawie plików znajdują się biblioteki szyfrujące i rozszerzenia jądra wymagane przez EFS. Zestaw plików **clic.rte** znajduje się na dysku AIX Expansion Pack.
2. Włącz EFS w systemie przy użyciu komendy **efsenable** (na przykład >efsenable –a). Gdy system poprosi o hasło, uzasadnione jest podanie hasła użytkownika root. Pliki kluczy użytkowników są tworzone automatycznie, a następnie użytkownik rozpoczyna sesję lub ponownie rozpoczyna sesję po uruchomieniu komendy **efsenable**. Gdy w systemie uruchomiono komendę **efsenable** –a, zostaje uruchomiony mechanizm EFS i nie ma potrzeby ponownego uruchamiania komendy **efsenable**.
3. Utwórz system plików z włączonym mechanizmem EFS, używając opcji –a efs=yes. Na przykład `crfs -v jfs2 -m /foo –A yes -a efs=yes -g rootvg -a size=20000`
4. Po podłączeniu systemu plików włącz dziedziczenie szyfrowania w systemie plików z włączonym mechanizmem EFS. W tym celu użyj komendy **efsmgr**. Aby kontynuować powyższy przykład, w którym utworzony został system plików **/foo**, uruchom następującą komendę: `efsmgr –s –E /foo`. Dzięki temu każdy plik tworzony i używany w tym systemie plików będzie szyfrowany.

Od tego momentu, gdy użytkownik lub proces z otwartym plikiem kluczy utworzy plik w tym systemie plików, będzie to plik zaszyfrowany. Gdy użytkownik lub plik odczytują plik, jest on automatycznie deszyfrowany dla użytkowników mających autoryzację zezwalającą na dostęp do pliku.

Więcej informacji na ten temat zawierają:

- Komendy **chfs**, **chgroup**, **chuser**, **cp**, **efsenable**, **efskeymgr**, **efsmgr**, **lsuser**, **ls**, **mkgroup**, **mkuser** i **mv**.
- Pliki `/etc/security/group` i `/etc/security/user`.

Zdalny dostęp do plików kluczy systemu EFS (Encrypted File System)
W środowisku przedsiębiorstwa można scentralizować pliki kluczy systemu EFS (Encrypted File System). Gdy bazy danych sterujące plikami kluczy są zapisane w każdym systemie niezależnie, zarządzanie tymi plikami kluczy może być trudne. Scentralizowany plik kluczy EFS systemu AIX umożliwia zapisanie baz danych plików kluczy użytkowników i grup w katalogu Lightweight Directory Access Protocol (LDAP), dzięki czemu można centralnie zarządzać plikiem kluczy EFS.
Pojęcia pokrewne
Protokół LDAP (Lightweight Directory Access Protocol)
Protokół LDAP (Lightweight Directory Access Protocol) definiuje standardową metodę dostępu do informacji i ich aktualizacji w katalogu (bazie danych) lokalnym lub zdalnym w przypadku modelu klient/serwer.

Przegląd zdalnego dostępu do plików kluczy systemu EFS (Encrypted File System)
W tym miejscu podano informacje o bazach danych systemu EFS (Encrypted File System), włączaniu LDAP dla komend EFS i dostępie do unikalnego pliku kluczy.

Wszystkie bazy danych pliku kluczy EFS w systemie AIX można zapisać w LDAP, w tym następujące bazy danych EFS:

- plik kluczy użytkownika,
- plik kluczy grupy,
- plik kluczy administratora,
- informacje cookie.

System AIX udostępnia programy narzędziowe pomocne podczas wykonywania następujących zadań zarządzania:

- eksport danych lokalnego pliku kluczy na serwer LDAP,
- konfigurowanie klienta pod kątem użycia danych pliku kluczy EFS w LDAP,
- sterowanie dostępem do danych pliku kluczy EFS,
- zarządzanie danymi LDAP z systemu klienta.

Wszystkie komendy zarządzania bazą danych kluczy EFS są włączone pod kątem obsługi bazy danych pliku kluczy LDAP. Jeśli w pliku `/etc/nscontrol.conf` nie określono systemowej kolejności

wyszukiwania, operacje dotyczące pliku kluczy zależą od atrybutu efs_keystore_access użytkownika i grupy. Jeśli atrybut efs_keystore_access będzie mieć wartość ldap, komendy EFS wykonują operacje dotyczące pliku kluczy w pliku kluczy LDAP.

W poniższej tabeli opisano zmiany w komendach EFS dla LDAP.

Tabela 12. Włączenie komend EFS dla LDAP

Komenda	**Informacje o LDAP**
Każda komenda EFS	Po nadaniu atrybutowi efs_keystore_access wartości ldap nie trzeba używać opcji specjalnej -L *domena* dla komendy, aby wykonać operacje dotyczące pliku kluczy w LDAP.
efskeymgr	Zawiera opcję -L moduł_ładowania, aby można było wykonać jawne operacje dotyczące pliku kluczy w LDAP.
efsenable	Zawiera opcję -d PodstawowaDN, aby można było wykonać początkowe konfigurowanie LDAP w celu dostosowania pliku kluczy EFS. Początkowe konfigurowanie obejmuje dodanie podstawowych nazw wyróżniających (DN) dla pliku kluczy EFS i utworzenie lokalnej struktury katalogów (/var/efs/).
efskstoldif	Generuje dane pliku kluczy EFS dla LDAP na podstawie danych w następujących bazach danych w systemie lokalnym: • /var/efs/users/*nazwa_użytkownika*/keystore • /var/efs/groups/*nazwa_grupy*/keystore • /var/efs/efs_admin/keystore • informacje cookie, jeśli istnieją, dla wszystkich plików kluczy.

Wszystkie pozycje pliku kluczy muszą być unikalne. Każda pozycja pliku kluczy bezpośrednio odpowiada nazwie wyróżniającej pozycji zawierającej nazwę użytkownika i grupy. System odpytuje identyfikatory użytkowników (uidNumber), identyfikatory grup (gidNumber) i nazwy wyróżniające. Zapytanie jest pomyślne, gdy nazwy użytkowników i grup odpowiadają nazwom wyróżniającym. Przed utworzeniem lub migracją pozycji pliku kluczy EFS w LDAP upewnij się, że identyfikatory i nazwy użytkowników oraz grup w systemie są unikalne.

Zadania pokrewne

Eksportowanie danych pliku kluczy systemu EFS (Encrypted File System) do LDAP
Serwer LDAP należy zapełnić danymi pliku kluczy, aby używać LDAP jako centralnego repozytorium dla pliku kluczy EFS (Encrypted File System).

Konfigurowanie klienta LDAP dla pliku kluczy EFS (Encrypted File System)
Aby używać danych pliku kluczy EFS (Encrypted File System) zapisanych w LDAP, należy skonfigurować system jako klienta LDAP.

Eksportowanie danych pliku kluczy systemu EFS (Encrypted File System) do LDAP

Serwer LDAP należy zapełnić danymi pliku kluczy, aby używać LDAP jako centralnego repozytorium dla pliku kluczy EFS (Encrypted File System).

Przed utworzeniem lub migracją pozycji pliku kluczy EFS w LDAP upewnij się, że identyfikatory i nazwy użytkowników oraz grup w systemie są unikalne.

Aby zapełnić serwer LDAP danymi pliku kluczy EFS, wykonaj następujące kroki:

1. Na serwerze LDAP zainstaluj schemat pliku kluczy EFS dla LDAP:

a) Odtwórz schemat pliku kluczy EFS dla LDAP z pliku `/etc/security/ldap/sec.ldif` w systemie AIX.

b) Uruchom komendę **ldapmodify**, aby zaktualizować schemat serwera LDAP z użyciem schematu pliku kluczy EFS dla LDAP.

2. Uruchom komendę **efskstoldif**, aby odczytać dane w lokalnych plikach kluczy EFS i przekształcić te dane do formatu odpowiedniego dla LDAP.

   Aby zachować unikalny dostęp do pliku kluczy, rozważ umieszczenie danych pliku kluczy EFS znajdujących się w LDAP pod tą samą nadrzędną nazwą wyróżniającą co dane użytkowników i grup.
3. Zapisz te dane w pliku.
4. Uruchom komendę **ldapadd -b**, aby zapełnić serwer LDAP danymi pliku kluczy.

Pojęcia pokrewne

Przegląd zdalnego dostępu do plików kluczy systemu EFS (Encrypted File System)

W tym miejscu podano informacje o bazach danych systemu EFS (Encrypted File System), włączaniu LDAP dla komend EFS i dostępie do unikalnego pliku kluczy.

Konfigurowanie klienta LDAP dla pliku kluczy EFS (Encrypted File System)

Aby używać danych pliku kluczy EFS (Encrypted File System) zapisanych w LDAP, należy skonfigurować system jako klienta LDAP.

Aby skonfigurować klienta LDAP dla pliku kluczy EFS, wykonaj następujące kroki:

1. Uruchom komendę **/usr/sbin/mksecldap**, aby skonfigurować system jako klienta LDAP.

   Komenda **mksecldap** dynamicznie przeszukuje podany serwer LDAP, aby określić położenie danych pliku kluczy EFS. Następnie zapisuje ona wyniki w pliku `/etc/security/ldap/ldap.cfg`. Komenda **mksecldap** określa położenie danych pliku kluczy dla następujących jednostek: user, group, admin i efscookies.
2. Wykonaj jeden z poniższych kroków, aby włączyć LDAP jako domenę wyszukiwania dla danych pliku kluczy EFS:
   - Ustaw atrybut **efs_keystore_access** użytkownika i grupy na wartość **file** lub **ldap**.
   - Zdefiniuj kolejność przeszukiwania dla pliku kluczy na poziomie systemu, używając pliku `/etc/nscontrol.conf`. W poniższej tabeli przedstawiono przykład.

Tabela 13. Przykładowa konfiguracja dla pliku `/etc/nscontrol.conf`

Atrybut	Opis	Kolejność przeszukiwania (secorder):
efsusrkeystore	Ta kolejność przeszukiwania jest wspólna dla wszystkich użytkowników.	LDAP, pliki
efsgrpkeystore	Ta kolejność przeszukiwania jest wspólna dla wszystkich grup.	pliki, LDAP
efsadmkeystore	Ta kolejność przeszukiwania wyszukuje plik kluczy admin dla dowolnego docelowego pliku kluczy.	LDAP, pliki

Ostrzeżenie: Konfiguracja zdefiniowana w pliku `/etc/nscontrol.conf` przesłania wartości ustawione dla atrybutu **efs_keystore_access** użytkownika i grupy. Tak samo jest dla atrybutu **efs_adminks_access** użytkownika.

Po skonfigurowaniu systemu jako klienta LDAP i włączeniu LDAP jako domeny wyszukiwania dla danych pliku kluczy EFS demon klienta /usr/sbin/secldapclntd odtwarza dane pliku kluczy EFS z serwera LDAP za każdym razem, gdy wykonywane są operacje związane z plikiem kluczy LDAP.

Pojęcia pokrewne

Przegląd zdalnego dostępu do plików kluczy systemu EFS (Encrypted File System)
W tym miejscu podano informacje o bazach danych systemu EFS (Encrypted File System), włączaniu LDAP dla komend EFS i dostępie do unikalnego pliku kluczy.

Standardy PKCS11 (Public Key Cryptography Standards #11)

Podsystem PKCS11 udostępnia aplikacjom metodę dostępu do urządzeń sprzętowych (tokenów) bez względu na typ urządzenia.

Dane znajdujące się w tej sekcji dotyczą wersji 2.20 standardu PKCS11.

Podsystem PKCS11 używa następujących komponentów:

- Obiekt (`/usr/lib/pkcs11/ibm_pks11.so`) współużytkowany przez interfejs API, który jest udostępniany jako ogólny interfejs przeznaczony dla sterownika urządzenia, który obsługuje standard PKCS11. Warstwowa konstrukcja umożliwia używanie nowych urządzeń PKCS11, kiedy stają się dostępne, bez konieczności ponownej kompilacji istniejących aplikacji.
- Sterownik urządzenia PKCS11, który udostępnia możliwości aplikacjom podobne do możliwości udostępnianych innym komponentom jądra, takim jak EFS (Encrypted File System) i bezpieczeństwo IP (IPSec).
- Gdy platforma obsługuje narzędzie koprocesora kryptograficznego, sterownik urządzenia PKCS11 używa akceleracji sprzętowej dostępnej dla operacji AES (Advanced Encryption Standard), SHA (Secure Hash Algorithm) i HMAC (Hash Message Authentication Code). Aby uzyskać większą wydajność, można włączyć powinowactwo pamięci sieciowej.

Informacje pokrewne

Obsługa powinowactwa pamięci w systemie AIX

Koprocesor szyfrujący IBM 4758 model 2

Koprocesor szyfrujący IBM 4758 model 2 udostępnia bezpieczne środowisko obliczeniowe.

Przed skonfigurowaniem podsystemu PKCS11 należy sprawdzić, czy ten adapter został poprawnie skonfigurowany i czy jego mikrokod jest obsługiwany.

Akcelerator szyfrujący IBM 4960 Cryptographic Accelerator

Akcelerator szyfrujący IBM 4960 udostępnia środki do odciążenia transakcji szyfrujących. Przed skonfigurowaniem podsystemu PKCS11 należy sprawdzić, czy adapter został poprawnie skonfigurowany.

Sprawdzenie koprocesora szyfrującego IBM 4758 model 2 przeznaczonego do użycia w podsystemie PKCS11

Podsystem PKCS11 został zaprojektowany w sposób umożliwiający mu automatyczne wykrywanie adapterów obsługujących wywołania podsystemu PKCS11 podczas instalacji i restartu. Dlatego żaden koprocesor szyfrujący IBM 4758 model 2, który nie został poprawnie skonfigurowany, nie będzie dostępny z interfejsu PKCS11, a wywołania wysłane do takiego adaptera nie powiodą się.

Aby sprawdzić, czy adapter został skonfigurowany poprawnie, wykonaj następujące czynności:

1. Sprawdź, czy oprogramowanie adaptera zostało poprawnie zainstalowane, używając komendy:

   ```
   lsdev -Cc adapter | grep crypt
   ```

   Jeśli na liście nie ma koprocesora szyfrującego IBM 4758 model 2, sprawdź, czy jego karta została poprawnie osadzona i czy poprawnie zainstalowano obsługujące go oprogramowanie.
2. Sprawdź, czy do karty załadowano odpowiednie oprogramowanie wbudowane, wpisując:

   ```
   csufclu /tmp/l ST numer_poboczny_urządzenia
   ```

   Sprawdź, czy do obrazu segmentu 3 załadowano aplikację PKCS11. Jeśli nie, zajrzyj do dokumentacji danego adaptera, aby uzyskać najnowszy mikrokod i instrukcje dotyczące jego instalacji.

Uwaga: Jeśli ten program narzędziowy jest niedostępny, oznacza to, że oprogramowanie obsługujące nie zostało zainstalowane.

Sprawdzenie akceleratora szyfrującego IBM 4960 model 2 przeznaczonego do użycia w podsystemie PKCS11

Podsystem PKCS11 został zaprojektowany w sposób umożliwiający mu automatyczne wykrywanie adapterów obsługujących wywołania podsystemu PKCS11 podczas instalacji i restartu. Dlatego żaden akcelerator szyfrujący IBM 4960, który nie został poprawnie skonfigurowany, nie będzie dostępny z interfejsu PKCS11, a wywołania wysłane do takiego adaptera nie powiodą się.

Aby sprawdzić, czy oprogramowanie adaptera zostało poprawnie zainstalowane, używaj komendy:

```
lsdev -Cc adapter | grep ica
```

Jeśli na liście nie ma akceleratora szyfrującego IBM 4960, sprawdź, czy jego karta została poprawnie osadzona i czy poprawnie zainstalowano obsługujący go sterownik urządzenia.

Konfigurowanie podsystemu PKCS11 (Public Key Cryptography Standards #11)

Podsystem PKCS11 automatycznie wykrywa urządzenia obsługujące ten podsystem. Jednak aby niektóre aplikacje mogły używać tych urządzeń, wymagane jest wykonanie początkowej konfiguracji.

Zadania te można wykonać za pomocą interfejsu API (pisząc aplikację PKCS11) lub za pomocą interfejsu programu SMIT. Opcje programu SMIT dla pakietu PKCS11 są dostępne po wybraniu z głównego menu programu SMIT pozycji **Zarządzanie podsystemem PKCS11** lub za pomocą krótkiej ścieżki **`smit pkcs11`**.

Inicjowanie tokenu

Każdy adapter lub token podsystemu PKCS11 musi być zainicjowany zanim zostanie użyty.

Procedura inicjowania obejmuje ustawienie unikalnej etykiety tokenu. Etykieta ta umożliwia aplikacjom unikalne identyfikowanie tokenu. Etykiety nie mogą się więc powtarzać. Interfejs API nie sprawdza jednak, czy etykiety się nie powtarzają. Inicjowanie to można wykonać za pomocą aplikacji PKCS11 lub też może ją wykonać administrator systemu, korzystając z programu SMIT. Jeśli token dysponuje numerem PIN szefa bezpieczeństwa, wartość domyślna jest ustawiona na 87654321. Aby zapewnić bezpieczeństwo podsystemu PKCS11, wartość tę należy zmienić po zainicjowaniu.

Aby zainicjować token:

1. Wyświetl ekran zarządzania tokenami, wpisując `smit pkcs11`.
2. Wybierz opcję **Zainicjuj token**.
3. Z listy obsługiwanych adapterów wybierz adapter PKCS11.
4. Potwierdź wybór, naciskając klawisz Enter.

   Uwaga: Wykonanie tej czynności spowoduje wymazanie wszystkich informacji w tokenie.
5. Wpisz numer PIN szefa bezpieczeństwa (SB PIN) i unikalną etykietę tokenu.

Jeśli zostanie wprowadzony niepoprawny numer PIN, adapter będzie inicjowany lub reinicjowany po zakończeniu działania komendy.

Ustawianie numeru PIN szefa bezpieczeństwa

Poniższe czynności należy wykonać, aby zmienić numer PIN szefa bezpieczeństwa z jego wartości domyślnej.

Aby zmienić numer PIN z wartości domyślnej:

1. Wpisz `smit pkcs11`.
2. Wybierz opcję **Ustal numer PIN szefa bezpieczeństwa (SB)**.
3. Wybierz zainicjowany adapter, dla którego chcesz zmienić numer PIN.
4. Wpisz aktualny numer PIN i nowy numer PIN.
5. Sprawdź nowy numer PIN.

Inicjowanie numeru PIN użytkownika
Po zainicjowaniu tokenu może być konieczne ustawienie numeru PIN użytkownika, aby umożliwić aplikacjom dostęp do obiektów tokenu.

Aby sprawdzić, czy dane urządzenie wymaga, aby użytkownik zalogował się przed uzyskaniem dostępu do obiektów, skorzystaj z dokumentacji dotyczącej tego urządzenia.

Aby zainicjować numer PIN użytkownika:

1. Wyświetl ekran zarządzania tokenami, wpisując `smit pkcs11`.
2. Wybierz opcję **Zainicjuj numer PIN użytkownika**.
3. Z listy obsługiwanych adapterów wybierz adapter PKCS11.
4. Wpisz numer PIN szefa bezpieczeństwa i użytkownika.
5. Sprawdź numer PIN użytkownika.
6. Po weryfikacji numer PIN użytkownika musi być zmieniony.

Resetowanie numeru PIN użytkownika
W celu zresetowania numeru PIN użytkownika można go reinicjować używając numeru PIN szefa bezpieczeństwa lub można go ustawić używając istniejącego numeru PIN użytkownika.

Aby zresetować numer PIN użytkownika:

1. Wyświetl ekran zarządzania tokenami, wpisując `smit pkcs11`.
2. Wybierz opcję **Ustal numer PIN użytkownika**.
3. Wybierz zainicjowany adapter, dla którego chcesz zmienić PIN użytkownika.
4. Wpisz aktualny numer PIN użytkownika i nowy numer PIN.
5. Sprawdź nowy numer PIN użytkownika.

Użycie standardów PKCS11 (Public Key Cryptography Standards #11)
Aby aplikacja mogła używać podsystemu PKCS11, demon menedżera gniazd podsystemu musi być uruchomiony, a aplikacja musi załadować obiekt współużytkowany funkcji API.

Menedżer gniazd jest zwykle uruchamiany podczas startu systemu za pomocą pliku **inittab** wywołującego skrypt `/etc/rc.pkcs11`. Ten skrypt sprawdza adaptery w systemie przed uruchomieniem demona menedżera gniazd. Dlatego demon menedżera gniazd jest niedostępny przed zalogowaniem się użytkownika w systemie. Po uruchomieniu demona podsystem włącza zmiany dotyczące liczby i typów obsługiwanych adapterów bez konieczności interwencji administratora systemu.

Funkcja API może być załadowana albo przez konsolidację obiektu w czasie wykonania, albo za pomocą odroczonej konwersji symboli. Na przykład aplikacja może uzyskać listę funkcji PKCS11 w następujący sposób:

```
d CK_RV (*pf_init)();
void *d;
CK_FUNCTION_LIST *functs;

d = dlopen(e, RTLD_NOW);
if ( d == NULL ) {
   return FALSE;
}

pfoo = (CK_RV (*)())dlsym(d, “C_GetFunctionList”);
if (pfoo == NULL) {
   return FALSE;
}

rc = pf_init(&functs);
```

Narzędzia standardów PKCS11 (Public Key Cryptography Standards #11)
Do zarządzania systemami szyfrującymi w systemie operacyjnym AIX udostępniono dwa narzędzia: narzędzie do zarządzania kluczami PKCS11 (PKCS #11 Key Management) i narzędzie do administrowania PKCS11 (PKCS #11 Administration). Dostęp do tych narzędzi jest możliwy za pomocą interfejsu GUI opartego na Curses i za pomocą interfejsu wiersza komend.

Uwaga: Ułatwienia dostępu dla narzędzi środowiska szyfrującego AIX wymagają użycia funkcji przetwarzania wsadowego. Aby uzyskać szczegółowe informacje o używaniu funkcji przetwarzania wsadowego dla ułatwień dostępu, patrz “Przetwarzanie wsadowe” na stronie 192.

Narzędzie do zarządzania kluczami PKCS11 (PKCS #11 Key Management) jest scentralizowanym narzędziem służącym do zarządzania kluczami, certyfikatami i danymi PKCS11 w systemie operacyjnym AIX. Obiekty zarządzane za pomocą tego narzędzia są przechowywane w ramach obsługiwanych dostawców PKCS11, takich jak rodzina adapterów szyfrujących IBM (na przykład IBM 4758, 4960 i 4764) i środowisko szyfrujące AIX (AIX Cryptographic Framework). Za pomocą narzędzia do zarządzania kluczami PKCS11 można wykonać różne operacje. Należą do nich tworzenie żądań podpisania certyfikatu (CSR) PKCS #10 i generowanie samopodpisanych certyfikatów. Ponadto tego narzędzia można użyć do wyszukiwania, przeglądania, usuwania, importowania, eksportowania i tworzenia kopii zapasowych danych obiektów PKCS11, a także transportowania danych obiektów PKCS11 między znacznikami PKCS11. Wersję GUI tego narzędzia można uruchomić za pomocą komendy **p11km**. Narzędzie to ładuje wszystkie dostępne znaczniki PKCS11. Szczegóły dotyczące tych znaczników można przeglądać, używając klawiszy strzałek do przewijania listy znaczników. Aby wybrać znacznik, należy użyć klawiszy strzałek do podświetlenia znacznika, a następnie nacisnąć klawisz Enter. Wersję dla wiersza komend tego narzędzia można uruchomić za pomocą komendy:

```
p11km -b <plik wsadowy>
```

Narzędzie do administrowania PKCS11 (PKCS #11 Administration) jest scentralizowanym narzędziem służącym do zarządzania środowiskiem szyfrującym PKCS11 systemu AIX (AIX PKCS #11 Cryptographic Framework). Narzędzie to umożliwia administratorowi lub osobie odpowiedzialnej za bezpieczeństwo zarządzanie znacznikami kontrolowanymi przez środowisko AIX Cryptographic Framework. Tego narzędzia można użyć do inicjowania, tworzenia i niszczenia znaczników PKCS11, zarządzania szczelinami, resetowania haseł użytkowników, potwierdzania usunięć obiektów, określania relacji zaufania obiektów i strojenia środowiska AIX Cryptographic Framework pod kątem wydajności i ogólnych zadań administracyjnych. Wersję GUI tego narzędzia można uruchomić za pomocą komendy **p11admin**. Narzędzie to ładuje wszystkie dostępne znaczniki PKCS11. Szczegóły dotyczące tych znaczników można przeglądać, używając klawiszy strzałek do przewijania listy znaczników. Aby wybrać znacznik, należy użyć klawiszy strzałek do podświetlenia znacznika, a następnie nacisnąć klawisz Enter. Wersję wiersza komend tego narzędzia można uruchomić za pomocą komendy:

```
p11admin -b <plik wsadowy>
```

Profile komend
Do analizowania plików konfiguracyjnych używanych podczas tworzenia profili niestandardowych środowisko AIX Cryptographic Framework używa biblioteki OpenSSL. Profili tych można użyć do ustawiania atrybutów narzędzia, takich jak kolory interfejsu GUI dla komend **p11km** i **p11admin**.

Używając formatu pliku, który opisuje “Przetwarzanie wsadowe” na stronie 192, można utworzyć i zmodyfikować podane poniżej pliki profili w celu dostosowania interfejsu GUI.

Uwaga: Po utworzeniu plików profili należy nadać im nazwy i zapisać je w katalogu osobistym w następujący sposób:

```
$HOME/.p11km

$HOME/.p11admin
```

Obsługiwane są następujące atrybuty kolorów interfejsu GUI:

```
action_name = “GUI_COLORS”
gui_fg_color = “<nazwa koloru>” ## kolor pierwszego planu
gui_bg_color = “<nazwa koloru>” ## kolor tła
gui_vc_color = “<nazwa koloru>” ## kolor treści widoku
```

<*nazwa koloru*> jest jedną z następujących wartości:

LIGHT GRAY
WHITE

BLACK
DARK GRAY
RED
LIGHT RED
YELLOW
ORANGE or BROWN
GREEN
LIGHT GREEN
BLUE
LIGHT BLUE
CYAN
LIGHT CYAN
MAGENTA
LIGHT MAGENTA

Przykład: p11km profile ($HOME/.p11km)

```
[p11km_cmd]
gui_fg_color = “RED”
gui_bg_color = “BLACK”
gui_vc_color = “WHITE”
```

Przykład: p11admin Profile ($HOME/.p11admin)

```
[p11admin_cmd]
gui_fg_color = “BLUE”
gui_bg_color = “LIGHT GRAY”
gui_vc_color = “BLACK”
```

Przetwarzanie wsadowe
Komendy przetwarzania wsadowego można uruchamiać z wiersza komend. Służą one do wykonywania tych samych zadań, które są dostępne w wersjach GUI narzędzi PKCS11.

Komendy w narzędziu zarządzania kluczami PKCS11 (PKCS #11 Key Management- p11km) mają następujący format:

```
p11km -b <plik wsadowy>
```

Komendy w narzędziu administrowania kluczami PKCS11 (PKCS #11 Key Administration - p11admin) mają następujący format:

```
p11admin -b <plik wsadowy>
```

Ponieważ narzędzia te do analizowania plików wsadowych używają biblioteki OpenSSL, format plików wsadowych jest zgodny z typowym formatem plików konfiguracyjnych OpenSSL. Każda sekcja jest oddzielną komendą, a pary składające się z atrybutu i wartości udostępniają informacje wymagane do przetwarzania. Komenda w każdej sekcji jest przetwarzana w kolejności od góry do dołu. Jeśli konkretna komenda wsadowa nie powiedzie się, zostanie wygenerowany błąd, a przetwarzanie wsadowe zakończy się bez przetwarzania kolejnych komend w sekcji.

Poniżej został przedstawiony przykład formatu pliku konfiguracyjnego OpenSSL.

```
[sekcja1]
atrybut1 = “wartość1”
atrybut2 = “wartość2”
...
atrybutN = “wartośćN”
[sekcja2]
atrybut1 = “wartość1”
atrybut2 = “wartość2”
...
atrybutN = “wartośćN”
...
...
```

```
[sekcjaN]
atrybut1 = “wartość1”
atrybut2 = “wartość2”
...
atrybutN = “wartośćN”
```

Aby zapewnić współistnienie sekcji komend narzędzia PKCS11 z sekcjami pliku konfiguracyjnego OpenSSL, dla sekcji narzędzia PKCS11 użyj następujących przedrostków:

narzędzie p11km
p11km_cmd

narzędzie p11admin
p11admin_cmd

Każda sekcja p11km_cmd i p11admin_cmd powinna zawierać tylko jeden atrybut action_name z łańcuchem tekstowym identyfikującym konkretną komendę powiązaną z tą sekcją. Najprostszym przykładem jest plik zawierający jedną sekcję komend opisującą komendę, która nie ma żadnych dodatkowych parametrów. Poniżej został przedstawiony przykład użycia narzędzia p11km do uruchomienia komendy wsadowej wyświetlającej znaczniki PKCS11 dostępne w systemie:

```
[p11km_cmd_list_my_tokens]
action_name=”LIST_TOKENS”
```

Każda komenda wsadowa obsługuje opcjonalny atrybut boolowski:

```
start_gui=”<wartość boolowska>”
```

Jeśli uruchomisz komendę wsadową zawierającą ten atrybut boolowski o wartości TRUE, po wykonaniu tej komendy przetwarzanie wsadowe zostanie zakończone i rozpocznie działanie interfejs GUI.

Uwaga: Jeśli plik wsadowy zawiera komendę używającą opcjonalnego atrybutu **start_gui**, nie zostaną przetworzone żadne komendy wsadowe podane po tej komendzie.

Komendy wsadowe
Komendy wsadowe umożliwiają dostęp do narzędzi PKCS11 z wiersza komend.

Narzędzie do zarządzania kluczami PKCS11 (PKCS #11 Key Management - p11km) udostępnia podane poniżej komendy wsadowe.

Uwaga: Aby używać komend wsadowych, wykonaj następujące czynności:

1. Utwórz i zmodyfikuj plik wsadowy zgodnie z opisem w sekcji “Przetwarzanie wsadowe” na stronie 192.
2. Utwórz nowe sekcje p11km_cmd zawierające atrybuty komend wsadowych, które mają być używane.

Wyświetl dostępne znaczniki PKCS11
Generuje raport i wyświetla informacje o znaczniku i szczelinie dla dostępnych znaczników PKCS11.

Atrybuty wymagane

```
action_name = “LIST_TOKENS”
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Gdzie <*wartość boolowska*> to TRUE lub FALSE.

Przykład

```
[p11km_cmd_list_tokens]
action_name = “LIST_TOKENS”
```

Wyświetl dostępne mechanizmy PKCS11
Generuje raport i wyświetla dostępne mechanizmy PKCS11 obsługiwane przez konkretny znacznik PKCS11 (uzgodniony przez podanie wartości atrybutów sterownika i szczeliny).

Atrybuty wymagane

```
action_name = “LIST_MECHANISMS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Gdzie <*numer gniazda* oznacza dodatnią liczbą całkowitą, a <*nazwa sterownika*> jest jedną z następujących wartości:

Wartość	**Opis**
AIX	Środowisko Cryptographic Framework systemu operacyjnego AIX
IBM_4758_4960	Sprzętowe adaptery szyfrujące IBM 4758/4960
IBM_4764	Sprzętowy adapter szyfrujący IBM 4764
Other	Po podaniu wartości OTHER należy podać także atrybut **p11_driver_path**.

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Atrybuty dodatkowe

```
p11_driver_path = “<ścieżka do sterownika PKCS11>”
```

Gdzie <*ścieżka do sterownika PKCS11*> oznacza pełną ścieżkę i nazwę pliku w systemie UNIX biblioteki PKCS11 używanej dla tej komendy. Ten atrybut można podać tylko wtedy, gdy dla atrybutu **p11_driver** ustawiono wartość 0THER.

Przykład

```
[p11km_cmd_list_4764_slot_0_mechs]
action_name = “LIST_MECHANISMS”
p11_driver = “IBM_4764”
p11_slot = “0”
start_gui = “TRUE”
```

Wyświetl dostępne obiekty PKCS11

Generuje raport i wyświetla dostępne obiekty PKCS11 obsługiwane przez znacznik PKCS11 (uzgodniony przez podanie wartości atrybutów sterownika i szczeliny).

Atrybuty wymagane

```
action_name = “LIST_OBJECTS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
p11_login = "<wartość boolowska>"
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
p11_sensitive = "<wartość boolowska>"
start_gui = "<wartość boolowska>"
```

Gdzie <*klasa obiektu PKCS11*> jest jedną z następujących wartości zgodnie z definicją w specyfikacji PKCS11 RSA:

```
CKO_DATA
CKO_CERTIFICATE
CKO_PUBLIC_KEY
CKO_PRIVATE_KEY
CKO_SECRET_KEY
CKO_HW_FEATURE
```

```
CKO_DOMAIN_PARAMETERS
CKO_MECHANISM
CKO_VENDOR_DEFINED
```

Przykład

```
[p11km_cmd_list_private_objs]
action_name = “LIST_OBJECTS”
p11_login = “TRUE”
p11_private = “TRUE”
p11_driver = “AIX”
p11_slot = “5”
```

Zmień numer PIN użytkownika znacznika PKCS11:

Zmienia numer PIN użytkownika znacznika PKCS11, który jest używany podczas logowania się w tym znaczniku.

Atrybuty wymagane

```
action_name = “CHANGE_USER_PIN”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_change_my_pin]
action_name = “CHANGE_USER_PIN”
p11_slot = “1337”
p11_driver = “IBM_4764”
```

Usuń obiekty PKCS11

Usuwa obiekty PKCS11. Obiekty są usuwane na podstawie numerowanej listy obiektów wygenerowanej w wyniku działania komendy **LIST_OBJECTS** i użycia takiego samego szablonu z następującymi atrybutami:

```
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
p11_sensitive = "<wartość boolowska>"
p11_login = "<wartość boolowska>"
```

Ostrzeżenie: Ponieważ stan i spójność znacznika nie są zachowywane między procesami przetwarzania wsadowego, może mieć miejsce nieumyślnie usunięcie obiektów. Podana kolejność obiektów jest zmieniana, gdy obiekty są dodawane lub usuwane przez inne procesy uruchomione dla tego samego znacznika w okresie od chwili pierwotnego wyświetlenia obiektu do czasu jego usunięcia.

Atrybuty wymagane

```
action_name = “DELETE_OBJECTS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_objects = “<CSV>”
```

Gdzie <*CSV*> jest albo słowem ALL (wszystkie obiekty znacznika), albo listą oddzielonych przecinkami dodatnich liczb całkowitych odpowiadających obiektom w ponumerowanej kolejności wyświetlania za pomocą podanych poniżej atrybutów opcjonalnych.

Atrybuty opcjonalne

```
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
```

```
p11_sensitive = "<wartość boolowska>"
p11_login = "<wartość boolowska>"
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_delete_seven_objects]
action_name = “DELETE_OBJECTS”
p11_slot = “0”
p11_driver = “AIX”
p11_objects = “1,5,10,11,12,27,33”
p11_login = “TRUE”
```

Przenieś obiekty PKCS11:

Przenosi obiekty PKCS11. Obiekty są przenoszone na podstawie numerowanej listy obiektów wygenerowanej w wyniku działania komendy **LIST_OBJECTS** i użycia takiego samego szablonu.

Ostrzeżenie: Ponieważ stan i spójność znacznika nie są zachowywane między procesami przetwarzania wsadowego, może mieć miejsce nieumyślnie przeniesienie obiektów. Podana kolejność obiektów jest zmieniana, gdy obiekty są dodawane lub usuwane przez inne procesy uruchomione dla tego samego znacznika w okresie od chwili pierwotnego wyświetlenia obiektu do czasu jego przeniesienia.

Atrybuty wymagane

```
action_name = “MOVE_OBJECTS”
##########################################
###### Identyfikacja znacznika źródłowego: ######
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
##########################################
###### Identyfikacja znacznika docelowego: ######
p11_driver_target = “<nazwa sterownika>”
p11_slot_target = "<numer gniazda>"
##########################################
###### Obiekty przenoszone do celu: ######
p11_objects = “<CSV>”
```

Atrybuty opcjonalne

```
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
p11_sensitive = "<wartość boolowska>"
p11_login = "<wartość boolowska>"
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_move_three_objects]
action_name = “MOVE_OBJECTS”
p11_slot = “0”
p11_slot_target = “1”
p11_driver = “AIX”
p11_driver_target = “AIX”
p11_objects = “15,20,60”
p11_login = “FALSE”
```

Kopiuj obiekty PKCS11

Kopiuje obiekty PKCS11. Obiekty są kopiowane na podstawie numerowanej listy obiektów wygenerowanej w wyniku działania komendy **LIST_OBJECTS** i użycia takiego samego szablonu.

Ostrzeżenie: Ponieważ stan i spójność znacznika nie są zachowywane między procesami przetwarzania wsadowego, może zdarzyć się nieumyślnie skopiowanie obiektów. Podana kolejność obiektów jest zmieniana, gdy obiekty są dodawane lub usuwane przez inne procesy uruchomione dla tego samego znacznika w okresie od chwili pierwotnego wyświetlenia obiektu do czasu jego skopiowania.

Atrybuty wymagane

```
action_name = “COPY_OBJECTS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_driver_target = “<nazwa sterownika>”
p11_slot_target = "<numer gniazda>"
p11_objects = “<CSV>”
```

Atrybuty opcjonalne

```
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
p11_sensitive = "<wartość boolowska>"
p11_login = "<wartość boolowska>"
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_copy_one_private_object]
action_name = “COPY_OBJECTS”
p11_slot = “0”
p11_slot_target = “1”
p11_driver = “AIX”
p11_driver_target = “AIX”
p11_objects = “3”
p11_login = “TRUE” ## WYMAGANE DO ZARZ. OBIEKTEM PRYWATNYM
```

Eksportuj obiekty PKCS11 do pliku i utwórz ich kopię zapasową

Eksportuje obiekty PKCS11 i tworzy ich kopię zapasową. Obiekty są eksportowane, a ich kopia zapasowa jest tworzona na podstawie numerowanej listy obiektów wygenerowanej w wyniku działania komendy **LIST_OBJECTS** i użycia takiego samego szablonu.

Ostrzeżenie: Ponieważ stan i spójność znacznika nie są zachowywane między procesami przetwarzania wsadowego, może zdarzyć się nieumyślnie wyeksportowanie obiektów. Podana kolejność obiektów jest zmieniana, gdy obiekty są dodawane lub usuwane przez inne procesy uruchomione dla tego samego znacznika w okresie od chwili pierwotnego wyświetlenia obiektu do czasu jego wyeksportowania.

Atrybuty wymagane

```
action_name = “EXPORT_OBJECTS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_object_file = “<nazwa pliku>"
p11_objects = “<CSV>”
```

Atrybuty opcjonalne

```
p11_label = “<łańcuch>”
p11_class = “<klasa obiektu PKCS#11>”
p11_private = "<wartość boolowska>"
p11_trusted = "<wartość boolowska>"
p11_sensitive = "<wartość boolowska>"
p11_login = "<wartość boolowska>"
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_backup_objects]
action_name = “EXPORT_OBJECTS”
p11_slot = “0”
p11_driver = “AIX”
p11_objects = “ALL”
p11_login = “TRUE”
p11_object_file = “/home/user1/p11km.backup”
```

Importuj obiekty PKCS11 z pliku

Importuje utworzone obiekty PKCS11 z pliku eksportu PKCS11.

Atrybuty wymagane

```
action_name = “IMPORT_OBJECTS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_object_file = “<nazwa pliku>"
```

Atrybuty opcjonalne

```
p11_login = “<wartość boolowska>” # WYMAGANE DO ZAIMPORTOWANIA OBIEKTÓW PRYWATNYCH
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_import_my_backed_up_objects]
action_name = “IMPORT_OBJECTS”
p11_slot = “0”
p11_driver = “AIX”
p11_login = “TRUE”
p11_object_file = “/home/user1/p11km.backup”
```

Utwórz certyfikat samopodpisany

Tworzy samopodpisany certyfikat X.509 i powiązane obiekty PKCS11 w znaczniku PKCS11.

Atrybuty wymagane

```
action_name = “CREATE_SSC”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_login = “TRUE”
p11_ssc_label = “<łańcuch>”
p11_ssc_config = “<plik konfiguracyjny openssl>”
```

Gdzie <*plik konfiguracyjny openssl*> oznacza pełną ścieżkę i nazwę pliku konfiguracyjnego OpenSSL w systemie UNIX zapełnionego wartościami używanymi podczas tworzenia samopodpisanego certyfikatu.

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_self_signed_certificate]
action_name = “CREATE_SSC”
p11_slot = “0”
p11_driver = “AIX”
p11_login = “TRUE”
p11_ssc_label = “Lab RADIUS Server”
p11_ssc_config = “/etc/radius/EAP-TLS/openssl.cnf”
```

Utwórz żądanie podpisania certyfikatu PKCS10

Tworzy żądanie certyfikacji lub żądanie podpisania certyfikatu PKCS10

Atrybuty wymagane

```
action_name = “CREATE_CSR”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_login = “TRUE”
p11_csr_label = “<łańcuch>”
p11_csr_file = “<ścieżka do pliku wyjściowego CSR>”
p11_csr_type = “<DER lub Base64>"
p11_csr_config = “<plik konfiguracyjny openssl>”
```

Gdzie <*DER lub Base64*> generuje plik wyjściowy żądania CSR zakodowany za pomocą ASN.1 (DER) lub plik wyjściowy żądania CSR zakodowany za pomocą Base64, a <*ścieżka do pliku wyjściowego CSR*> oznacza pełną ścieżkę i nazwę pliku wyjściowego CSR w systemie UNIX.

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11km_cmd_my_pkcs10_base64]
action_name = “CREATE_SSC”
p11_slot = “0”
p11_driver = “AIX”
p11_login = “TRUE”
p11_csr_label = “Lab RADIUS Server”
p11_csr_type = “Base64”
p11_csr_file = “/etc/radius/EAP-TLS/certreq.b64”
p11_csr_config = “/etc/radius/EAP-TLS/openssl.cnf”
```

Narzędzie administrowania PKCS11 (PKCS #11 Administration - p11admin) udostępnia podane poniżej komendy wsadowe.

Uwaga: Aby używać komend wsadowych, wykonaj następujące czynności:

1. Utwórz i zmodyfikuj plik wsadowy zgodnie z opisem w sekcji “Przetwarzanie wsadowe” na stronie 192.
2. Utwórz nowe sekcje p11km_cmd zawierające atrybuty komend wsadowych, które mają być używane.

Wyświetl dostępne znaczniki PKCS11

Generuje raport i wyświetla informacje o znaczniku i szczelinie dla dostępnych znaczników PKCS11.

Atrybuty wymagane

```
action_name = “ADM_LIST_TOKENS”
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Gdzie <*wartość boolowska*> to TRUE lub FALSE.

Przykład

```
[p11admin_cmd_list_tokens]
action_name = “ADM_LIST_TOKENS”
```

Wyświetl dostępne mechanizmy PKCS11

Generuje raport i wyświetla dostępne mechanizmy PKCS11 obsługiwane przez znacznik PKCS11 (uzgodniony przez podanie wartości atrybutów sterownika i szczeliny).

Atrybuty wymagane

```
action_name = “ADM_LIST_MECHANISMS”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Gdzie <*numer gniazda* oznacza dodatnią liczbą całkowitą, a <*nazwa sterownika*> jest jedną z następujących wartości:

Wartość	**Opis**
AIX	Środowisko Cryptographic Framework systemu operacyjnego AIX
IBM_4758_4960	Sprzętowe adaptery szyfrujące IBM 4758/4960
IBM_4764	Sprzętowy adapter szyfrujący IBM 4764
Other	Po podaniu wartości OTHER należy podać także atrybut **p11_driver_path**.

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Atrybuty dodatkowe

```
p11_driver_path = “<ścieżka do sterownika PKCS11>”
```

Gdzie <*ścieżka do sterownika PKCS11*> oznacza pełną ścieżkę i nazwę pliku w systemie UNIX biblioteki PKCS11 używanej dla tej komendy. Ten atrybut można podać tylko wtedy, gdy dla atrybutu **p11_driver** ustawiono wartość 0THER.

Przykład

```
[p11admin_cmd_list_4764_slot_0_mechs]
action_name = “ADM_LIST_MECHANISMS”
p11_driver = “IBM_4764”
p11_slot = “0”
start_gui = “TRUE”
```

Wyświetl informacje o znaczniku PKCS11

Wyświetla informacje o znaczniku i szczelinie PKCS11 dla znacznika PKCS11.

Atrybuty wymagane

```
action_name = “ADM_SHOW_TOKEN_INFO”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd]
action_name = “ADM_SHOW_TOKEN_INFO”
p11_slot = “411”
p11_driver = “IBM_4764”
```

Zainicjuj znacznik PKCS11:

Inicjuje znacznik PKCS11. Proces inicjowania resetuje znacznik, kasuje wszystkie zapisane obiekty i dane PKCS11 oraz umożliwia ponowne włączenie znacznika.

Ostrzeżenie: Ponieważ wszystkie obiekty i dane PKCS11 są kasowane podczas tego procesu, przed zainicjowaniem znacznika PKCS11 należy się upewnić, że te dane i obiekty nie są już potrzebne.

Atrybuty wymagane

```
action_name = “ADM_INIT_TOKEN”
p11_driver = “<nazwa sterownika>”
p11_slot = “<numer gniazda>” ## TAKI SAM, JAK W 'p11_init_slot'
p11_init_slot = “<numer gniazda>” ## TAKI SAM, JAK W 'p11_slot'
p11_init_label = “<łańcuch>” ## ETYKIETA NOWEGO ZNACZNIKA
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd]
action_name = “ADM_INIT_TOKEN”
p11_slot = “1”
p11_driver = “IBM_4764”
p11_init_slot = “1”
p11_init_label = “ABC Token”
```

Wyświetl zegar dla znacznika PKCS11

Wyświetla zegar sprzętowy dla znacznika PKCS11, jeśli ten znacznik ma zegar.

Atrybuty wymagane

```
action_name = “ADM_CLOCK_VIEW”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd]
action_name = “ADM_CLOCK_VIEW”
p11_slot = “1”
p11_driver = “IBM_4764”
```

Ustaw zegar dla znacznika PKCS11

Ustawia zegar sprzętowy dla znacznika PKCS11, jeśli ten znacznik ma zegar.

Atrybuty wymagane

```
action_name = “ADM_CLOCK_SET”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
p11_clock_set = “<dane zegara>”
```

Gdzie <*dane zegara*> oznacza bieżącą datę i godzinę wyrażoną jako czas uniwersalny w formacie: GG:MM:SS MM-DD-RRRR.

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd]
action_name = “ADM_CLOCK_SET”
p11_slot = “1”
p11_driver = “IBM_4764”
p11_clock_set = “23:59:59 12-31-1999”
```

Resetuj numer PIN dla użytkownika znacznika PKCS11

Resetuje numer PIN dla użytkownika znacznika PKCS11.

Atrybuty wymagane

```
action_name = “ADM_RESET_USER_PIN”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd_change_so_pin]
action_name = “ADM_RESET_USER_PIN”
p11_driver = “AIX”
p11_slot = “0”
```

Zmień numer PIN dla osoby odpowiedzialnej za bezpieczeństwo znacznika PKCS11

Zmienia numer PIN dla osoby odpowiedzialnej za bezpieczeństwo znacznika PKCS11. Tego numeru PIN używa się podczas wykonywania zadań administracyjnych.

Atrybuty wymagane

```
action_name = “ADM_CHANGE_SO_PIN”
p11_driver = “<nazwa sterownika>”
p11_slot = "<numer gniazda>"
```

Atrybuty opcjonalne

```
start_gui = "<wartość boolowska>"
```

Przykład

```
[p11admin_cmd_change_so_pin]
action_name = “ADM_CHANGE_SO_PIN”
p11_slot = “888”
p11_driver = “IBM_4764”
```

Moduły PAM (Pluggable Authentication Modules)

Struktura modułu PAM umożliwia administratorom systemów łączenie wielu mechanizmów uwierzytelniania w jeden system za pomocą podłączanych modułów.

Aplikacje, które wykorzystują moduł PAM, mogą zostać *przełączone* na nowe rozwiązania technologiczne bez konieczności modyfikowania istniejących aplikacji. Elastyczność ta umożliwia administratorom:

- wybieranie w systemie dowolnej usługi uwierzytelniania dla aplikacji,
- używanie wielu mechanizmów uwierzytelniania dla danej usługi,
- dodawanie nowych modułów usług uwierzytelniania bez konieczności modyfikowania istniejących aplikacji,
- wykorzystywanie wcześniej wprowadzonych haseł do uwierzytelniania w wielu modułach.

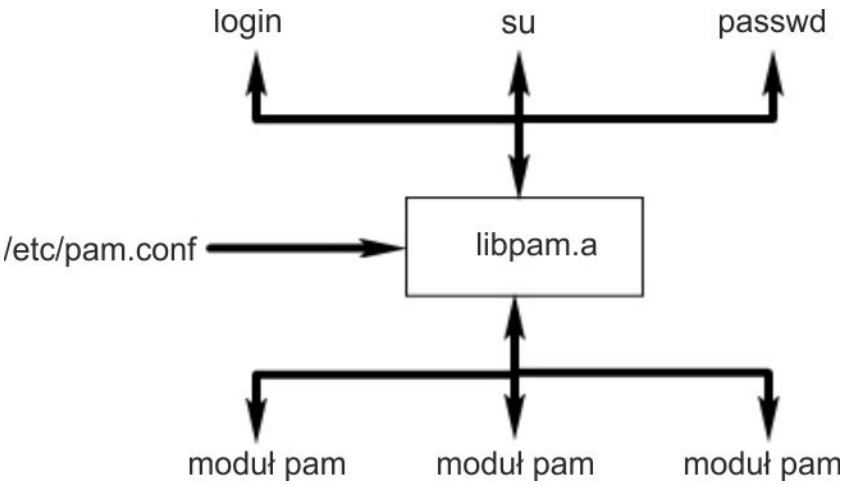
Na strukturę modułu PAM składają się biblioteka, podłączane moduły i plik konfiguracyjny. Biblioteka PAM implementuje aplikacyjny interfejs programowy modułu (API) PAM, ponadto zarządza transakcjami modułu PAM i wywołuje usługowe interfejsy programowe (SPI) zdefiniowane w podłączanych modułach. Podłączane moduły są ładowane dynamicznie przez bibliotekę w zależności od usługi wywołującej i wartości jej pozycji w pliku konfiguracyjnym. Prawidłowe działanie zależy nie tylko od podłączanego modułu, ale i od zachowania zdefiniowanego dla danej usługi. Dzięki koncepcji *stosu* usługę można tak skonfigurować, aby używała wielu metod uwierzytelniania. Jeśli jest to obsługiwane, to moduły można także skonfigurować, tak aby korzystały z wcześniej wysłanego hasła, zamiast żądać jego wprowadzenia.

Administrator systemu może skonfigurować system AIX do używania modułu PAM, modyfikując atrybut **auth_type** w sekcji usw w pliku `/etc/security/login.cfg`. Ustawienie atrybutu `auth_type = PAM_AUTH` powoduje włączenie komend modułu PAM, tak aby na potrzeby uwierzytelniania można było wywoływać bezpośrednio funkcje API modułu PAM, a nie używać historycznych procedur uwierzytelniania w systemie AIX. Konfiguracja ta odbywa się podczas pracy systemu i nie wymaga restartu systemu. Więcej informacji na temat atrybutu **auth_type** zawiera pomoc dotycząca pliku `/etc/security/login.cfg`. W celu umożliwienia rozpoznawania atrybutu **auth_type** i włączenia obsługi uwierzytelniania PAM zmodyfikowano następujące rodzime komendy systemu AIX oraz aplikacje:

- **login**
- **passwd**
- **su**
- **ftp**
- **telnet**
- **rlogin**
- **rexec**
- **rsh**
- **snappd**
- **imapd**

- **dtaction**
- **dtlogin**
- **dtsession**

Poniższy rysunek ilustruje interakcje pomiędzy aplikacjami z włączoną obsługą PAM, biblioteką PAM, plikiem konfiguracyjnym i modułami PAM w systemie, który został skonfigurowany do używania modułów PAM. Aplikacje z włączoną obsługą PAM wywołują funkcje API z biblioteki PAM. W zależności od wartości pozycji w pliku konfiguracyjnym dla danej aplikacji biblioteka określa odpowiedni moduł do załadowania i wywołuje funkcje SPI PAM w module. Komunikacja między modułem PAM a aplikacją odbywa się za pomocą funkcji konwersacji zaimplementowanej w aplikacji. W zależności od tego, czy działanie modułu zakończyło się pomyślnie i od zachowania zdefiniowanego w pliku konfiguracyjnym, może być potrzebny inny moduł. Jeśli tak, to proces jest kontynuowany, w przeciwnym przypadku dane są przekazywane z powrotem do aplikacji.



Rysunek 3. Struktura i elementy modułu PAM

Biblioteka PAM
Biblioteka PAM `/usr/lib/libpam.a` zawiera interfejs API PAM, który pełni rolę wspólnego interfejsu wszystkich aplikacji PAM oraz steruje ładowaniem modułów.

Moduły są ładowane przez bibliotekę PAM w zależności od zachowania stosu zdefiniowanego w pliku `/etc/pam.conf`.

Poniższe funkcje API PAM wywołują określone funkcje SPI PAM znajdujące się w PAM. Na przykład funkcja API `pam_authenticate` wywołuje funkcję SPI `pam_sm_authenticate` w module PAM.

- `pam_authenticate`
- `pam_setcred`
- `pam_acct_mgmt`
- `pam_open_session`
- `pam_close_session`
- `pam_chauthtok`

Biblioteka PAM obejmuje także kilka interfejsów API środowiska PAM umożliwiających aplikacjom wywoływanie modułów PAM i przekazywanie do nich informacji. W poniższej tabeli zebrano interfejsy API środowiska PAM, które zaimplementowano w systemie AIX, oraz należące do nich funkcje:

Interfejs API środowiska PAM	Funkcja
`pam_start`	Nawiązuje sesję PAM
`pam_end`	Kończy sesję PAM
`pam_get_data`	Wyszukuje dane charakterystyczne dla modułu

Interfejs API środowiska PAM	Funkcja
pam_set_data	Ustawia dane charakterystyczne dla modułu
pam_getenv	Pobiera wartość zdefiniowanej zmiennej środowiskowej PAM
pam_getenvlist	Pobiera listę wszystkich zdefiniowanych zmiennych środowiskowych PAM oraz ich wartości
pam_putenv	Ustawia zmienną środowiskową PAM
pam_get_item	Wyszukuje wspólne informacje PAM
pam_set_item	Ustawia wspólne informacje PAM
pam_get_user	Wyszukuje nazwę użytkownika
pam_strerror	Pobiera standardowe komunikaty o błędach modułu PAM

Moduły PAM
Moduły PAM pozwalają na łączne lub niezależne użycie w systemie wielu mechanizmów uwierzytelniania.

Dany moduł PAM musi mieć zaimplementowany przynajmniej jeden z czterech typów modułów. Typy modułów zostały opisane poniżej razem z odpowiadającymi im funkcjami SPI PAM, które muszą być dostosowane do typu modułu.

Moduły uwierzytelniające
Uwierzytelniają użytkowników, ustawiają, odświeżają lub niszczą referencje. Moduły te identyfikują użytkownika w oparciu o jego uwierzytelnienie i referencje.

Funkcje modułu uwierzytelniającego:

- pam_sm_authenticate
- pam_sm_setcred

Moduły zarządzania kontami
Określają poprawność konta użytkownika i jego późniejsze (po identyfikacji przez moduł uwierzytelniający) prawa dostępu. Moduły te zazwyczaj sprawdzają datę ważności konta i ograniczenia dotyczące hasła.

Funkcje modułu zarządzania kontami:

- pam_sm_acct_mgmt

Moduły zarządzania sesjami
Inicjują i kończą sesje użytkowników. Dodatkowo mogą obsługiwać kontrolę sesji.

Funkcje modułu zarządzania sesjami:

- pam_sm_open_session
- pam_sm_close_session

Moduły zarządzania hasłami
Wykonują zmiany hasła i powiązane z tym zarządzanie atrybutami.

Funkcje modułu zarządzania hasłami:

- pam_sm_chauthtok

Plik konfiguracyjny PAM
Plik konfiguracyjny /etc/pam.conf składa się z pozycji usług dla każdego typu modułu PAM i służy do kierowania usług do zdefiniowanej dla nich ścieżki modułu.

Pozycje w pliku składają się z następujących pól oddzielanych niewidocznymi znakami:

```
nazwa_usługi typ_modułu opcja_sterująca ścieżka_modułu opcje_modułu
```

Poniżej podano opisy tych pól:

nazwa_usługi
Nazwa usługi. Słowo kluczowe OTHER (pozostałe) służy do zdefiniowania domyślnego modułu dla aplikacji nieuwzględnionych w pozycji.

typ_modułu
Typ modułu dla usługi. Poprawne typy modułów to `auth`, `account`, `session` lub `password`. Jeden moduł obsługuje jeden lub więcej typów modułów.

opcja_sterująca
Zachowanie stosu dla modułu. Obsługiwane opcje sterujące to: required (wymagane), requisite (konieczne), sufficient (wystarczające) oraz optional (opcjonalne).

ścieżka_modułu

Określa moduł do załadowania dla usługi. Poprawną wartością parametru *ścieżka_modułu* może być pełna ścieżka do modułu lub tylko nazwa modułu. Jeśli zostanie podana pełna ścieżka modułu, biblioteka PAM użyje wartości zmiennej *module_path* do załadowania usług 32-bitowych lub podkatalogu 64 dla usług 64-bitowych. W przypadku niepodania pełnej ścieżki do modułu biblioteka PAM dołącza na początku nazwy modułu ścieżkę `/usr/lib/security` (dla usług 32-bitowych) lub `/usr/lib/security/64` (dla usług 64-bitowych).

opcje_modułu
Określa ograniczoną listę opcji, które mogą być przekazywane do modułów obsługujących. Wartości w tym polu zależą od opcji obsługiwanych przez moduł zdefiniowany w polu *ścieżka_modułu*. Pole to jest opcjonalne.

Pozycje zniekształcone lub z niepoprawnymi wartościami w polach **typ_modułu** lub **opcja_sterująca** są przez bibliotekę PAM ignorowane. Pozycje zaczynające się jednym lub większą liczbą znaków # są także ignorowane, gdyż znak ten oznacza komentarz.

Technologia PAM posługuje się pojęciem znanym powszechnie jako stos, który umożliwia korzystanie z wielu mechanizmów używanych dla każdej usługi. Stos jest implementowany w pliku konfiguracyjnym przez utworzenie wielu pozycji dla usług z taką samą wartością pola **typ_modułu**. Moduły są wywoływane w kolejności, w jakiej wymieniono je w pliku dla danej usługi, a końcowy rezultat jest określony przez pole **opcja_sterująca** podane dla każdej pozycji. Poprawne wartości pola **opcja_sterująca** i odpowiadające im zachowania w stosie są następujące:

Wartość pola control_flag	Zachowanie
required (wymagane)	Aby uwierzytelnianie powiodło się, wszystkie wymagane moduły ze stosu muszą poprawnie zakończyć działanie. Jeśli działanie jednego lub większej liczby modułów nie powiedzie się, wszystkie wymagane moduły ze stosu zostaną użyte, ale zwracany jest błąd z pierwszego wymaganego modułu, który się nie powiódł się.
requisite (konieczne)	Podobnie do required (wymagane), jeśli wywołanie modułu z opcją requisite (konieczne) nie powiedzie się, pozostałe moduły w stosie nie będą przetwarzane i zostanie zwrócony pierwszy kod błędu z modułu required (wymagane) lub requisite (konieczne).
sufficient (wystarczające)	Jeśli moduł z opcją sufficient zakończy się pomyślnie i przed nim pomyślnie zakończyły się wszystkie moduły wymagane i wystarczające, to pozostałe moduły ze stosu są ignorowane i zwracany jest kod pomyślnego zakończenia.
optional (opcjonalne)	Jeśli żaden z modułów ze stosu nie jest wymagany i nie powiódł się żaden z modułów wystarczających, wtedy przynajmniej jeden z modułów opcjonalnych musi zakończyć się powodzeniem. Jeśli inny moduł ze stosu zakończył się powodzeniem, to niepowodzenie modułu opcjonalnego jest ignorowane.

Następujący podzbiór /etc/pam.conf jest przykładem stosu dla typu modułu auth usługi logowania.

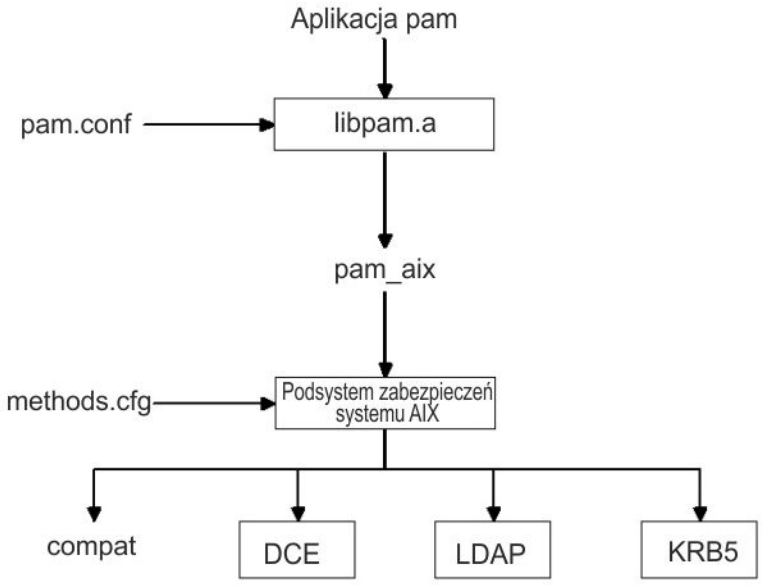
```
#
# Plik konfiguracyjny PAM /etc/pam.conf
#

# Zarządzanie uwierzytelnianiem
login   auth     required       /usr/lib/security/pam_ckfile    file=/etc/nologin
login   auth     required       /usr/lib/security/pam_aix
login   auth     optional       /usr/lib/security/pam_test      use_first_pass
OTHER   auth     required       /usr/lib/security/pam_prohibit
```

Przykładowy plik konfiguracyjny zawiera trzy pozycje dla usługi logowania. Po określeniu zarówno opcji pam_ckfile, jak i pam_aix jako required (wymagane), obydwa te moduły zostaną uruchomione. Aby końcowy wynik był pomyślny, obydwa te moduły muszą zostać przetworzone pomyślnie. Trzecia pozycja dla modułu pam_test jest opcjonalna i zarówno jej powodzenie, jak i niepowodzenie, nie wpłyną na możliwość zalogowania się użytkownika. Opcja use_first_pass modułu pam_test wymaga użycia wprowadzonego wcześniej hasła, zamiast oczekiwania na nowe.

Użycie słowa kluczowego OTHER w miejscu nazwy usługi umożliwia utworzenie pozycji domyślnej dla innych usług, niezdefiniowanych jawnie w pliku konfiguracyjnym. Skonfigurowanie wartości domyślnej daje pewność, że wszystkie przypadki dla danego typu modułu będą obsłużone przynajmniej przez jeden moduł. W tym przykładzie wszystkie usługi inne niż logowanie nie powiodą się, ponieważ moduł pam_prohibit zwraca błąd PAM na samym wstępie.

Moduł pam_aix
Moduł pam_aix umożliwia aplikacjom działającym z PAM dostęp do usług bezpieczeństwa systemu AIX, dostarczając interfejs wywołujący odpowiednik usług AIX (jeśli taki istnieje).

Usługi te są wykonywane z kolei przez ładowalny moduł uwierzytelniania lub wbudowaną funkcję systemu AIX, w zależności od definicji użytkownika i odpowiedniej konfiguracji w pliku methods.cfg. Kody błędów wygenerowane podczas wykonania usługi systemu AIX są odwzorowywane na odpowiednie kody błędów PAM.



Rysunek 4. Ścieżka między aplikacją PAM a podsystemem bezpieczeństwa systemu AIX

Rysunek pokazuje ścieżkę wywołania interfejsu API aplikacji PAM, jeśli plik /etc/pam.conf został skonfigurowany, tak aby korzystał z modułu pam_aix. Jak pokazano na diagramie, integracja umożliwia użytkownikowi uwierzytelnianie przez dowolny z ładowalnych modułów uwierzytelniania (DCE, LDAP lub KRB5) lub przez pliki systemu AIX (compat - sprawdzanie zgodności).

Moduł pam_aix jest instalowany w katalogu /usr/lib/security. Aby zintegrować moduł pam_aix, należy tak skonfigurować plik /etc/pam.conf, aby używał tego modułu. Stos jest nadal dostępny, ale nie został pokazany w poniższym przykładzie pliku /etc/pam.conf:

```
#
# Zarządzanie uwierzytelnianiem
#
OTHER   auth     required       /usr/lib/security/pam_aix

#
# Zarządzanie kontami
#
OTHER   account  required       /usr/lib/security/pam_aix

#
# Zarządzanie sesjami
#
OTHER   session  required       /usr/lib/security/pam_aix

#
# Zarządzanie hasłami
#
OTHER   password required       /usr/lib/security/pam_aix
```

Moduł pam_aix zawiera implementację funkcji SPI pam_sm_authenticate, pam_sm_chauthok i pam_sm_acct_mgmt. Zaimplementowane są także funkcje SPI pam_sm_setcred, pam_sm_open_session i pam_sm_close_session, ale zwracają tylko PAM_SUCCESS.

Oto przybliżone odwzorowanie wywołania podsystemu bezpieczeństwa AIX przez SPI PAM:

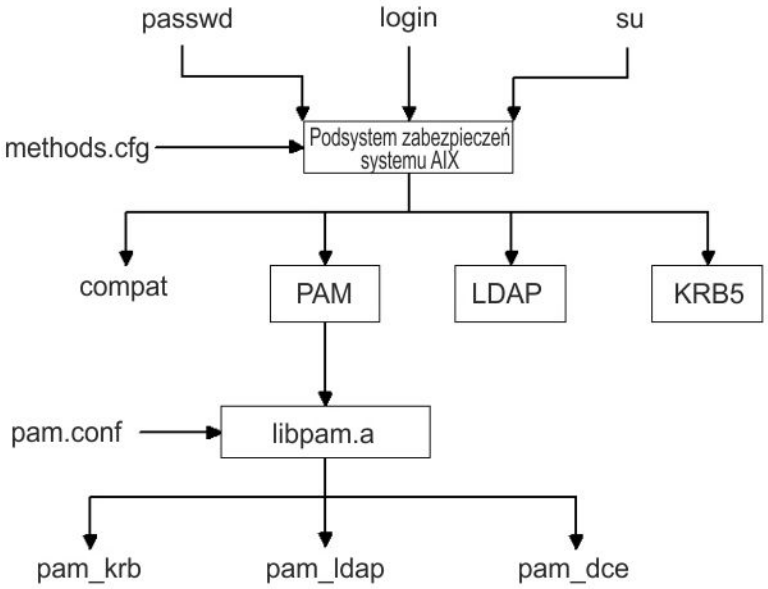
```
 SPI PAM                    AIX
=========                  =====
pam_sm_authenticate   -->  authenticate
pam_sm_chauthtok      -->  passwdexpired, chpass
                           Uwaga: passwdexpired jest sprawdzane tylko, jeśli
                           przesłano opcję PAM_CHANGE_EXPIRED_AUTHTOK.
pam_sm_acct_mgmt      -->  loginrestrictions, passwdexpired
pam_sm_setcred        -->  Brak odwzorowania do porównania, zwrócono PAM_SUCCESS
pam_sm_open_session   -->  Brak odwzorowania do porównania, zwrócono PAM_SUCCESS
pam_sm_close_session  -->  Brak odwzorowania do porównania, zwrócono PAM_SUCCESS
```

Dane, w zamierzeniu wysłane do podsystemu bezpieczeństwa systemu AIX, mogą przed użyciem przez moduł zostać ustawione za pomocą funkcji pam_set_item albo moduł pam_aix poprosi o te dane, jeśli nie zostały jeszcze wprowadzone.

Moduł ładowalny uwierzytelniania PAM
Usługi bezpieczeństwa systemu AIX można skonfigurować w taki sposób, aby wywoływały moduły PAM za pomocą istniejącej struktury ładowalnych modułów uwierzytelniania systemu AIX.

Uwaga: Przed wersją 5.3 systemu AIX moduł uwierzytelniania PAM był używany do zapewnienia uwierzytelniania PAM dla rodzimych aplikacji AIX. Ze względu na różnice w zachowaniu między tym rozwiązaniem a rzeczywistym rozwiązaniem PAM, moduł ładowalny uwierzytelniania PAM nie jest już zalecany do zapewnienia uwierzytelniania PAM dla rodzimych aplikacji AIX. Zamiast tego atrybut auth_type w sekcji usw pliku /etc/security/login.cfg powinien zostać ustawiony na wartość PAM_AUTH, aby włączyć uwierzytelnianie PAM w systemie AIX. Więcej informacji na temat atrybutu auth_type znajduje się w pliku /etc/security/login.cfg. Używanie ładowalnego modułu uwierzytelniania PAM jest nadal obsługiwane, ale nie jest zalecane. Do włączania uwierzytelniania PAM należy użyć atrybutu auth_type.

Gdy plik /usr/lib/security/methods.cfg jest prawidłowo skonfigurowany, moduł ładowany PAM kieruje usługi bezpieczeństwa systemu AIX (passwd, login, itp.) do biblioteki PAM. Biblioteka PAM sprawdza plik /etc/pam.conf, aby określić, którego modułu PAM użyć, i wywołuje odpowiednią funkcję SPI PAM. Wartości zwracane przez PAM są odwzorowywane na kody błędów systemu AIX i zwracane do programu wywołującego.



Rysunek 5. Ścieżka między usługami zabezpieczeń systemu AIX i modułem PAM

Rysunek pokazuje ścieżkę wywołania usługi bezpieczeństwa systemu AIX, gdy moduł PAM jest prawidłowo skonfigurowany. Przedstawione moduły PAM (pam_krb, pam_ldap i pam_dce) są wymienione jako przykłady rozwiązań innych firm.

Moduł ładowalny PAM jest zainstalowany w katalogu `/usr/lib/security`, który służy tylko do uwierzytelniania. Może być używany tylko w połączeniu z bazą danych. W przykładzie pokazano sekcje, które należy dodać do pliku `methods.cfg`, aby utworzyć moduł PAM z bazą danych nazwaną files. Słowo kluczowe BUILTIN dla atrybutu db oznacza, że bazę danych stanowią pliki systemu UNIX.

```
PAM:
        program = /usr/lib/security/PAM

PAMfiles:
        options = auth=PAM,db=BUILTIN
```

Tworzenie i modyfikowanie użytkowników jest następnie wykonywane z użyciem opcji -R za pomocą komend administracyjnych i z ustawianiem atrybutu *SYSTEM* podczas tworzenia użytkownika. Na przykład:

```
mkuser -R PAMfiles SYSTEM=PAMfiles registry=PAMfiles użytkownik pam
```

Działanie to powoduje, że przyszłe wywołania usług bezpieczeństwa systemu AIX (login, passwd itp.) będą używały ładowanego modułu PAM w celu uwierzytelnienia. W tym przykładzie do utworzenia modułu użyliśmy bazy danych **files**, jednak po zainstalowaniu można użyć innej bazy danych, na przykład LDAP. Utworzenie użytkowników zgodnie z powyższym opisem da w wyniku następujące odwzorowanie zabezpieczeń systemu AIX na wywołania funkcji API PAM:

```
         Komenda AIX             Funkcja API PAM
        =====                   =========
        authenticate       -->  pam_authenticate
        chpass             -->  pam_chauthtok
        passwdexpired      -->  pam_acct_mgmt
        passwdrestrictions -->  Brak odwzorowania do porównania, zwrócono sukces
```

Dostosowanie pliku `/etc/pam.conf` umożliwia przekierowanie wywołań funkcji API PAM do odpowiedniego modułu PAM w celu uwierzytelnienia. Aby jeszcze bardziej udoskonalić mechanizm uwierzytelniania, można zaimplementować stos.

Dane, o które pyta usługa bezpieczeństwa systemu AIX, są przekazywane do modułu PAM przez funkcję `pam_set_item`, gdyż nie ma możliwości przystosowania przez PAM dialogu użytkownika. Moduły PAM,

napisane w celu zintegrowania z modułem PAM, powinny otrzymywać wszystkie dane z wywołania funkcji pam_get_item i nie powinny prosić użytkownika o wprowadzenie danych, gdyż robi to usługa bezpieczeństwa.

Udostępniono wykrywanie pętli, aby zapobiec potencjalnym błędom konfiguracji, powodującym, że usługa bezpieczeństwa systemu AIX zostaje przekierowana do PAM, a następnie moduł PAM do wykonania zadania próbuje wywołać usługę bezpieczeństwa systemu AIX. Wykrycie pętli spowoduje natychmiastowe niepowodzenie planowanej operacji.

Uwaga: Plik /etc/pam.conf *nie* powinien wykorzystywać modułu pam_aix, jeśli używana jest integracja usługi bezpieczeństwa systemu AIX z modułem PAM, gdyż może to spowodować powstanie pętli.

Dodawanie modułu PAM
Dodanie modułu PAM powoduje włączenie wielu mechanizmów uwierzytelniania.

1. Umieść 32-bitową wersję modułu w katalogu /usr/lib/security a 64-bitową wersję modułu - w katalogu /usr/lib/security/64.
2. Zmień właściciela plików na użytkownika root i ustaw uprawnienia na wartość 555.

   Biblioteka PAM nie załaduje żadnych modułów, które nie są własnością użytkownika root.
3. Zaktualizuj plik konfiguracyjny /etc/pam.conf, aby w pozycjach dla wymaganej nazwy usługi była wpisana nazwa tego modułu.
4. Przetestuj tę usługę, aby sprawdzić jej funkcjonalność.

   Nie kończ sesji, dopóki nie wykonasz testu rozpoczęcia nowej sesji.

Zmiana pliku /etc/pam.conf
Przed zmianą pliku /etc/pam.conf trzeba wziąć pod uwagę kilka zagadnień.

Podczas dokonywania zmian w pliku konfiguracyjnym /etc/pam.conf należy zwrócić uwagę na następujące wymagania:

- Właścicielem pliku powinien być zawsze użytkownik root i grupa security. Uprawnienia dla pliku powinny wynosić 644, w celu umożliwienia wszystkim odczytu, lecz uprawnienie do zapisu powinien mieć tylko użytkownik root.
- W celu wzmocnienia bezpieczeństwa, należy rozważyć skonfigurowanie dokładnie każdej usługi z włączonym PAM, a następnie używanie modułu pam_prohibit dla słowa kluczowego usługi OTHER.
- Należy zapoznać się z dokumentacją dostarczoną z wybranym modułem i określić, jakie opcje i opcje sterujące on obsługuje, oraz jakie mają one znaczenie.
- Należy starannie wybrać kolejność modułów, pamiętając o działaniu opcji sterujących required (wymagane), requisite (konieczne), sufficient (wystarczające) i optional (opcjonalne) w stosie modułów.

Uwaga: Niepoprawna konfiguracja pliku konfiguracyjnego PAM może spowodować brak możliwości zalogowania się do systemu, ponieważ konfiguracja ma zastosowanie do wszystkich użytkowników włącznie z użytkownikiem root. Po wprowadzeniu zmian w pliku, zawsze przed wylogowaniem się z systemu należy przetestować aplikacje, dla których zostały wprowadzone zmiany. Aby odzyskać system, do którego nie można się zalogować, należy go uruchomić w trybie konserwacji i poprawić plik konfiguracyjny /etc/pam.conf.

Włączanie debugowania PAM
Podczas wykonywania, biblioteka PAM (Pluggable Authentication Modules) może udostępniać informacje debugowania. Po włączeniu w systemie zbierania danych diagnostycznych można zebrane dane wykorzystać do śledzenia wywołań funkcji API PAM i do określenia punktów awarii w bieżącej konfiguracji PAM.

Aby włączyć wyjście debugowania modułu PAM, wykonaj następujące kroki:

1. Utwórz pusty plik o nazwie pam_debug w katalogu /etc za pomocą komendy **touch**, jeśli taki plik nie istnieje. Biblioteka PAM sprawdza plik /etc/pam_debug i jeśli go znajdzie, włącza protokołowanie systemowe danych wyjściowych.

2. Dokonaj zmian w pliku `/etc/syslog.conf`, aby określić plik, w którym będą zapisywane komunikaty syslog `auth` o żądanym poziomie priorytetu. Aby na przykład wysyłać komunikaty na poziomie debugowania PAM do pliku `/var/log/auth.log`, dodaj następujący tekst jako nowy wiersz do pliku syslog.conf:

```
*.debug /var/log/auth.log
```

3. Utwórz plik wyjściowy przywoływany w kroku “2” na stronie 210, `/var/log/auth.log`, za pomocą komendy **touch**, jeśli jeszcze nie istnieje.
4. Zrestartuj demona syslogd, aby uwzględnić zmiany w konfiguracji. Wykonaj następujące kroki:
   a. Zatrzymaj demona syslog, wprowadzając następującą komendę:

```
stopsrc -s syslogd
```

   b. Uruchom demona syslog, wprowadzając następującą komendę:

```
startsrc -s syslogd
```

Gdy aplikacja PAM zostanie zrestartowana, komunikaty będą gromadzone w pliku wyjściowym zdefiniowanym w pliku konfiguracyjnym `/etc/syslog.conf`.

Obsługa OpenSSH i Kerberos w wersji 5

Protokół Kerberos jest mechanizmem uwierzytelniania, który udostępnia bezpieczny sposób uwierzytelniania użytkowników sieci. Uniemożliwia on transmisję haseł w postaci jawnego tekstu za pomocą sieci, szyfrując komunikaty uwierzytelniania między klientami a serwerami. Ponadto protokół Kerberos zapewnia w systemie autoryzację za pomocą tokenów administrowania lub referencji.

Aby uwierzytelnić użytkownika za pomocą protokołu Kerberos, użytkownik uruchamia komendę **kinit** w celu uzyskania początkowego uwierzytelnienia z centralnego serwera Kerberos, znanego jako centrum dystrybucji kluczy (Key Distribution Center - KDC). Centrum KDC weryfikuje użytkownika i przekazuje z powrotem do użytkownika początkowe uwierzytelnienie, znane jako Bilet nadania biletu (Ticket-Granting Ticket - TGT). Następnie użytkownik może uruchomić zdalną sesję użytkownika za pomocą usługi, takiej jak Telnet lub OpenSSH z obsługą Kerberos. Kerberos uwierzytelnia użytkownika, uzyskując jego uwierzytelnienia z centrum KDC. Kerberos uwierzytelnia użytkownika bez konieczności interakcji z jego strony, dlatego użytkownicy nie muszą wprowadzać haseł, aby się zalogować. Kerberos w wersji IBM jest znany jako usługa uwierzytelniania sieciowego (Network Authentication Service - NAS). Usługę NAS można zainstalować z dysku CD AIX Expansion Pack. Znajduje się ona w pakietach `krb5.client.rte` i `krb5.server.rte`. Począwszy od wersji OpenSSH 3.6 z lipca 2003, OpenSSH obsługuje uwierzytelnianie Kerberos 5 i autoryzację za pomocą usługi NAS w wersji 1.3.

OpenSSH, wersja 3.8 lub nowsza, obsługuje uwierzytelnianie Kerberos 5 i autoryzację poprzez usługę NAS, wersja 1.4. Wszystkie migracje z poprzednich wersji usługi NAS (Kerberos) muszą być przeprowadzone przed aktualizacją OpenSSH. OpenSSH, wersja 3.8.x współpracuje tylko z usługą NAS, wersja 1.4 lub nowsza.

AIX używa OpenSSH z uwierzytelnianiem Kerberos jako metody opcjonalnej. Jeśli biblioteki Kerberos nie są zainstalowane w systemie, uruchomienie uwierzytelniania Kerberos przez OpenSSH jest pomijane, a OpenSSH próbuje użyć następnej skonfigurowanej metody uwierzytelniania (takiej jak uwierzytelnianie systemu AIX).

Po zainstalowaniu protokołu Kerberos, a przed skonfigurowaniem serwerów do jego obsługi, zaleca się przeczytanie dokumentacji. Więcej informacji na temat sposobu instalowania i administrowania Kerberos zawiera publikacja *IBM Network Authentication Service Version 1.3 for AIX : Administrator's and User's Guide* dostępna w ścieżce `/usr/lpp/krb5/doc/html/język/ADMINGD.htm`.

Informacje pokrewne

OpenSSH

Obrazy OpenSSH
Aby zainstalować obrazy OpenSSH, należy wykonać następujące czynności:

1. Przejdź do serwisu WWW AIX Web Download Pack Programs.

   Uwaga: Obraz OpenSSH jest dostarczany jako część nośnika podstawowego systemu AIX, ale obraz ten domyślnie nie jest instalowany.
2. Kliknij opcję **Downloads** (Pobieranie) w sekcji Additional information (Informacje dodatkowe).
3. Zaloguj się, używając własnego identyfikatora i hasła do uzyskania dostępu do pakietów.
4. Wybierz opcję **OpenSSH** i kliknij opcję **Continue** (Kontynuuj).
5. Zaakceptuj umowę licencyjną, aby pobrać pakiet.
6. Za pomocą komendy **uncompress** *nazwa_pakietu* rozpakuj pakiet obrazu. Na przykład:

   ```
   uncompress OpenSSH_6.0.0.6203.tar.Z
   ```
7. Za pomocą komendy **tar -xvf** *nazwa_pakietu* rozpakuj (untar) pakiet. Na przykład:

   ```
   tar -xvf OpenSSH_6.0.0.6203.tar
   ```
8. Uruchom komendę **inutoc**.
9. Uruchom komendę **smitty install**.
10. Wybierz **Instalacja i aktualizacja oprogramowania**.
11. Wybierz **Uaktualnij zainstalowane oprogramowanie do najnowszej wersji (aktualizacja wszystkiego)**.
12. Wpisz kropkę (.) w polu **WEJŚCIOWE urządzenie / katalog oprogramowania** i naciśnij klawisz Enter.
13. Przewiń w dół do pola **ZAAKCEPTUJ nowe umowy licencyjne** i naciśnij klawisz Tab, aby zmienić wartość pola na **Tak**.
14. Aby rozpocząć instalowanie, dwa razy naciśnij klawisz Enter.

Obrazy OpenSSH są obrazami poziomu podstawowego, a nie poprawkami PTF. Podczas instalacji cały kod z poprzedniej wersji jest zastępowany obrazami nowej wersji.

Konfigurowanie kompilacji OpenSSH
Poniższe informacje zawierają omówienie sposobu kompilowania kodu OpenSSH dla systemu AIX.

Podczas konfigurowania OpenSSH dla AIX wersja 6.1 otrzymane dane wyjściowe są podobne do następujących:

```
OpenSSH has been configured with the following options:
                     User binaries: /usr/bin
                   System binaries: /usr/sbin
               Configuration files: /etc/ssh
                   Askpass program: /usr/sbin/ssh-askpass
                      Manual pages: /usr/man
                          PID file: /etc/ssh
  Privilege separation chroot path: /var/empty
           sshd default user PATH: /usr/bin:/bin:/usr/sbin:/sbin:/usr/
                                   local/bin

                    Manpage format: man
                       PAM support: yes
                   OSF SIA support: no
                 KerberosV support: yes
                 Smartcard support: no
                   SELinux support: no
                     S/KEY support: no
             TCP Wrappers support: yes
             MD5 password support: no
                  libedit support: no
  Solaris process contract support: no
              Solaris project support: no
       IP address in $DISPLAY hack: no
           Translate v4 in v6 hack: no
                 BSD Auth support: no
             Random number source: OpenSSL TYLKO wewnętrznie

             Host: powerpc-ibm-aix6.1.0.0
          Compiler: cc
```

```
Compiler flags: -bloadmap:file -qnostdinc -qnolm -qlist -qsource -qattr=full
Preprocessor flags: -I/gsa/ausgsa/projects/o/openssh/freeware5/openssl-0.9.8r/
            include -I/gsa/ausgsa/projects/o/openssh/zlib -I/usr/include

      Linker flags: -L/gsa/ausgsa/projects/o/openssh/freeware5/
                lib -L/gsa/ausgsa/projects/o/openssh/zlib -L/usr/include
                -Wl,-blibpath:/usr/lib:/lib
         Libraries: -lcrypto -lz -lc  -lcrypt -lefs   -lwrap -lpam -ldl
```

Uwaga: Opcje kompilacji dla systemów AIX wersja 6.1 i AIX wersja 7.1 są podobne, ponieważ kod binarny dla obu tych wersji jest taki sam.

Używanie oprogramowania OpenSSH z protokołem Kerberos
Użycie OpenSSH z protokołem Kerberos wymaga przeprowadzenia początkowej konfiguracji.

Wykonanie podanych poniżej kroków umożliwia przygotowanie początkowej konfiguracji, która jest wymagana do używania OpenSSH z Kerberos.

1. Na klientach i serwerach OpenSSH musi znajdować się plik `/etc/krb5.conf`. Plik ten informuje Kerberos, którego centrum KDC należy użyć, jak długi ma być czas życia biletu itd. Poniżej został przedstawiony przykład pliku `krb5.conf`:

   ```
   [libdefaults]
   ticket_lifetime = 600
   default_realm = OPENSSH.AUSTIN.XYZ.COM
   default_tkt_enctypes = des3-hmac-sha1 des-cbc-crc
   default_tgs_enctypes = des3-hmac-sha1 des-cbc-crc

   [realms]
   OPENSSH.AUSTIN.xyz.COM = {
       kdc = kerberos.austin.xyz.com:88
       kdc = kerberos-1.austin.xyz.com:88
       kdc = kerberos-2.austin.xyz.com:88
       admin_server = kerberos.austin.xyz.com:749
       default_domain = austin.xyz.com
   }

   [domain_realm]
       .austin.xyz.com = OPENSSH.AUSTIN.XYZ.COM
       kdc.austin.xyz.com = OPENSSH.AUSTIN.XYZ.COM
   ```

2. Ponadto do pliku `/etc/services` na każdym komputerze klienta musisz dodać następujące usługi Kerberos:

   ```
   kerberos      88/udp    kdc    # Kerberos V5 KDC
   kerberos      88/tcp    kdc    # Kerberos V5 KDC
   kerberos-adm  749/tcp          # Kerberos 5 admin/changepw
   kerberos-adm  749/udp          # Kerberos 5 admin/changepw
   krb5_prop     754/tcp          # Kerberos slave
                                  #  propagation
   ```

3. Jeśli używane centrum KDC korzysta z LDAP jako rejestru do przechowywania informacji o użytkownikach, przeczytaj sekcję “Moduł ładowalny uwierzytelniania LDAP” na stronie 158 i publikacje dotyczące protokołu Kerberos. Ponadto upewnij się, że zostały wykonane następujące czynności:

   - Centrum KDC zostało uruchomione na kliencie LDAP. Demon klienta LDAP możesz uruchomić za pomocą komendy **secldapclntd**.
   - Na serwerze LDAP został uruchomiony demon serwera LDAP `slapd`.

4. Na serwerze OpenSSH do pliku `/etc/ssh/sshd_config` dodaj następujące wiersze:

   ```
   KerberosAuthentication yes
   KerberosTicketCleanup yes
   GSSAPIAuthentication yes
   GSSAPICleanupCredentials yes
   UseDNS yes
   ```

   Jeśli wiersz UseDNS ma wartość **Yes**, serwer ssh wykonuje odwrotne szukanie hosta, w celu odnalezienia nazwy łączącego się klienta. Jest to konieczne w przypadku korzystania z

uwierzytelniania w oparciu o hosta lub gdy użytkownik chce, aby zamiast adresów IP w informacjach dotyczących ostatniego logowania wyświetlane były nazwy hostów.

Uwaga: Niektóre sesje ssh podczas odwrotnego wyszukiwania nazwy zawieszają się, ponieważ serwery DNS stają się nieosiągalne. Jeśli tak się zdarzy, można pominąć wyszukiwanie DNS, ustawiając parametr UseDNS na wartość no. Jeśli parametr UseDNS nie zostanie jawnie podany w pliku `/etc/ssh/sshd_config`, wartością domyślną jest `UseDNS yes`.

5. Na serwerze SSH uruchom komendę **`startsrc -g ssh`**, aby uruchomić demon serwera ssh.
6. Na komputerze klienta SSH uruchom komendę **`kinit`**, aby uzyskać początkowe uwierzytelnienie (bilet nadania biletu). Aby sprawdzić, czy uzyskałeś bilet nadania biletu, uruchom komendę **`klist`**. Wykonanie tej komendy powoduje wyświetlenie wszystkich uwierzytelnień, które należą do Ciebie.
7. Połącz się z serwerem, uruchamiając komendę **`ssh`** *nazwa_użytkownika@nazwa_serwera*.
8. Jeśli protokół Kerberos został poprawnie skonfigurowany do uwierzytelnienia użytkownika, nie zostanie wyświetlona zachęta do podania hasła, a użytkownik zostanie automatycznie zalogowany na serwerze SSH.

Zabezpieczenie sieci

Poniższe sekcje zawierają omówienie sposobu instalowania i konfigurowania bezpieczeństwa IP, identyfikowania usług sieciowych, które są niezbędne, a które niepotrzebne, a także informacje na temat kontrolowania i monitorowania bezpieczeństwa w sieci.

Bezpieczeństwo TCP/IP

Jeśli w systemie zainstalowano oprogramowanie Transmission Control Protocol/Internet Protocol (TCP/IP) i Network File System (NFS), można skonfigurować go do komunikacji przez sieć.

W tym rozdziale nie opisano podstawowych założeń protokołu TCP/IP, lecz podano tu raczej zagadnienia dotyczące bezpieczeństwa tego protokołu. Informacje na temat instalowania i początkowej konfiguracji protokołu TCP/IP zawiera sekcja Transmission Control Protocol/Internet Protocol w książce *Zarządzanie sieciami i komunikacją*.

Administrator systemu musi zapewnić pewien poziom bezpieczeństwa. Bezpieczeństwo systemu może być elementem szerszej strategii zabezpieczeń korporacji. System może potrzebować również dostępu do systemów instytucji rządowych i dlatego do komunikacji wymagany będzie określony poziom bezpieczeństwa. Te standardy bezpieczeństwa mogą mieć zastosowanie do sieci, systemu operacyjnego, aplikacji a nawet programów napisanych przez administratora systemu.

W tej sekcji opisano opcje zabezpieczające udostępniane wraz z protokołem TCP/IP zarówno w trybie standardowym, jak i w systemie chronionym oraz omówiono niektóre zagadnienia dotyczące bezpieczeństwa w środowisku sieciowym.

Po zainstalowaniu oprogramowania TCP/IP i NFS należy użyć krótkiej ścieżki **`tcpip`** programu SMIT, aby skonfigurować system.

Więcej informacji na temat komendy **`dacinet`** zawiera podręcznik *Commands Reference*.

Bezpieczeństwo a system operacyjny

Wiele opcji zabezpieczających dostępnych dla TCP/IP, takich jak kontrola dostępu do sieci i kontrola sieci, jest opartych na opcjach dostępnych w systemie operacyjnym.

W poniższych sekcjach omówiono bezpieczeństwo TCP/IP.

Kontrola dostępu do sieci

Strategia bezpieczeństwa sieci jest rozszerzeniem strategii bezpieczeństwa systemu operacyjnego i obejmuje uwierzytelnianie użytkowników, uwierzytelnianie połączeń i zabezpieczenie danych.

Składa się z następujących głównych komponentów:

- Uwierzytelnianie użytkowników jest zapewniane na zdalnym hoście za pomocą nazwy i hasła użytkownika w ten sam sposób, który jest używany, gdy użytkownik loguje się w systemie lokalnym. Zaufane komendy TCP/IP, takie jak **ftp**, **rexec** i **telnet** mają takie same wymagania i przechodzą przez taki sam proces weryfikacji, jak zaufane komendy w systemie operacyjnym.
- Uwierzytelnianie połączeń jest dostarczane, aby zapewnić zdalnemu hostowi oczekiwany adres IP i nazwę. Zapobiega to sytuacji, gdy zdalny host podszywa się pod inny zdalny host.
- Bezpieczeństwo importu i eksportu danych umożliwia przepływ danych o określonym poziomie bezpieczeństwa do i z adapterów interfejsu sieciowego o tych samych poziomach bezpieczeństwa i uprawnień. Na przykład ściśle tajne dane mogą przepływać tylko między adapterami, dla których ustawiono poziom bezpieczeństwa ściśle tajne.

Kontrola sieci
Kontrola sieci jest realizowana przez TCP/IP za pomocą podsystemu kontrolującego aplikacje.

Celem tej kontroli jest rejestrowanie działań dotyczących bezpieczeństwa systemu oraz użytkowników za nie odpowiedzialnych.

Kontrolowane są następujące zdarzenia aplikacji:

- dostęp do sieci,
- połączenie,
- eksport danych,
- import danych,

Tworzenie i usuwanie obiektów jest kontrolowane przez system operacyjny. Rekordy kontroli aplikacji zawieszają i wznawiają kontrolę, aby uniknąć nadmiarowej kontroli wykonywanej przez jądro.

Zaufana ścieżka, zaufana powłoka i sekwencja SAK
System operacyjny udostępnia *zaufaną ścieżkę*, aby uniemożliwić nieautoryzowanym programom odczyt danych z terminalu użytkownika. Ścieżka ta jest używana, gdy w systemie wymagana jest zabezpieczona ścieżka komunikacyjna, na przykład wtedy, gdy są zmieniane hasła lub gdy odbywa się logowanie do systemu.

System operacyjny udostępnia także *zaufaną powłokę* (**tsh**) pozwalającą na uruchamianie wyłącznie zaufanych programów, które zostały przetestowane i uznane za bezpieczne. TCP/IP obsługuje obie te opcje wraz z *sekwencją przywołania bezpiecznej komunikacji* (Secure Attention Key - SAK), która ustanawia środowisko niezbędne dla bezpiecznej komunikacji między użytkownikiem a systemem. Lokalna sekwencja SAK jest dostępna za każdym razem, gdy używany jest protokół TCP/IP. Zdalna sekwencja SAK jest dostępna za pomocą komendy **telnet**.

Lokalna sekwencja SAK pełni w komendzie **telnet** tę samą funkcję, którą pełni w innych programach systemu operacyjnego: powoduje ona zakończenie procesu **telnet** i wszystkich pozostałych procesów powiązanych z terminalem, na którym uruchomiono komendę **telnet**. W programie telnet można jednak wysłać żądanie zaufanej ścieżki do zdalnego systemu za pomocą komendy **telnet send sak** (podczas pracy w trybie komendy **telnet**). Można także zdefiniować pojedynczy klucz, aby zainicjować żądanie SAK za pomocą komendy **telnet set sak**.

Więcej informacji na temat bazy TCB zawiera sekcja “Zaufana Baza Przetwarzania” na stronie 2.

Bezpieczeństwo komend TCP/IP
Niektóre komendy TCP/IP zapewniają podczas pracy chronione środowisko. Należą do nich komendy **ftp**, **rexec** i **telnet**.

Funkcja **ftp** zapewnia bezpieczeństwo podczas przesyłania plików. Komenda **rexec** udostępnia chronione środowisko do uruchamiania komend na odległym hoście. Funkcja **telnet** zapewnia bezpieczeństwo podczas logowania na odległym hoście.

Komendy **ftp**, **rexec** i **telnet** zapewniają bezpieczeństwo tylko podczas pracy. Oznacza to, że nie konfigurują one chronionego środowiska, z którego mogłyby skorzystać inne komendy. Aby chronić system podczas wykonywania innych operacji, należy użyć komendy **securetcpip**. Komenda ta

umożliwia zabezpieczanie systemu przez wyłączanie niezaufanych demonów i aplikacji i przez udostępnianie opcji bezpieczeństwa protokołu sieciowego warstwy IP.

Komendy **ftp**, **rexec**, **securetcpip** i **telnet** udostępniają następujące formy zabezpieczeń systemu i danych:

ftp
Komenda **ftp** udostępnia chronione środowisko do przesyłania plików. Gdy użytkownik wywołuje komendę **ftp**, nawiązując połączenie ze zdalnym hostem, jest on proszony o podanie identyfikatora. Jako identyfikator domyślny wyświetlany jest obecny identyfikator użytkownika na hoście lokalnym. Użytkownik jest proszony o podanie hasła na zdalnym hoście.

Automatyczny proces logowania przeszukuje lokalny plik $HOME/.netrc użytkownika w celu znalezienia identyfikatora użytkownika i hasła, które można użyć na odległym hoście. Ze względów bezpieczeństwa, uprawnienia do pliku $HOME/.netrc muszą być ustawione na 600 (odczyt i zapis tylko przez właściciela). W przeciwnym razie automatyczne logowanie się nie powiedzie.

Uwaga: Ponieważ użycie pliku .netrc wymaga zapisania haseł w pliku niezaszyfrowanym, opcja automatycznego logowania komendy **ftp** jest niedostępna, gdy system został skonfigurowany za pomocą komendy **securetcpip**. Opcję tę można ponownie włączyć, usuwając komendę **ftp** z sekcji tcpip pliku /etc/security/config.

Aby używać funkcji przesyłania plików, komenda **ftp** wymaga połączeń TCP/IP: jednego dla protokołu FTP, a drugiego dla przesyłania danych. Połączeniem podstawowym jest połączenie protokołu i jest ono bezpieczne, ponieważ jest ustanawiane przez niezawodne porty komunikacyjne. Połączenie drugorzędne jest wymagane do przesyłania danych i zarówno lokalny, jak i zdalny host sprawdzają, czy druga strona połączenia jest ustanowiona z tym samym hostem, z którym nawiązano połączenie podstawowe. Jeśli połączenia podstawowe i drugorzędne nie zostały ustanowione z tym samym hostem, komenda **ftp** najpierw wyświetla komunikat o błędzie informujący o braku uwierzytelnienia połączenia danych, a następnie kończy pracę. Weryfikacja drugorzędnego połączenia uniemożliwia trzeciemu hostowi przechwycenie danych przeznaczonych dla innego hosta.

rexec
Komenda **rexec** udostępnia chronione środowisko do wykonywania komend na odległym hoście. Użytkownik jest proszony o podanie identyfikatora i hasła.

Opcja automatycznego logowania powoduje, że komenda **rexec** przeszukuje lokalny plik $HOME/.netrc użytkownika w celu znalezienia identyfikatora użytkownika i hasła dla zdalnego hosta. Ze względów bezpieczeństwa, uprawnienia do pliku $HOME/.netrc muszą być ustawione na 600 (odczyt i zapis tylko przez właściciela). W przeciwnym razie automatyczne logowanie się nie powiedzie.

Uwaga: Ponieważ użycie pliku .netrc wymaga zapisania haseł w pliku niezaszyfrowanym, opcja automatycznego logowania komendy **rexec** jest niedostępna, gdy system pracuje w trybie chronionym. Opcję tę można ponownie włączyć, usuwając wpis z sekcji tcpip pliku /etc/security/config.

securetcpip
Komenda **securetcpip** włącza opcje bezpieczeństwa TCP/IP. Po wprowadzeniu tej komendy dostęp do niezaufanych komend jest usuwany z systemu. Jej uruchomienie powoduje usunięcie następujących komend:

- **rlogin** i **rlogind**,
- **rcp**, **rsh** i **rshd**,
- **tftp** i **tftpd**,
- **trpt**.

Komendy **securetcpip** używa się w celu przekształcenia systemu ze standardowego poziomu bezpieczeństwa do wyższego poziomu bezpieczeństwa. Po przekształceniu systemu nie należy ponownie uruchamiać komendy **securetcpip**, chyba że reinstaluje się TCP/IP.

telnet lub tn

Komenda **telnet** (TELNET) udostępnia chronione środowisko do logowania się na odległym hoście. Użytkownik jest proszony o podanie identyfikatora i hasła. Terminal użytkownika jest traktowany tak samo jak terminal podłączony bezpośrednio do hosta. Oznacza to, że dostęp do terminalu jest kontrolowany przez bity uprawnień. Inni użytkownicy nie mają dostępu do odczytu terminalu, ale mogą do niego zapisywać komunikaty, jeśli właściciel nada im uprawnienie do zapisu. Komenda **telnet** udostępnia za pomocą sekwencji SAK także dostęp do zaufanej powłoki w systemie zdalnym. Ta sekwencja różni się od sekwencji wywołującej lokalną zaufaną ścieżkę i może być definiowana w ramach komendy **telnet**.

Dostęp do wykonywania zdalnych komend

Użytkownicy na hostach wymienionych w pliku `/etc/hosts.equiv` mogą uruchamiać we własnym systemie niektóre komendy bez podawania hasła.

W poniższej tabeli podano informacje dotyczące wyświetlania, dodawania i usuwania zdalnych hostów za pomocą interfejsu SMIT lub interfejsu wiersza komend.

Tabela 14. Zadania dostępu umożliwiające wykonywanie zdalnych komend.

Zadanie	Krótka ścieżka SMIT	Komenda lub plik
Wyświetlenie zdalnych hostów, które mają dostęp do wykonywania komend	**smit lshostsequiv**	przejrzyj plik `/etc/hosts.equiv`
Dodanie zdalnego hosta do dostępu do wykonywania komend	**smit mkhostsequiv**	zmodyfikuj plik `/etc/hosts.equiv`[Uwaga]
Usunięcie zdalnego hosta z dostępu do wykonywania komend	**smit rmhostsequiv**	zmodyfikuj plik `/etc/hosts.equiv`[Uwaga]

Uwaga: Więcej informacji na temat tych procedur zawiera sekcja "hosts.equiv File Format for TCP/IP" w podręczniku *Files Reference*.

Użytkownicy z ograniczonym dostępem do programu FTP

Użytkownicy wymienieni w pliku `/etc/ftpusers` nie mają zdalnego dostępu do FTP. Przyjmijmy na przykład, że użytkownik A jest zalogowany w systemie zdalnym i zna hasło użytkownika B w używanym systemie. Jeśli użytkownik B jest wymieniony w pliku `/etc/ftpusers`, użytkownik A nie może za pomocą programu FTP przesłać plików na lub z konta użytkownika B, nawet jeśli użytkownik A zna hasło użytkownika B.

W poniższej tabeli podano informacje dotyczące wyświetlania, dodawania i usuwania użytkowników z ograniczonym dostępem za pomocą programu SMIT lub wiersza komend.

Zadania dotyczące zdalnego użytkownika FTP		
Zadanie	**Krótka ścieżka SMIT**	**Komenda lub plik**
Wyświetlenie użytkowników z ograniczonym dostępem do programu FTP	**smit lsftpusers**	Przejrzyj plik `/etc/ftpusers`
Dodanie użytkownika z ograniczonym dostępem	**smit mkftpusers**	Zmodyfikuj plik `/etc/ftpusers`
Usunięcie użytkownika z ograniczonym dostępem	**smit rmftpusers**	Zmodyfikuj plik `/etc/ftpusers`

Zaufane procesy

Zaufany program lub zaufany proces jest skryptem powłoki, demonem lub programem spełniającym określony standard bezpieczeństwa. Te standardy bezpieczeństwa są ustanawiane i konserwowane przez Departament Obrony Stanów Zjednoczonych, który ponadto certyfikuje niektóre zaufane programy.

Programy zaufane mogą być zaufane na różnych poziomach. Istnieją następujące poziomy bezpieczeństwa: A1, B1, B2, B3, C1, C2 i D, przy czym poziom A1 zapewnia najwyższy poziom bezpieczeństwa. Każdy poziom bezpieczeństwa musi spełniać określone wymagania. Na przykład poziom bezpieczeństwa C2 obejmuje następujące standardy:

integralność programu
Proces wykonuje dokładnie to, co było zamierzone.

modułowość
Kod źródłowy procesu jest podzielony na moduły, na które nie mogą bezpośrednio wpływać i do których nie mogą bezpośrednio uzyskiwać dostępu inne moduły.

zasada najmniejszych uprawnień
Przez cały czas użytkownik pracuje na najniższym poziomie uprawnień. Oznacza to, że jeśli użytkownik ma dostęp tylko do przeglądania danego pliku, to nie ma on dostępu do zmiany tego pliku.

ograniczenie ponownego wykorzystania obiektów
Uniemożliwia użytkownikowi na przykład przypadkowe znalezienie sekcji pamięci, oznaczonej jako przeznaczona do nadpisania, która nie została jeszcze wyzerowana i która może zawierać newralgiczne dane.

TCP/IP zawiera niewiele demonów zaufanych i wiele demonów niezaufanych.

Do demonów zaufanych należą:

- **ftpd**
- **rexecd**
- **telnetd**

Do demonów niezaufanych należą:

- **rshd**
- **rlogind**
- **tftpd**

Aby system był zaufany, musi on działać z bazą TCB, czyli w przypadku pojedynczego hosta komputer musi być bezpieczny. W przypadku sieci, wszystkie serwery plików, bramy i inne hosty muszą być bezpieczne.

Sieciowa Zaufana Baza Przetwarzania (NTCB)

Baza NTCB składa się ze sprzętu i oprogramowania zapewniającego bezpieczeństwo sieci. W tej sekcji zdefiniowano komponenty bazy NTCB w powiązaniu z protokołem TCP/IP.

Sprzętowe opcje bezpieczeństwa sieci są udostępniane za pomocą adapterów sieciowych używanych z protokołem TCP/IP. Adaptery te sterują przychodzącymi danymi przez odbiór tylko tych danych, które są przeznaczone dla systemu lokalnego i danych rozgłaszania odbieranych przez wszystkie systemy.

Komponent programowy bazy NTCB składa się tylko z tych programów, które uważa się za zaufane. Programy i powiązane z nimi pliki, które nie są częścią bezpiecznego systemu, są wymienione w poniższych tabelach. Poszczególne tabele dotyczą różnych katalogów.

Katalog /etc				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
gated.conf	root	system	0664	rw-rw-r—
gateways	root	system	0664	rw-rw-r—
hosts	root	system	0664	rw-rw-r—

Katalog /etc *(kontynuacja)*				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
hosts.equiv	root	system	0664	rw-rw-r—
inetd.conf	root	system	0644	rw-r—r—
named.conf	root	system	0644	rw-r—r—
named.data	root	system	0664	rw-rw-r—
networks	root	system	0664	rw-rw-r—
protocols	root	system	0644	rw-r—r—
rc.tcpip	root	system	0774	rwxrwxr—
resolv.conf	root	system	0644	rw-rw-r—
services	root	system	0644	rw-r—r—
3270.keys	root	system	0664	rw-rw-r—
3270keys.rt	root	system	0664	rw-rw-r—

Katalog /usr/bin				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
host	root	system	4555	r-sr-xr-x
hostid	bin	bin	0555	r-xr-xr-x
hostname	bin	bin	0555	r-xr-xr-x
finger	root	system	0755	rwxr-xr-x
ftp	root	system	4555	r-sr-xr-x
netstat	root	bin	4555	r-sr-xr-x
rexec	root	bin	4555	r-sr-xr-x
ruptime	root	system	4555	r-sr-xr-x
rwho	root	system	4555	r-sr-xr-x
talk	bin	bin	0555	r-xr-xr-x
telnet	root	system	4555	r-sr-xr-x

Katalog /usr/sbin				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
arp	root	system	4555	r-sr-xr-x
fingerd	root	system	0554	r-xr-xr—
ftpd	root	system	4554	r-sr-xr—
gated	root	system	4554	r-sr-xr—
ifconfig	bin	bin	0555	r-xr-xr-x
inetd	root	system	4554	r-sr-xr—
named	root	system	4554	r-sr-x—

Katalog /usr/sbin *(kontynuacja)*				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
ping	root	system	4555	r-sr-xr-x
rexecd	root	system	4554	r-sr-xr—
route	root	system	4554	r-sr-xr—
routed	root	system	0554	r-xr-x—-
rwhod	root	system	4554	r-sr-xr—
securetcpip	root	system	0554	r-xr-xr—
setclock	root	system	4555	r-sr-xr-x
syslogd	root	system	0554	r-xr-xr—
talkd	root	system	4554	r-sr-xr—
telnetd	root	system	4554	r-sr-xr—

Katalog /usr/ucb				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
tn	root	system	4555	r-sr-xr-x

Katalog /var/spool/rwho				
Nazwa	**Właściciel**	**Grupa**	**Tryb**	**Uprawnienia**
rwho (katalog)	root	system	0755	drwxr-xr-x

Bezpieczeństwo danych i bezpieczeństwo informacji
Opcja zabezpieczająca protokołu TCP/IP nie szyfruje danych użytkowników przesyłanych przez sieć.

Należy określić ryzyko występujące podczas komunikacji, w wyniku którego hasła i inne newralgiczne informacje mogą zostać ujawnione i w oparciu o ocenę tego ryzyka zastosować odpowiednie środki zaradcze.

Użycie opcji zabezpieczającej protokołu TCP/IP w środowisku Departamentu Obrony może wymagać zastosowania się do standardów DOD 5200.5 i NCSD-11 w celu zapewnienia bezpieczeństwa komunikacji.

Oparta o użytkowników kontrola dostępu do portów TCP z indywidualną kontrolą dostępu do portów internetowych
W celu zapewnienia komunikacji między hostami AIX indywidualna kontrola dostępu do portów internetowych (DACinet) wykorzystuje opartą na użytkownikach kontrolę dostępu do portów TCP.

System AIX może używać dodatkowego nagłówka TCP do przesyłania między systemami informacji o użytkownikach i grupach. Opcja DACinet umożliwia administratorowi w systemie docelowym kontrolę dostępu w oparciu o port docelowy, identyfikator użytkownika inicjującego połączenie i host.

Ponadto opcja DACinet umożliwia administratorowi ograniczenie dostępu do lokalnych portów i przeznaczenie ich do wykorzystania tylko przez użytkownika root. Systemy typu UNIX, takie jak AIX, traktują porty poniżej portu 1024 jako porty uprzywilejowane, które mogą być otwierane tylko przez użytkownika root. System AIX umożliwia podanie dodatkowych portów powyżej portu 1024, które mogą być otwierane tylko przez użytkownika root, co uniemożliwia użytkownikom pracę z serwerami na powszechnie znanych portach.

W zależności od ustawień system inny niż DACinet jest lub nie jest w stanie połączyć się z systemem DACinet. Odmowę dostępu można ustawić w początkowym stanie opcji DACinet. Po włączeniu opcji DACinet jej wyłączenie jest niemożliwe.

Komenda **dacinet** akceptuje adresy, które są podane jako nazwy hostów, adresy hostów w postaci dziesiętnej z kropkami i adresy sieciowe, po których podana jest długość przedrostka sieciowego.

Poniższy przykład pokazuje pojedynczy host o znanej pełnej nazwie: *host.domena.org*:

```
    host.domena.org
```

Poniższy przykład pokazuje pojedynczy host znany z adresu IP 10.0.0.1:

```
    10.0.0.1
```

Poniższy przykład przedstawia całą sieć, której pierwsze 24 bity (długość przedrostka sieciowego) zawierają wartość 10.0.0.0:

```
    10.0.0.0/24
```

Ta sieć zawiera wszystkie adresy IP między 10.0.0.1 a 10.0.0.254.

Kontrola dostępu dla usług opartych na protokole TCP
Opcja DACinet używa pliku uruchamiania `/etc/rc.dacinet` i plików konfiguracyjnych `/etc/security/priv`, `/etc/security/services` i `/etc/security/acl`.

Porty wymienione w pliku `/etc/security/services` są zwalniane ze sprawdzeń list ACL. Plik ten ma taki sam format, jak plik `/etc/services`. Najprostszym sposobem jego zainicjowania jest skopiowanie pliku z katalogu `/etc` do katalogu `/etc/security`, a następnie usunięcie wszystkich potów, dla których powinny być zastosowane listy ACL. Listy ACL są przechowywane w dwóch miejscach. Aktywne listy ACL są przechowywane w jądrze i można je odczytać za pomocą komendy `dacinet aclls`. Listy ACL, które będą reaktywowane podczas następnego startu systemu przez `/etc/rc.tcpip`, są przechowywane w katalogu `/etc/security/acl`. Używany jest format:

```
service host/prefix-length [user|group]
```

Usługę można podać w postaci numerycznej lub w sposób podany w pliku `/etc/services`, host może być nazwą hosta lub adresem sieciowym z podaną maską podsieci, a nazwę użytkownika lub grupę podaje się z przedrostkiem u: lub g:. Jeśli nie zostanie podany żaden użytkownik lub grupa, lista ACL bierze pod uwagę tylko wysyłający host. Poprzedzenie usługi przedrostkiem - powoduje jawne wyłączenie dostępu. Listy ACL są oceniane zgodnie z pierwszym dopasowaniem. Można więc określić dostęp dla grupy użytkowników, ale jednocześnie jawnie odmówić dostępu użytkownikowi należącemu do tej grupy, umieszczając regułę dotyczącą tego użytkownika przed regułą dotyczącą grupy.

Plik `/etc/services` zawiera dwie pozycje z numerami, które nie są obsługiwane w systemie AIX. Administrator systemu musi usunąć oba wiersze tego pliku przed wykonaniem komendy **mkCCadmin**. Z pliku `/etc/services` należy usunąć wiersze:

```
sco_printer     70000/tcp     sco_spooler    # For System V print IPC
sco_s5_port     70001/tcp     lpNet_s5_port  # For future use
```

Przykłady użycia opcji DACinet
Przykładowo używając opcji DACinet w celu ograniczenia dostępu do portu przychodzącego TCP/25 tylko do użytkownika root z opcją DACinet, tylko użytkownicy root z innych hostów AIX mogą uzyskać dostęp do tego portu, ograniczając w ten sposób możliwości zwykłych użytkowników fałszowania poczty elektronicznej, przesyłając ją za pomocą usługi Telnet do portu TCP/25.

Poniższy przykład ilustruje sposób konfigurowania protokołu X (X11) dla dostępu tylko przez użytkowników root. Należy upewnić się, że pozycja X11 została usunięta z pliku `/etc/security/services`, co umożliwi zastosowanie listy ACL dla tej usługi.

Przyjmując, że podmaska 10.1.1.0/24 dotyczy wszystkich podłączonych systemów, pozycje listy ACL ograniczające dostęp tylko dla użytkowników root dla X (TCP/6000) w pliku `/etc/security/acl` będą miały postać:

```
      6000    10.1.1.0/24 u:root
```

Podczas ograniczania usługi Telnet do użytkowników w grupie friends, bez względu na to, z którego systemu pochodzą, po usunięciu pozycji telnet z pliku `/etc/security/services` należy użyć następującej pozycji ACL:

```
telnet    0.0.0.0/0   g:friends
```

Aby uniemożliwić użytkownikowi fred dostęp do serwera WWW, ale zezwolić na ten dostęp pozostałym użytkownikom, należy podać:

```
-80    0.0.0.0/0 u:fred
80     0.0.0.0/0
```

Uprzywilejowane porty dla uruchomionych usług lokalnych
Aby uniemożliwić zwykłym użytkownikom uruchamianie serwerów na konkretnych portach, porty te można oznaczyć jako porty uprzywilejowane.

Zwykle każdy użytkownik może otworzyć dowolny port powyżej 1024. Przykładowo użytkownik może umieścić serwer w porcie 8080, który jest często używany do uruchamiania serwerów proxy WWW lub w porcie 1080, gdzie zwykle znajduje się serwer SOCKS. W celu uprzywilejowania portów w uruchomionym systemie można użyć komendy **`dacinet setpriv`**. Porty, które podczas uruchamiania systemu mają zostać oznaczone jako uprzywilejowane, należy podać w pliku `/etc/security/priv`.

Porty te można podać za pomocą nazw symbolicznych zgodnie z ich definicją w pliku `/etc/services` lub podając numery portów. Poniższe pozycje uniemożliwią użytkownikom innym niż root uruchamianie serwerów SOCKS lub serwerów Lotus Notes z ich najczęściej używanych portów:

```
1080
lotusnote
```

Uwaga: Ta opcja nie uniemożliwia użytkownikowi (user) uruchamiania programów. Uniemożliwia ona tylko użytkownikowi uruchomienie usług w dobrze znanych portach, w których zazwyczaj można się ich spodziewać.

Usługi sieciowe

Informacje na temat identyfikowania i zabezpieczania usług sieciowych z otwartymi portami komunikacyjnymi.

Wykorzystanie portów

Poniższa tabela zawiera omówienie wykorzystania znanych portów w systemie operacyjnym AIX.

Uwaga: Listę zbudowano na podstawie wyników przeglądu pewnej liczby systemów AIX o różnych konfiguracjach zainstalowanego oprogramowania.

Poniższa lista może nie zawierać informacji o wykorzystaniu portów przez całe oprogramowanie występujące w systemie operacyjnym AIX:

Port/Protokół	Nazwa usługi	Aliasy
13/tcp	daytime	Daytime (RFC 867)
13/udp	daytime	Daytime (RFC 867)
21/tcp	ftp	File Transfer [Control]
21/udp	ftp	File Transfer [Control]
23/udp	telnet	Telnet

Port/Protokół	Nazwa usługi	Aliasy
23/udp	telnet	Telnet
25/tcp	smtp	Simple Mail Transfer
25/udp	smtp	Simple Mail Transfer
37/tcp	time	Time
37/udp	time	Time
111/tcp	sunrpc	SUN Remote Procedure Call
111/udp	sunrpc	SUN Remote Procedure Call
161/tcp	snmp	SNMP
161/udp	snmp	SNMP
199/tcp	smux	SMUX
199/udp	smux	SMUX
512/tcp	exec	zdalne wykonywanie procesów
513/tcp	login	zdalne logowanie przy użyciu usługi telnet
514/tcp	shell	cmd
514/udp	syslog	Syslog
518/tcp	ntalk	Talk
518/udp	ntalk	Talk
657/tcp	rmc	RMC
657/udp	rmc	RMC
1334/tcp	writesrv	writesrv
1334/udp	writesrv	writesrv
2279/tcp	xmquery	xmquery
2279/udp	xmquery	xmquery
32768/tcp	filenet-tms	FileNet TMS
32768/udp	filenet-tms	FileNet TMS
32769/tcp	filenet-rpc	FileNet RPC
32769/udp	filenet-rpc	FileNet RPC
32770/tcp	filenet-nch	FileNet NCH
32770/udp	filenet-nch	FileNet NCH
32771/tcp	filenet-rmi	FileNet RMI
32771/udp	filenet-rmi	FileNet RMI
32772/tcp	filenet-pa	FileNet Process Analyzer
32772/udp	filenet-pa	FileNet Process Analyzer
32773/tcp	filenet-cm	FileNet Component Manager
32773/udp	filenet-cm	FileNet Component Manager

Port/Protokół	Nazwa usługi	Aliasy
32774/tcp	filenet-re	FileNet Rules Engine
32774/udp	filenet-re	FileNet Rules Engine
32775/tcp	filenet-pch	Performance Clearinghouse
32775/udp	filenet-pch	Performance Clearinghouse
32776/tcp	filenet-peior	FileNet BPM IOR
32776/udp	filenet-peior	FileNet BPM IOR
32777/tcp	filenet-obrok	FileNet BPM CORBA
32777/udp	filenet-obrok	FileNet BPM CORBA

Identyfikowanie usług sieciowych z otwartymi portami komunikacyjnymi
Aplikacje klient/serwer otwierają porty komunikacyjne na serwerze, umożliwiając aplikacjom nasłuchiwanie przychodzących żądań klientów.

Ponieważ otwarte porty są wrażliwe na ewentualne ataki na bezpieczeństwo, należy zidentyfikować, które aplikacje mają otwarte porty i zamknąć te, które są niepotrzebnie otwarte. Praktyka ta jest przydatna, ponieważ pozwala zrozumieć, w jaki sposób systemy są dostępne dla każdego, kto dysponuje dostępem do Internetu.

Aby określić, które porty są otwarte, wykonaj następujące czynności:

1. Zidentyfikuj usługi za pomocą komendy **netstat**:

   ```
   # netstat -af inet
   ```

   Poniżej został przedstawiony przykład danych wyjściowych tej komendy. Ostatnia kolumna danych wyjściowych komendy **netstat** wskazuje stan danej usługi. Usługi oczekujące na przychodzące żądania są w stanie LISTEN.

   W tym miejscu przedstawiono przykład wyjścia komendy po uruchomieniu komendy **netstat**.

Aktywne połączenie internetowe (w tym serwery)

Proto	Recv-Q	Send-Q	Adres lokalny	Adres obcy	Stan
tcp4	0	0	*.echo	*.*	LISTEN
tcp4	0	0	*.discard	*.*	LISTEN
tcp4	0	0	*.daytime	*.*	LISTEN
tcp	0	0	*.chargen	*.*	LISTEN
tcp	0	0	*.ftp	*.*	LISTEN
tcp4	0	0	*.telnet	*.*	LISTEN

W tym miejscu przedstawiono przykład wyjścia komendy po uruchomieniu komendy **netstat**. *(kontynuacja)*

Aktywne połączenie internetowe (w tym serwery)

Proto	Recv-Q	Send-Q	Adres lokalny	Adres obcy	Stan
tcp4	0	0	*.smtp	*.*	LISTEN
tcp4	0	0	*.time	*.*	LISTEN
tcp4	0	0	*.www	*.*	LISTEN
tcp4	0	0	*.sunrpc	*.*	LISTEN
tcp	0	0	*.smux	*.*	LISTEN
tcp	0	0	*.exec	*.*	LISTEN
tcp	0	0	*.login	*.*	LISTEN
tcp4	0	0	*.shell	*.*	LISTEN
tcp4	0	0	*.klogin	*.*	LISTEN
udp4	0	0	*.kshell	*.*	LISTEN
udp4	0	0	*.echo	*.*	
udp4	0	0	*.discard	*.*	
udp4	0	0	*.daytime	*.*	
udp4	0	0	*.chargen	*.*	
udp4	0	0	*.time	*.*	
udp4	0	0	*.bootpc	*.*	

W tym miejscu przedstawiono przykład wyjścia komendy po uruchomieniu komendy **netstat**. *(kontynuacja)*

Aktywne połączenie internetowe (w tym serwery)

Proto	Recv-Q	Send-Q	Adres lokalny	Adres obcy	Stan
udp4	0	0	*.sunrpc	*.*	
udp4	0	0	255.255.255.255.ntp	*.*	
udp4	0	0	1.23.123.234.ntp	*.*	
udp4	0	0	localhost.domain.ntp	*.*	
udp4	0	0	name.domain..ntp	*.*	

.....

2. Otwórz plik `/etc/services` i sprawdź usługi IANA (Internet Assigned Numbers Authority), aby odwzorować usługę na numery portów w systemie operacyjnym.

   Poniżej przedstawiono przykładowy fragment pliku `/etc/services`:

```
tcpmux  1/tcp  # TCP Port Service Multiplexer
tcpmux  1/tcp  # TCP Port Service Multiplexer
Compressnet  2/tcp  # Management Utility
Compressnet  2/udp  # Management Utility
Compressnet  3/tcp  # Compression Process
Compressnet  3/udp  Compression Process
Echo  7/tcp
Echo  7/udp
discard  9/tcp  sink null
discard  9/udp  sink null
..............
rfe  5002/tcp  # Radio Free Ethernet
rfe  5002/udp  # Radio Free Ethernet
rmonitor_secure  5145/tcp
rmonitor_secure  5145/udp
pad12sim  5236/tcp
pad12sim  5236/udp
sub-process  6111/tcp  # HP SoftBench Sub-Process Cntl.
sub-process  6111/udp  # HP SoftBench Sub-Process Cntl.
xdsxdm  6558/ucp
xdsxdm  6558/tcp
afs3-fileserver  7000/tcp  # File Server Itself
afs3-fileserver  7000/udp  # File Server Itself
af3-callback  7001/tcp  # Callbacks to Cache Managers
af3-callback  7001/udp  # Callbacks to Cache Managers
```

3. Zamknij niepotrzebne porty, usuwając uruchomione usługi.

Uwaga: Port 657 jest używany przez program RMC (Resource Monitoring and Control)do komunikacji pomiędzy węzłami. Nie można zablokować ani nałożyć ograniczeń na ten port.

Identyfikowanie gniazd TCP i UDP

Należy użyć komendy **lsof**, która jest odmianą komendy **netstat -af**, aby zidentyfikować gniazda TCP, które są w stanie LISTEN i bezczynne gniazda UDP, które oczekują na dostarczenie danych.

Na przykład, aby wyświetlić gniazda TCP w stanie LISTEN i gniazda UDP w stanie IDLE, należy uruchomić komendę **lsof**:

```
# lsof -i | egrep "COMMAND|LISTEN|UDP"
```

Wygenerowane dane wyjściowe są podobne do następujących:

Komenda	PID	Użytk.	FD	Typ	Urządz.	Wielk/OFF	Węzeł	Nazwa
dtlogin	2122	root	5u	IPv4	0x70053c00	0t0	UDP	*:xdmcp
dtlogin	2122	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
syslogd	2730	root	4u	IPv4	0x70053600	0t0	UDP	*:syslog
X	2880	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
X	2880	root	8u	IPv4	0x700546dc	0t0	TCP	*:6000(LISTEN)
dtlogin	3882	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)
glbd	4154	root	4u	IPv4	0x7003f300	0t0	UDP	*:32803
glbd	4154	root	9u	IPv4	0x7003f700	0t0	UDP	*:32805
dtgreet	4656	root	6u	IPv4	0x70054adc	0t0	TCP	*:32768(LISTEN)

Po określeniu identyfikatora procesu można uzyskać więcej informacji na temat danego programu, uruchamiając komendę:

```
# ps -fp numer_identyfikatora_PID
```

Dane wyjściowe tej komendy zawierają ścieżkę do komendy, której można użyć, aby wyświetlić pomoc dla tego programu.

Bezpieczeństwo protokołu IP (Internet Protocol)

Bezpieczeństwo IP, przez zabezpieczenie komunikacji danych na poziomie warstwy IP, umożliwia nawiązywanie bezpiecznych połączeń przez Internet oraz wewnątrz sieci przedsiębiorstwa.

Przegląd bezpieczeństwa IP

Bezpieczeństwo IP pozwala indywidualnym użytkownikom lub organizacjom chronić komunikację dla wszystkich aplikacji bez konieczności ich modyfikowania. A zatem transmisja danych, takich jak wiadomości e-mail lub dane przedsiębiorstwa specyficznych aplikacji, może być chroniona.

Bezpieczeństwo IP a system operacyjny

System operacyjny korzysta z bezpieczeństwa IP (IPsec), które jest otwartą, standardową technologią bezpieczeństwa opracowaną przez grupę wykonawczą IETF (Internet Engineering Task Force).

Bezpieczeństwo IP udostępnia zabezpieczenie wszystkich danych oparte na szyfrowaniu, w warstwie IP stosu komunikacyjnego. Nie wymaga wprowadzania zmian w istniejących aplikacjach. Bezpieczeństwo IP jest strukturą zabezpieczeń sieci standardu przemysłowego wybraną przez grupę IETF dla środowisk IP w wersji 4 i 6.

Bezpieczeństwo IP zabezpiecza komunikację danych przez wykorzystanie następujących technik szyfrujących:

Uwierzytelnianie
Proces, podczas którego sprawdzana jest tożsamość hosta lub punktu końcowego.

Sprawdzanie integralności
Proces zapewniający, że podczas przesyłania danych przez sieć nie dojdzie do ich modyfikacji.

Szyfrowanie
Proces zapewniający prywatność przez "ukrycie" danych oraz prywatnych adresów IP podczas przesyłania danych przez sieć.

Algorytmy uwierzytelniania sprawdzają tożsamość wysyłającego oraz integralność danych, używając szyfrującej funkcji mieszającej, w celu przetworzenia pakietu danych (z dołączonymi polami nagłówka stałego adresu IP), korzystając z tajnego klucza do utworzenia unikalnego streszczenia. Po stronie odbiorcy dane są przetwarzane za pomocą tej samej funkcji i klucza. Jeśli dane zostały zmienione lub klucz wysyłającego nie jest poprawny, datagram jest usuwany.

Szyfrowanie korzysta z algorytmu szyfrowania w celu zmodyfikowania i losowego dobrania danych, używając pewnego algorytmu i klucza do utworzenia zaszyfrowanych danych zwanych *cyphertext (tekstem zaszyfrowanym)*. Szyfrowanie powoduje, że danych podczas przesyłania nie da się odczytać. Po otrzymaniu danych są one odtwarzane za pomocą tego samego algorytmu i klucza (z symetrycznymi algorytmami szyfrowania). Przy szyfrowaniu wymagane jest uwierzytelnianie, w celu sprawdzenia integralności zaszyfrowanych danych.

Te podstawowe usługi są zaimplementowane w bezpieczeństwie IP za pomocą protokołów ESP (Encapsulating Security Payload) i AH (Authentication Header). Protokół ESP zapewnia poufność przez szyfrowanie oryginalnego pakietu IP, budowanie nagłówka ESP i umieszczanie zaszyfrowanego tekstu w ładunku ESP.

Protokół AH może być wykorzystany oddzielnie do uwierzytelniania i sprawdzania integralności, jeśli poufność nie jest konieczna. Przy korzystaniu z protokołu AH, dla pól statycznych nagłówka IP oraz danych stosowany jest algorytm mieszający, w celu utworzenia streszczenia zabezpieczonego kluczem. Odbiorca korzysta ze swojego klucza do obliczenia i porównania streszczenia, aby upewnić się, że pakiet nie został zmieniony i aby potwierdzić tożsamość nadawcy.

Opcje bezpieczeństwa IP
Bezpieczeństwo IP obejmuje następujące opcje:

Protokół IKE dla systemu operacyjnego AIX udostępnia następujące opcje:

- obsługa 128-bitowych, 192-bitowych i 256-bitowych algorytmów AES,
- przyspieszenie sprzętu za pomocą adaptera 10/100 Mbps Ethernet PCI Adapter II,
- obsługa protokołu AH przez zastosowanie RFC 2402 i protokołu ESP przez zastosowanie RFC 2406,
- możliwość konfigurowania tuneli ręcznych w celu zapewnienia współdziałania z innymi systemami, które nie obsługują metody automatycznego odświeżania klucza IKE oraz w celu korzystania z tuneli protokołu IP w wersji 6,
- hermetyzowanie trybu tunelu oraz trybu transportu dla tuneli hosta lub bramy,
- algorytmy uwierzytelniania HMAC (Hashed Message Authentication Code - Kod uwierzytelniania komunikatu mieszającego), MD5 (Message Digest 5 - Streszczenie komunikatu) i HMAC SHA (Secure Hash Algorithm - Bezpieczny algorytm mieszający),
- do algorytmów szyfrujących należą: 56-bitowy algorytm szyfrowania DES (Data Encryption Standard) CBC (Cipher Block Chaining) z 64-bitowym wektorem początkowym (initial vector - IV), potrójny algorytm DES, algorytm DES CBC 4 (32-bitowy wektor początkowy) i algorytm AES CBC,
- podwójna obsługa stosu IP (protokoły IP w wersji 4 i 6),

- dane przesyłane przy użyciu protokołu IP w wersji 4 i 6 mogą być hermetyzowane i filtrowane; ponieważ stosy IP są odrębne, funkcja bezpieczeństwa IP dla każdego stosu może być konfigurowana niezależnie,
- filtrowanie komunikacji zabezpieczonej i niezabezpieczonej przez różne charakterystyki protokołu IP, takie jak adresy IP źródła i miejsca docelowego, interfejs, protokół, numery portów i inne,
- automatyczne tworzenie i usuwanie reguł filtrowania dla większości typów tuneli,
- użycie nazw hostów dla adresów miejsc docelowych podczas definiowania tuneli i reguł filtrowania; nazwy hostów są automatycznie przekształcane na adresy IP (gdy dostępny jest serwer DNS),
- zapisywanie zdarzeń bezpieczeństwa IP w dzienniku **syslog**,
- użycie śledzenia systemu oraz statystyk w celu określenia problemu,
- działanie domyślne zdefiniowane przez użytkownika pozwalające na określenie, czy komunikacja, która nie jest zgodna ze zdefiniowanymi tunelami, jest dozwolona.

Protokół IKE dla systemu AIX 6.1 TL 05 lub nowszych wersji udostępnia następujące opcje dodatkowe:

- obsługa IPSec przez zastosowanie RFC 4301, obsługa AH przez zastosowanie RFC 4302 i obsługa ESP przez zastosowanie RFC 4303,
- algorytmy uwierzytelniania Cipher-based Message Authentication Code (CMAC) AES XCBC,
- algorytmy szyfrowania AES 128-bitowe, 192-bitowe, 256-bitowe GCM (16-bitowy IV), AES-128-GMAC, AES-192-GMAC i AES-256-GMAC,
- obsługa zakresu portów dla reguł filtrowania,
- numery ESN (Extended Sequence Number).

Opcje protokołu Internet Key Exchange
Protokół IKE dla systemu AIX udostępnia następujące opcje:

Protokół IKE dla systemu AIX 6.1 lub nowszych wersji udostępnia następujące opcje dodatkowe:

- obsługę AH dla HMAC SHA2 256-bitowy (TL 04 lub w nowszej wersji),
- obsługę szyfrowania ESP GCM AES 128-bitowy, 192-bitowy, 256-bitowy z (16-bitowy IV), algorytmy GMAC AES 128-bitowy, 192-bitowy, 256-bitowy; obsługę uwierzytelniania ESP z HMAC MD5 i HMAC SHA1 (TL 04 lub w nowszej wersji),
- obsługiwane są IKEv1 (RFC2409) i IKEv2 (RFC4306) (TL 02 lub w nowszej wersji); IKEv1 jest obsługiwany przez demon **isakmpd**, a IKEv2 jest obsługiwany przez demon **ikev2d** (TL 02 lub w nowszej wersji); tunele IKEv1 i IKEv2 mogą współistnieć,
- obsługę algorytmów integralności CMAC_AES_XCBC i HMAC_SHA2_256 (TL 04 lub w nowszej wersji),
- obsługę algorytmu PRF PRF_SHA2_256 (TL 04 lub w nowszej wersji),
- obsługę grup 14, 19 i 24 Diffie Hellman (TL 04 lub w nowszej wersji).

Powiązania bezpieczeństwa
Budowanie bloków, na których opiera się chroniona komunikacja, jest pojęciem znanym jako *powiązanie bezpieczeństwa*. Powiązania bezpieczeństwa łączą określony zestaw parametrów bezpieczeństwa z rodzajem ruchu danych.

Razem z zabezpieczeniem danych przez bezpieczeństwo IP, dla każdego kierunku, każdego rodzaju nagłówka, protokołu AH lub ESP istnieje oddzielne powiązanie bezpieczeństwa. Informacje zawarte w powiązaniu bezpieczeństwa obejmują adresy IP stron komunikujących się, unikalny identyfikator znany jako interfejs SPI (Security Parameters Index), algorytmy wybrane do uwierzytelniania lub szyfrowania, klucze uwierzytelniające i szyfrujące oraz czas życia klucza. Poniższy rysunek przedstawia powiązania bezpieczeństwa pomiędzy hostem A i hostem B.

Rysunek 6. Ustanowienie chronionego tunelu między hostami A i B

Na ilustracji przedstawiono tunel wirtualny biegnący między hostem A i hostem B. Powiązanie bezpieczeństwa A jest przedstawione w postaci strzałki skierowanej od hosta A do hosta B. Powiązanie bezpieczeństwa B jest przedstawione w postaci strzałki skierowanej od hosta B do hosta A. Powiązanie bezpieczeństwa składa się z adresu docelowego, interfejsu SPI, klucza, algorytmu i formatu szyfrowania, algorytmu uwierzytelniania oraz czasu ważności klucza.

Celem zarządzania kluczami jest wynegocjowanie i obliczenie powiązań bezpieczeństwa, które chronią ruch danych IP.

Tunele i zarządzanie kluczem
Tunel służy do negocjowania powiązań bezpieczeństwa, które są wymagane do skonfigurowania bezpiecznej konfiguracji między dwoma hostami, oraz do zarządzania tymi powiązaniami.

Obsługiwane są następujące rodzaje tuneli, z których każdy korzysta z innej techniki zarządzania kluczami:

- tunele IKE (z dynamicznie zmieniającymi się kluczami, standard grupy IETF),
- tunele ręczne (ze statycznymi, trwałymi kluczami, standard grupy IETF).

Obsługa tunelu IKE (Internet Key Exchange)
Tunele IKE są oparte na standardach Internet Security Association and Key Management Protocol(ISAKMP)/Oakley opracowanych przez grupę IETF. Przy użyciu tego protokołu parametry bezpieczeństwa są negocjowane i odświeżane, a klucze wymieniane w bezpieczny sposób.

Obsługiwane są następujące typy uwierzytelniania:

- Wstępny klucz wspólny.
- Podpisy certyfikatu cyfrowego X.509v3.
- W systemie AIX 6.1 TL 04 lub w nowszej jego wersji IKEv2 obsługuje podpisy certyfikatu cyfrowego ECDSA-256 w ramach metody uwierzytelniania X509v3 opartej na certyfikatach cyfrowych.

Negocjacja korzysta z dostępu dwufazowego. Pierwsza faza uwierzytelnia komunikujące się strony i określa algorytmy, które mają być użyte do chronionej komunikacji w fazie drugiej. Podczas fazy drugiej negocjowane są parametry bezpieczeństwa IP, które będą używane podczas przesyłania danych oraz są tworzone i wymieniane powiązania bezpieczeństwa i klucze.

W poniższej tabeli przedstawione zostały algorytmy uwierzytelniające, które mogą być wykorzystane przez protokoły bezpieczeństwa AH i ESP do obsługi tunelu IKE.

Tabela 15. Algorytm uwierzytelniania do obsługi tunelu IKE		
Algorytm	**Protokół AH protokołu IP w wersji 4 i 6**	**Protokół ESP protokołu IP w wersji 4 i 6**
Kod HMAC MD5	X	X
Kod HMAC SHA1	X	X
Algorytm szyfrowania DES CBC 8		X
Potrójny algorytm DES CBC		X
Algorytm AES CBC (128, 192, 256)		X
Protokół ESP Null		X
AES-XCBC-MAC-96	X	X
AES GCM (128, 192, 256)		X
AES GMAC (128, 192, 256)	X	
ESP_ENCR_NULL_ AUTH_AES_GMAC		X

Obsługa tunelu ręcznego
Tunele ręczne są zgodne z wcześniejszymi wersjami i współdziałają z komputerami, które nie obsługują protokołów IKE do zarządzania kluczami. Wadą tuneli ręcznych jest to, że wartości klucza są statyczne. Klucze szyfrujące i uwierzytelniające są takie same przez cały czas trwania tunelu i muszą być aktualizowane ręcznie.

W poniższej tabeli przedstawione zostały algorytmy uwierzytelniające, które mogą być wykorzystane przez protokoły zabezpieczeń AH i ESP do obsługi tunelu ręcznego.

Algorytm	**Protokół AH protokołu IP w wersji 4**	**Protokół AH protokołu IP w wersji 6**	**Protokół ESP protokołu IP w wersji 4**	**Protokół ESP protokołu IP w wersji 6**
Kod HMAC MD5	X	X	X	X
Kod HMAC SHA1	X	X	X	X
Algorytm AES CBC (128, 192, 256)			X	X
Potrójny algorytm DES CBC			X	X
Algorytm szyfrowania DES CBC 8			X	X
Algorytm szyfrowania DES CBC 4			X	X

Ponieważ tunele IKE oferują efektywniejsze zabezpieczenie, zalecane jest korzystanie z tej metody zarządzania kluczem.

Możliwość filtrowania rodzimego

Filtrowanie jest podstawową funkcją, za pomocą której pakiety przychodzące i wychodzące mogą być akceptowane lub odrzucane w oparciu o różne charakterystyki. Pozwala to użytkownikowi lub administratorowi systemu skonfigurować hosta w celu sterowania ruchem danych między nim a innymi hostami.

Filtrowanie odbywa się na podstawie różnych właściwości pakietu, takich jak adresy miejsca źródłowego i docelowego, wersja protokołu IP (4 lub 6), maska podsieci, protokół, port, charakterystyki routingu, fragmentacja, interfejs oraz definicje tunelu.

Do powiązania pewnych rodzajów ruchu danych ze szczególnym tunelem używane są reguły, znane jako *reguły filtrowania*. W konfiguracji podstawowej dla tuneli ręcznych, kiedy użytkownik definiuje tunel między hostami, reguły filtrowania są automatycznie generowane w ten sposób, żeby ruch danych z danego hosta był kierowany przez tunel chroniony. Jeśli wymaganych jest więcej rodzajów ruchu danych (na przykład z podsieci do podsieci), można modyfikować lub zastąpić reguły filtrowania, aby pozwolić na precyzyjne sterowanie ruchem danych przy użyciu danego tunelu.

W przypadku tuneli IKE reguły filtrowania również są generowane automatycznie i wstawiane do tabeli filtrów po aktywowaniu tunelu.

Podobnie, kiedy tunel jest modyfikowany lub usuwany, reguły filtrowania dla tego tunelu są automatycznie usuwane, co upraszcza konfigurację bezpieczeństwa IP i pomaga zredukować błędy popełniane przez człowieka. Definicje tunelu mogą być rozpowszechniane i współużytkowane za pomocą narzędzi importu i eksportu wśród wielu komputerów oraz firewalli, co jest bardzo pomocne przy administrowaniu dużą liczbą komputerów.

Reguły filtrowania wiążą poszczególne typy ruchu danych z tunelem, ale filtrowane dane nie muszą koniecznie przemieszczać się w tunelu. Ten aspekt reguł filtrowania pozwala, aby system operacyjny udostępniał podstawową funkcjonalność firewalla, dla użytkowników, którzy chcą ograniczyć ruch danych do lub ze swoich komputerów w sieci intranet lub w sieci, która nie ma zabezpieczenia w postaci prawdziwego firewalla. W tym scenariuszu reguły filtrowania udostępniają drugą barierę zabezpieczenia w grupie komputerów.

Po wygenerowaniu, reguły filtrowania są przechowywane w tabeli i ładowane do jądra. Kiedy pakiety są gotowe do wysłania lub odebrania z sieci, następuje sprawdzenie listy reguł filtrowania z góry na dół, aby określić, czy pakiet powinien być przyjęty, odrzucony czy wysłany przez tunel. Kryterium reguły jest porównywane z charakterystyką pakietu, dopóki nie zostanie stwierdzona zgodność lub osiągnięta reguła domyślna.

Funkcja bezpieczeństwa IP implementuje także filtrowanie niezabezpieczonych pakietów w oparciu o bardzo szczegółowe kryteria zdefiniowane przez użytkownika, które pozwalają na sterowanie ruchem danych IP między sieciami i komputerami, które nie wymagają właściwości uwierzytelniania lub szyfrowania bezpieczeństwa IP.

Obsługa certyfikatu cyfrowego

Opcja bezpieczeństwa IP obsługuje certyfikaty cyfrowe X.509 w wersji 3.

Narzędzie Key Manager zarządza zgłoszeniami certyfikatu, obsługuje bazę danych kluczy i przeprowadza pozostałe funkcje związane z administrowaniem.

Certyfikaty cyfrowe zostały opisane w sekcji na temat konfiguracji certyfikatów cyfrowych. Narzędzie Key Manager oraz jego funkcje zostały opisane w sekcji na temat używania narzędzia IBM Key Manager

Sieci VPN (Virtual Private Network) a bezpieczeństwo IP

Sieć VPN w bezpieczny sposób rozszerza prywatną sieć intranet przez sieć publiczną, taką jak Internet.

Sieci VPN przesyłają informacje przez coś, co jest zasadniczo tunelem prywatnym w sieci Internet, do i od użytkowników zdalnych, biur oddziałów oraz partnerów w biznesie lub dostawców. Przedsiębiorstwa mogą korzystać z dostępu do Internetu przez dostawców usług internetowych (ISP), używając linii bezpośrednich lub lokalnych numerów telefonów i eliminując w ten sposób dzierżawę linii, która jest droższa, połączenia międzymiastowe oraz darmowe numery telefonów. Sieć VPN może korzystać z bezpieczeństwa IP, ponieważ jest to struktura zabezpieczeń sieci standardu przemysłowego wybrana

przez grupę IETF dla środowisk IP w wersji 4 i 6 i nie wymaga dokonywania zmian w istniejących aplikacjach.

Zalecanym źródłem informacji na temat planowania implementacji sieci VPN w systemie AIX jest Rozdział 9 podręcznika *A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management*, ISBN SG24-5309-00. Ten podręcznik dostępny jest także w sieci WWW pod adresem: http://www.redbooks.ibm.com/redbooks/SG245309.html.

Instalowanie opcji bezpieczeństwa IP
Opcja bezpieczeństwa IP w systemie AIX jest instalowana i ładowana oddzielnie.

Wymagane jest zainstalowanie następujących zestawów plików:

- `bos.net.ipsec.rte` (środowisko wykonawcze dla środowiska i komend jądra bezpieczeństwa IP),
- `bos.msg.`*`JĘZYK`*`.net.ipsec` (gdzie *JĘZYK* jest podanym językiem, na przykład en_US),
- `bos.net.ipsec.keymgt`,
- `clic.rte` (CryptoLite for C, zestaw plików dla algorytmu szyfrowania DES, potrójnego szyfrowania DES i szyfrowania AES)

W celu obsługi podpisów cyfrowych protokołu IKE należy z dysku Expansion Pack zainstalować także zestaw plików `GSKit z` pakietu Expansion Pack.

Uwaga: Podczas tworzenia nowej bazy danych plików kluczy dla obsługi cyfrowych podpisów IKE przy użyciu programu GSkit8 w wersji 8.0.50.69 lub nowszej, należy utworzyć plik ukryty przy użyciu opcji *-v1 stash*. W poniższym przykładzie przedstawiono użycie komendy **gsk8capicmd** z opcją *-v1 stash*.

```
gsk8capicmd -keydb -create -db <nazwa_bazy_kluczy> -pw <hasło_bazy_kluczy> -type cms -stash -v1
stash
```

Po zainstalowaniu zestawów zabezpieczenia IP można załadować oddzielnie dla protokołu IP w wersji 4 i 6, korzystając z zalecanej procedury opisanej w sekcji “Ładowanie opcji bezpieczeństwa IP” na stronie 232 lub przy użyciu komendy **mkdev**.

Ładowanie opcji bezpieczeństwa IP
Aby automatycznie załadować moduły podczas uruchamiania opcji bezpieczeństwa IP, należy użyć programu SMIT. Ponadto program SMIT zapewnia, że rozszerzenia jądra i demony IKE są ładowane we właściwej kolejności.

Uwaga: Ładowanie opcji bezpieczeństwa IP włącza funkcję filtrowania. Ważne jest, aby przed ładowaniem upewnić się, że utworzone zostały prawidłowe reguły filtrowania. W przeciwnym przypadku komunikacja z zewnątrz może być zablokowana.

Jeśli ładowanie zakończy się pomyślnie, komenda **lsdev** pokaże urządzenia bezpieczeństwa IP jako `Available` (dostępne).

```
lsdev -C -c ipsec

   ipsec_v4 Available IP Version 4 Security Extension
   ipsec_v6 Available IP Version 6 Security Extension
```

Po załadowaniu rozszerzenia jądra bezpieczeństwa IP, tunele i filtry są gotowe do konfigurowania.

Planowanie konfigurowania bezpieczeństwa IP
Podczas konfigurowania bezpieczeństwa IP należy najpierw zaplanować konfigurowanie tuneli i filtrów.

Po określeniu prostego tunelu dla każdego rodzaju komunikacji można automatycznie wygenerować reguły filtrowania. Jeśli wymagane jest bardziej złożone filtrowanie, jego reguły można skonfigurować oddzielnie.

Bezpieczeństwo IP można skonfigurować za pomocą wtyczki sieci VPN lub programu SMIT (System Management Interface Tool). Podczas korzystania z programu SMIT, dostępne są następujące krótkie ścieżki:

smit ips4_basic
Podstawowa konfiguracja dla protokołu IP w wersji 4.

smit ips6_basic
Podstawowa konfiguracja dla protokołu IP w wersji 6.

Przed rozpoczęciem konfigurowania bezpieczeństwa IP dla danego ośrodka, należy zdecydować, która metoda będzie używana; na przykład, czy preferowane jest użycie tuneli lub filtrów (lub obu), który rodzaj tunelu najbardziej pasuje do potrzeb użytkownika i tak dalej. W poniższych sekcjach znaleźć można informacje, których znajomość ułatwi podjęcie decyzji:

Przyspieszenie sprzętowe
Adapter 10/100 Mbps Ethernet PCI Adapter II (opcja o kodzie 4962) oferuje ochronę IP opartą na standardach; został on zaprojektowany w celu odciążenia funkcji ochrony IP systemu operacyjnego AIX.

Jeśli w systemie AIX jest zainstalowany adapter 10/100 Mbps Ethernet PCI Adapter II, stos bezpieczeństwa IP korzysta z jego następujących możliwości:

- szyfrowania i deszyfrowania za pomocą algorytmów szyfrowania DES lub potrójnego DES,
- uwierzytelniania za pomocą algorytmów MD5 lub SHA-1,
- przechowywania informacji o powiązaniach bezpieczeństwa.

Funkcje adaptera używane są zamiast algorytmów programowych. Adapter 10/100 Mbps Ethernet PCI Adapter II jest dostępny dla tuneli ręcznych i IKE.

Opcja przyspieszenia sprzętowego bezpieczeństwa IP jest dostępna w wersji 5.1.0.25 lub nowszej zestawów plików `bos.net.ipsec.rte` i `devices.pci.1410ff01.rte`.

Istnieje ograniczenie liczby powiązań ochrony, które mogą być odciążone przez adapter sieciowy po stronie odbiorcy (ruch przychodzący). Po stronie przesyłającego (ruch wychodzący) wszystkie pakiety, które korzystają z obsługiwanej konfiguracji, są odciążane przez adapter. Niektóre konfiguracje tuneli nie mogą być w ten sposób odciążone.

Adapter 10/100 Mbps Ethernet PCI Adapter II obsługuje następujące opcje:

- szyfrowanie DES, 3DES lub NULL przez protokół ESP,
- uwierzytelnianie HMAC-MD5 lub HMAC-SHA-1 przez protokoły ESP lub AH, ale nie przez oba na raz (jeśli używany jest równocześnie protokół ESP i AH, to protokół ESP musi być wykonany jako pierwszy; tak jest zawsze w przypadku tuneli IKE, w przypadku tuneli ręcznych użytkownik sam może wybrać kolejność),
- tryb transportu i tunelu,
- odciążenie pakietów IPV4.

Uwaga: Adapter 10/100 Mbps Ethernet PCI Adapter II nie obsługuje pakietów z opcjami IP.

Aby włączyć adapter 10/100 Mbps Ethernet PCI Adapter II dla ochrony IP, należy odłączyć interfejs sieciowy, a następnie włączyć opcję IPsec Offload.

Aby odłączyć interfejs sieciowy, w programie SMIT wykonaj poniższe instrukcje:

Aby włączyć opcję IPsec Offload, w programie SMIT wykonaj poniższe instrukcje:

1. Zaloguj się jako użytkownik **root**.
2. W wierszu komend wpisz `smitty eadap` i naciśnij Enter.
3. Wybierz opcję **Zmień / pokaż charakterystykę adaptera sieciowego typu Ethernet** i naciśnij Enter.
4. Wybierz adapter 10/100 Mbps Ethernet PCI Adapter II i naciśnij Enter.
5. Zmień pole Odciążenie ochrony IP na tak i naciśnij Enter.

Aby odłączyć interfejs sieciowy, w wierszu komend wpisz następującą komendę:

```
# ifconfig enX detach
```

Aby włączyć atrybut IPsec offload, w wierszu komend wpisz następującą komendę:

```
# chdev -l entX -a ipsec_offload=yes
```

Aby sprawdzić, czy atrybut IPsec offload został włączony, w wierszu komend wpisz następującą komendę:

```
# lsattr -El entX detach
```

Aby wyłączyć atrybut IPsec offload, w wierszu komend wpisz następującą komendę:

```
# chdev -l entX -a ipsec_offload=no
```

Aby upewnić się, że konfiguracja tunelu korzysta z zalet atrybutu IPsec offload, należy użyć komendy **enstat**. Komenda ta pokazuje wszystkie statystyki przesyłanych i odbieranych pakietów IPsec, gdy atrybut IPsec offload jest włączony. Na przykład, jeśli interfejsem Ethernet jest **ent1**, należy wpisać następującą komendę:

```
# entstat -d ent1
```

Wyświetlone zostaną informacje podobne do poniższego przykładu:

```
.
.
.
10/100 Mbps Ethernet PCI Adapter II (1410ff01) Specific Statistics:
--------------------------------------------
.
.
.
Transmit IPsec packets: 3
Transmit IPsec packets dropped: 0
Receive IPsec packets: 2
Receive IPsec packets dropped: 0
```

Parametr strojony sieci
W zależności od liczby tuneli w konfiguracji można zwiększyć maksymalną wielkość buforu dla gniazda.

Jeśli w środowisku działa wiele tuneli i dla parametru strojonego **sb_max** pozostawiono wartość domyślną, proces demona IKE i proces demona menedżera tuneli mogą przestać odpowiadać ze względu na duże obciążenie sieci.

Dla parametru strojonego **sb_max** istnieje możliwość użycia następujących wartości:

- 10 MB dla 500 tuneli
- 20 MB dla 1000 tuneli

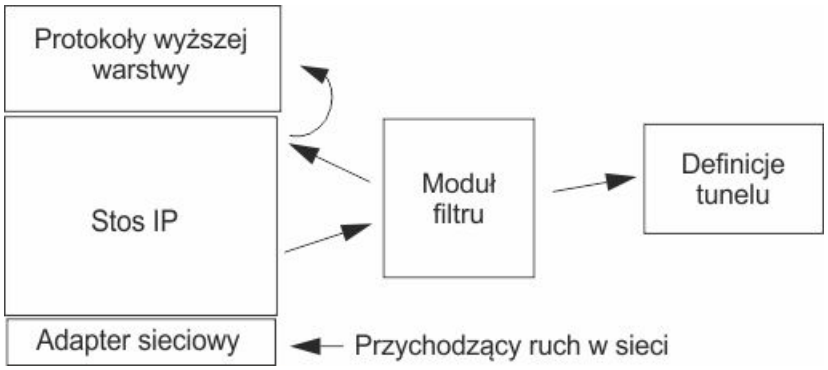
Informacje pokrewne
Parametr strojony sb_max

Porównanie tuneli i filtrów
Tunele i *filtry* to dwa różne elementy bezpieczeństwa IP. Tunele wymagają filtrów, ale filtry nie wymagają tuneli.

Filtrowanie jest funkcją, za pomocą której pakiety przychodzące i wychodzące mogą być akceptowane lub odrzucane w oparciu o różne charakterystyki zwane *regułami*. Ta funkcja pozwala administratorowi systemu skonfigurować hosta, aby sterował ruchem danych między nim a innymi hostami. Filtrowanie odbywa się na podstawie różnych właściwości pakietu, takich jak adresy miejsca źródłowego i docelowego, wersja protokołu IP (4 lub 6), maska podsieci, protokół, port, charakterystyki routingu, fragmentacja, interfejs oraz definicje tunelu. To filtrowanie odbywa się na poziomie warstwy IP, nie są więc wymagane żadne zmiany w aplikacjach.

Tunele określają powiązania bezpieczeństwa pomiędzy dwoma hostami. Powiązania te wymagają specyficznych parametrów zabezpieczeń, które są współużytkowane między punktami końcowymi tunelu.

Na poniższym rysunku pokazano, w jaki sposób pakiet przechodzi z adaptera sieciowego do stosu IP. Z tego poziomu wywoływany jest moduł filtru, aby określić, czy pakiet ma być przyjęty, czy odrzucony. Jeśli określony jest identyfikator tunelu, zamiast istniejących definicji tunelu sprawdzany jest pakiet. Jeśli dehermetyzacja z tunelu powiedzie się, pakiet jest przepuszczany do wyższej warstwy protokołu. W przypadku pakietów wychodzących wszystko odbywa się w odwrotnej kolejności. Tunel wykorzystuje regułę filtrowania, aby powiązać pakiet z konkretnym tunelem, ale funkcja filtrowania może wystąpić bez przekazywania pakietu do tunelu.



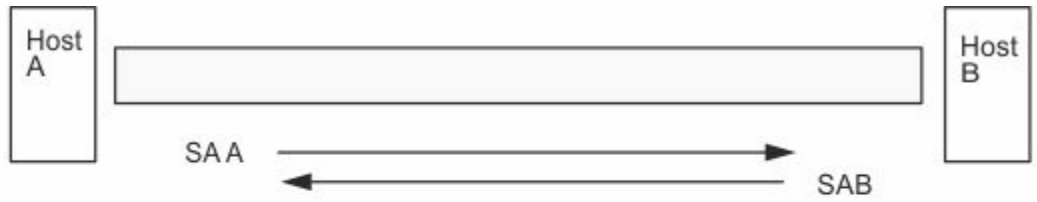
Rysunek 7. Routing pakietu sieciowego

Na ilustracji przedstawiono trasę, jaką pokonuje pakiet sieciowy. Przychodzący z sieci pakiet trafia do adaptera sieciowego, a następnie przechodzi do stosu IP, skąd jest wysyłany do modułu filtru. Z modułu pakiet jest wysyłany albo do definicji tunelu, albo jest zwracany do stosu IP, skąd jest przekazywany dalej protokołom wyższej warstwy.

Tunele i powiązania bezpieczeństwa

Tunele są używane, gdy wymagane jest uwierzytelnianie lub uwierzytelnianie i szyfrowanie danych. Tunele są definiowane na podstawie określania powiązań bezpieczeństwa między dwoma hostami. Powiązania bezpieczeństwa definiują parametry dla algorytmów szyfrowania i uwierzytelniania oraz charakterystyk tunelu.

Na poniższym rysunku przedstawiono tunel wirtualny między hostem A i hostem B.



Powiązanie bezpieczeństwa (Security Association - SA) składa się z następujących elementów:

Adres docelowy
SPI
Klucz
Algorytm i format szyfrowania
Algorytm uwierzytelniania
Czas życia klucza

Rysunek 8. Ustanowienie chronionego tunelu między hostami A i B

Na ilustracji przedstawiono tunel wirtualny biegnący między hostem A i hostem B. Powiązanie bezpieczeństwa A jest przedstawione w postaci strzałki skierowanej od hosta A do hosta B. Powiązanie bezpieczeństwa B jest przedstawione w postaci strzałki skierowanej od hosta B do hosta A. Powiązanie bezpieczeństwa składa się z adresu docelowego, interfejsu SPI, klucza, algorytmu szyfrowania i formatu, algorytmu uwierzytelniania oraz czasu ważności klucza.

Interfejs SPI (Security Parameter Index) oraz adres docelowy identyfikują unikalne powiązanie bezpieczeństwa. Parametry te są wymagane, aby jednoznacznie określić tunel. Pozostałe parametry, takie

jak algorytm szyfrowania, algorytm uwierzytelniania, klucze oraz czas ważności klucza można określić lub skorzystać z wartości domyślnych.

Uwagi dotyczące tunelu
Przed podjęciem decyzji, jaki rodzaj tunelu wykorzystać na potrzeby bezpieczeństwa IP, należy rozważyć kilka zagadnień.

Tunele IKE różnią się od tuneli ręcznych, ponieważ konfigurowanie strategii zabezpieczeń jest procesem innym niż definiowanie punktów końcowych tunelu.

W przypadku tuneli IKE mamy do czynienia z dwukrokowym procesem uzgadniania. Każdy krok procesu uzgadniania nazywany jest *fazą*, a każda faza może mieć oddzielne strategie bezpieczeństwa.

Kiedy rozpoczyna się uzgadnianie klucza internetowego, konieczne jest skonfigurowanie bezpiecznego kanału. Proces ten nazywany jest fazą *zarządzania kluczem* lub *fazą 1*. Podczas tej fazy każda ze stron, w celu uwierzytelnienia drugiej strony i przyjęcia informacji identyfikatora, korzysta z wstępnych kluczy wspólnych lub certyfikatów cyfrowych. W fazie tej konfigurowane jest powiązanie bezpieczeństwa, podczas którego obie strony określają, w jaki sposób zaplanować bezpieczną komunikację oraz jakie zabezpieczenia mają być użyte do komunikacji podczas fazy drugiej. Wynikiem tej fazy jest tunel *IKE* lub tunel *fazy 1*.

Druga faza nazywana jest fazą *zarządzania danymi* lub *fazą 2* i korzysta ona w celu utworzenia powiązań bezpieczeństwa dla protokołów AH i ESP, które aktualnie zabezpieczają komunikację z tunelu IKE. Faza ta określa także dane, które będą korzystały z tunelu bezpieczeństwa IP. Może określić na przykład następujące elementy:

- maskę podsieci,
- zakres adresu,
- kombinację protokołu i numeru portu.

Rysunek 9. Proces konfigurowania tunelu IKE

Na powyższej ilustracji przedstawiono dwukrokowy, dwufazowy proces konfigurowania tunelu IKE.

Uwaga: IKEv2 także składa się z dwóch faz. Pierwszą fazę nazywa się fazą *IKE SA* lub *fazą 1*. Drugą fazę nazywa się fazą *CHILD SA* lub *fazą 2*. W przeciwieństwie do sposobu, w jaki tunele są ustanawiane w IKEv1, gdy tunel fazy 1 jest ustanawiany w IKEv2, tunel fazy 2 jest aktywowany automatycznie. Konfiguracja tuneli IKEv2 jest podobna do konfiguracji tuneli IKEv1.

W wielu przypadkach punkty końcowe tunelu zarządzania kluczem (IKE) będą takie same, jak punkty końcowe tunelu zarządzania danymi (bezpieczeństwo IP). Punktami końcowymi tunelu IKE są identyfikatory komputerów ustanawiających negocjację. Punkty końcowe tunelu bezpieczeństwa IP opisują rodzaj komunikacji, jakiej będzie używał tunel bezpieczeństwa IP. Dla prostych tuneli łączących host z hostem, dla których cały ruch danych między dwoma tunelami jest zabezpieczany przez ten sam tunel, punkty końcowe dla fazy 1 i fazy 2 są takie same. Kiedy stronami negocjacji są dwie bramy, punktami końcowymi tunelu IKE są także dwie bramy, a tunelu bezpieczeństwa IP - komputery lub podsieci (za bramami) bądź zasięg adresów (za bramami) użytkowników tunelu.

Parametry i strategia zarządzania kluczem
Strategię zarządzania kluczem można dostosować do własnych potrzeb, określając parametry, które mają być wykorzystane podczas negocjacji IKE. Na przykład istnieją strategie zarządzania kluczem dla wstępnych kluczy wspólnych lub uwierzytelniania trybu podpisu. Dla fazy 1 użytkownik musi określić pewne właściwości zabezpieczenia zarządzania kluczami, za pomocą których będzie dokonywana wymiana.

Faza 1 (faza zarządzania kluczami) ustawia następujące parametry konfiguracyjne tunelu IKE:

Key Management (Phase 1) Tunnel (Tunel zarządzania kluczami - faza 1)
Nazwa danego tunelu IKE. Dla każdego tunelu muszą być określone punkty końcowe negocjacji. Są to dwa komputery, z których planowane jest wysyłanie i sprawdzanie poprawności komunikatów IKE. Nazwa tunelu może opisywać jego punkty końcowe, na przykład `VPN Boston` lub `VPN Acme`

Host Identity Typ (Rodzaj tożsamości hosta)
Rodzaj identyfikatora, który będzie wykorzystany do wymiany IKE. Rodzaj identyfikatora i jego wartość musi być zgodna z wartością wstępnego klucza wspólnego, aby zapewnić przeprowadzenie właściwego wyszukiwania klucza. Jeśli do wyszukiwania wartości wstępnego klucza wspólnego używany jest oddzielny identyfikator, to *identyfikator hosta* jest identyfikatorem hosta, a jego *rodzajem* jest KEY_ID. Rodzaj KEY_ID jest przydatny w przypadku, gdy pojedynczy host ma więcej niż jedną wartość wstępnego klucza wspólnego.

Host Identity (Tożsamość hosta)
Wartość identyfikatora hosta reprezentowana jako adres IP, pełna nazwa domeny (fully qualified domain name - FQDN) lub użytkownik pełnej nazwy domeny (*użytkownik*@*FQDN*). Na przykład jdoe@studentmail.ut.edu.

IP Address (Adres IP)
Adres IP zdalnego hosta. Ta wartość jest wymagana, kiedy rodzajem identyfikatora hosta jest KEY_ID lub gdy identyfikator hosta nie może być przetłumaczony na adres IP. Na przykład, gdy nazwa użytkownika nie może być przetłumaczona za pomocą lokalnego serwera nazw, trzeba podać adres IP dla strony zdalnej.

Parametry i strategia zarządzania danymi
Podczas fazy 1 konfiguracji tunelu IKE ustawiane są parametry propozycji zarządzania danymi. Są one tymi samymi parametrami bezpieczeństwa IP wykorzystywanymi w tunelach ręcznych i opisują rodzaj zabezpieczenia, jaki ma być używany w celu bezpiecznego ruchu danych w tunelu. Dla jednego tunelu fazy 1 można uruchomić kilka tuneli fazy 2.

Przestawione poniżej rodzaje identyfikatorów punktów końcowych opisują rodzaj danych, korzystających z tunelu danych bezpieczeństwa IP:

Host, Subnet (Podsieć) lub Range (Zakres)
Opisuje, czy ruch danych przemieszczających się w tunelu będzie dla określonego hosta, podsieci czy zakresu adresu.

Host/Subnet ID (Identyfikator hosta/podsieci)
Zawiera tożsamość hosta lub podsieci systemów lokalnych lub zdalnych, inicjując ruch danych przez tunel. Określa identyfikatory wysyłane podczas negocjacji fazy 2 oraz reguły filtrowania, które zostaną utworzone, jeśli negocjacja się powiedzie.

Subnet mask (Maska podsieci)
Opisuje wszystkie adresy IP wewnątrz podsieci (na przykład host 9.53.250.96 i maska 255.255.255.0).

Starting IP Address Range (Początek zakresu adresów IP)
Udostępnia początkowy adres IP dla zakresu adresów, które będą wykorzystywane przez tunel (na przykład 9.53.250.96 od 9.53.250.96 do 9.53.250.93).

Ending IP Address Range (Koniec zakresu adresów IP)
Udostępnia końcowy adres IP dla zakresu adresów, które będą wykorzystywane przez tunel (na przykład 9.53.250.93 od 9.53.250.96 do 9.53.250.93).

Port
Opisuje dane korzystające z określonego numeru portu (na przykład 21 lub 23).

Protocol (Protokół)
Opisuje dane transportowane za pomocą określonego protokołu (na przykład TCP lub UDP). Określa protokół wysyłany podczas negocjacji fazy 2 oraz reguły filtrowania, które zostaną utworzone, jeśli negocjacja się powiedzie. Protokół lokalnego punktu końcowego musi odpowiadać protokołowi zdalnego punktu końcowego.

End Port (Port końcowy)
Opisuje port końcowy dla przesyłania danych (na przykład 100 lub 500). Domyślnym portem końcowym jest 65355.

Ograniczenie: Dla IKEv2 jako selektorów ruchu danych należy używać tylko zakresów adresów IPv4 lub IPv6. Port końcowy ma zastosowanie tylko dla IKEv2 i systemu AIX w wersji 6.1 TL 04 lub nowszej.

Wybieranie rodzaju tunelu
Decyzja o wyborze tuneli ręcznych lub IKE zależy od rodzaju obsługi tunelu dostępnej w zdalnym punkcie końcowym i wymaganego rodzaju zarządzania kluczem.

Należy używać tuneli IKE (jeśli są dostępne), ponieważ oferują one opartą na standardzie przemysłowym, zabezpieczoną negocjację klucza i jego odświeżanie. Wykorzystują także zaletę nagłówków protokołów ESP i AH grupy IETF oraz obsługują zabezpieczenie przeciwpowtórzeniowe. Opcjonalnie można także skonfigurować tryb podpisu i używać certyfikatów cyfrowych.

Tunele ręczne powinny być używane w przypadku, jeśli zdalny punkt końcowy korzysta z jednego z algorytmów wymagających tuneli ręcznych. Tunele ręczne zapewniają współdziałanie z większą liczbą hostów. Ponieważ klucze są statyczne, trudno je zmienić, mogą być niewygodne do aktualizowania, także nie są całkowicie bezpieczne. Tunele ręczne mogą być wykorzystywane między hostem działającym pod kontrolą tego systemu operacyjnego, a dowolnym innym komputerem korzystającym z ochrony IP i mającym wspólny zestaw algorytmów szyfrujących i uwierzytelniających. Większość dostawców oferuje zestaw Keyed MD5 z algorytmem szyfrowania DES lub HMAC MD5 z algorytmem DES. Ten podzbiór współpracuje z prawie wszystkimi implementacjami ochrony IP.

Procedura wykorzystywana podczas konfigurowania tuneli ręcznych zależy od tego, czy konfigurowany jest pierwszy host tunelu, czy drugi, który musi mieć parametry zgodne z ustawieniami hosta pierwszego. Jeśli konfigurowany jest host pierwszy, klucze mogą być wygenerowane automatycznie, a algorytmy mogą być domyślne. W przypadku konfigurowania hosta drugiego, jeśli jest to możliwe, należy zaimportować informacje o tunelu ze zdalnego punktu końcowego.

Ważne jest także określenie, czy system zdalny znajduje się za firewallem. Jeśli tak jest, jego konfiguracja musi zawierać informacje o tym firewallu.

Używanie protokołu IKE z protokołem DHCP lub z adresami przydzielanymi dynamicznie
Powszechnym scenariuszem korzystania z bezpieczeństwa IP razem z systemem operacyjnym jest inicjowanie sesji IKE z serwerem przez systemy zdalne, których tożsamość nie może być powiązana z adresem IP.

Taki przypadek może wystąpić w środowisku LAN, w którym bezpieczeństwo IP jest wykorzystywana do łączenia serwerem sieciowym i oczekiwane jest szyfrowanie danych. Inny często spotykany przypadek to łączenie klientów zdalnych z serwerem przy użyciu pełnej nazwy domeny (FQDN) lub adresu e-mail (user@FQDN) w celu określenia identyfikatora zdalnego.

Jeśli używany jest tryb główny z identyfikatorami nie opartymi na adresie IP, w fazie zarządzania kluczami (faza 1) jedynym obsługiwanym trybem uwierzytelniania jest podpis RSA. Tak więc, jeśli ma być używane uwierzytelnianie wstępnych kluczy wspólnych, należy użyć trybu agresywnego lub trybu głównego z adresami IP jako identyfikatorami. W rzeczywistości, jeśli liczba klientów DHCP, z którymi nawiązywany jest tunel IPsec, jest bardzo duża, to definiowanie unikalnych wstępnych kluczy wspólnych dla każdego klienta DHCP jest niewygodne, dlatego w takim wypadku zaleca się używanie uwierzytelniania z podpisami RSA. Można także w definicji tunelu używać identyfikatora grupy jako identyfikatora zdalnego, a więc tunel jest definiowany tylko jeden raz dla wszystkich klientów DHCP (patrz przykładowy plik definicji tunelu, `/usr/samples/ipsec/group_aix_responder.xml`). Identyfikator grupowy jest unikalną cechą IPsec w systemie AIX. Można zdefiniować identyfikator grupowy i włączyć do niego wszystkie identyfikatory IKE (takie, jak pojedynczy adres IP), pełne nazwy domen, użytkowników pełnych nazw domen, zakresy adresów IP i tak dalej. Identyfikatora tego następnie należy użyć w definicjach tunelu jako zdalnego identyfikatora w fazie 1 lub w fazie 2.

Uwaga: Jeśli używany jest identyfikator grupy, tunel należy zdefiniować tylko w roli odpowiadającego. Oznacza to, że tunel może być aktywowany tylko po stronie klienta DHCP.

Dla fazy zarządzania danymi (fazy 2), podczas tworzenia powiązań bezpieczeństwa IP do szyfrowania ruchu danych korzystającego z protokołu TCP lub UDP można skonfigurować ogólny tunel zarządzania danymi. Dlatego każde żądanie, które zostało uwierzytelnione w fazie 1, będzie korzystało z tunelu ogólnego dla fazy zarządzania danymi, jeśli adres IP nie jest skonfigurowany jawnie w bazie danych. Pozwala to wszystkim adresom porównywać tunel ogólny i może być wykorzystywane tak długo, jak długo rygorystyczne sprawdzanie bezpieczeństwa opartego na kluczu publicznym w fazie 1 będzie pomyślne.

Korzystanie z języka XML w celu definiowania ogólnego tunelu zarządzania danymi
Ogólny tunel zarządzania danymi można zdefiniować w formacie XML zrozumiałym dla **ikedb**.

Sekcja “Użycie interfejsu wiersza komend do konfigurowania tunelu IKE” na stronie 240 zawiera więcej informacji na temat interfejsu IKE XML i komendy **ikedb**. Ogólne tunele zarządzania danymi są używane z protokołem DHCP. Format XML korzysta z nazwy etykiety IPSecTunnel. W innym kontekście zwany jest on również *tunelem fazy 2*. *Ogólny tunel zarządzania danymi* nie jest prawdziwym tunelem, ale używane jest w nim zabezpieczenie IPSecProtection, jeśli przychodzący komunikat zarządzania danymi (w określonym tunelu zarządzania kluczem) nie pasuje do żadnego tunelu zarządzania danymi dla danego tunelu zarządzania kluczem. Jest on używany jedynie wtedy, gdy systemem odpowiadającym jest system AIX. Określanie ochrony IPSecProtection dla ogólnego tunelu zarządzania danymi jest opcjonalne.

Ogólny tunel zarządzania danymi jest definiowany w elemencie IKEProtection. Używane są do tego dwa atrybuty języka XML: *IKE_IPSecDefaultProtectionRef* i *IKE_IPSecDefaultAllowedTypes*.

Najpierw trzeba zdefiniować zabezpieczenie IPSecProtection, które będzie używane domyślnie, jeśli nie zostanie dopasowany żaden IPSecTunnels (tunel zarządzania danymi). Zabezpieczenie IPSecProtection, które jest używane domyślnie, musi mieć nazwę IPSec_ProtectionName zaczynającą się od `_defIPSprot_`.

Następnie należy przejść do elementu IKEProtection, dla którego będzie używane domyślnie zabezpieczenie IPSecProtection. Należy także określić atrybut **IKE_IPSecDefaultProtectionRef**, który zawiera nazwę domyślnego zabezpieczenia IPSec_Protection.

Dla danego elementu IKEProtection należy określić również wartość atrybutu **IKE_IPSecDefaultAllowedTypes**. Może on mieć jedną lub więcej wartości spośród wymienionych poniżej (jeśli użytych jest wiele wartości, należy oddzielić je spacjami):

```
Local_IPV4_Address
Local_IPV6_Address
Local_IPV4_Subnet
Local_IPV6_Subnet
Local_IPV4_Address_Range
Local_IPV6_Address_Range
Remote_IPV4_Address
```

```
Remote_IPV6_Address
Remote_IPV4_Subnet
Remote_IPV6_Subnet
Remote_IPV4_Address_Range
Remote_IPV6_Address_Range
```

Wartości te odpowiadają rodzajom identyfikatorów określonych przez inicjator. Podczas negocjacji IKE bieżące identyfikatory są ignorowane. Podane zabezpieczenie IPSecProtection jest używane, jeśli atrybut **IKE_IPSecDefaultAllowedTypes** zawiera łańcuch rozpoczynający się od `Local_`, co odpowiada rodzajowi identyfikatora lokalnego inicjatora oraz łańcuch rozpoczynający się od `Remote_`, co odpowiada rodzajowi identyfikatora zdalnego inicjatora. Innymi słowy, jeśli ma być użyte odpowiednie zabezpieczenie IPSec_Protection, to każdy atrybut **IKE_IPSecDefaultAllowedTypes** musi mieć przynajmniej jedną wartość `Local_` i jedną wartość `Remote_`.

Przykład ogólnego tunelu zarządzania danymi
Tunel zarządzania danymi można wykorzystywać do wysyłania komunikatów do systemu.

Inicjator wysyła w fazie 2 (zarządzanie danymi) następujący komunikat do systemu AIX:

```
Local ID type:    IPV4_Address
local ID:         192.168.100.104

remote ID type:   IPV4_Subnet
remote ID:        10.10.10.2
remote netmask:   255.255.255.192
```

W systemie AIX nie ma tunelu zarządzania danymi odpowiadającego tym identyfikatorom, ale jest zabezpieczenie IPSecProtection z atrybutami zdefiniowanymi następująco:

```
IKE_IPSecDefaultProtectionRef="_defIPSprot_protection4"
IKE_IPSecDefaultAllowedTypes="Local_IPV4_Address
                              Remote_IPV4_Address
                              Remote_IPV4_Subnet
                              Remote_IPV4_Address_Range"
```

Rodzaj identyfikatora lokalnego przychodzącego komunikatu, IPV4_Address, odpowiada jednej z wartości Local_ spośród dozwolonych rodzajów - Local_IPV4_Address. Do wartości Remote_IPV4_Subnet pasuje także identyfikator zdalny komunikatu - IPV4_Subnet. Dlatego negocjacja tunelu zarządzania danymi będzie kontynuowana za pomocą atrybutu `_defIPSprot_protection4` jako zabezpieczenia IPSecProtection.

Plik `/usr/samples/ipsec/default_p2_policy.xml` jest plikiem XML definiującym ogólne zabezpieczenie IPSecProtection, który może być użyty jako przykład.

Konfigurowanie tuneli IKE (Internet Key Exchange)
Tunele IKE można konfigurować za pomocą programu SMIT lub wiersza komend.

Używanie interfejsu programu SMIT do konfigurowania tunelu IKE
Do skonfigurowania tuneli IKE i wykonania podstawowych funkcji obsługi bazy danych IKE można użyć interfejsu programu SMIT.

Program ten, w celu dodawania, usuwania i modyfikowania definicji tuneli IKE, korzysta z podstawowych funkcji komend języka XML. Jest on używany do szybkiego konfigurowania tuneli IKE i udostępnia przykłady składni języka XML używane do tworzenia definicji tunelu IKE. Menu programu SMIT dla tuneli IKE pozwala także na składowanie, odtwarzanie i inicjowanie bazy danych IKE.

Aby skonfigurować tunel IKE korzystający z protokołu IPv4, należy użyć krótkiej ścieżki **`smitty ike4`**. Aby skonfigurować tunel IKE korzystający z protokołu IPv6, należy użyć krótkiej ścieżki **`smitty ike6`**. Funkcje bazy danych IKE można znaleźć w menu Advanced IP Security Configuration (Zaawansowana konfiguracja bezpieczeństwa IP).

Użycie interfejsu wiersza komend do konfigurowania tunelu IKE
Komenda **`ikedb`** pozwala użytkownikowi odtwarzać, aktualizować, usuwać, importować i eksportować informacje z bazy danych IKE, za pomocą interfejsu języka XML.

Komenda ta pozwala użytkownikowi zapisywać do (wstawiać) lub odczytywać z (pobierać) bazy danych IKE. Format wejściowy i wyjściowy jest plikiem XML (Extensible Markup Language). Format pliku XML jest określony przez jego definicję rodzaju dokumentu (Document Type Definition - DTD). Za pomocą komendy **ikedb** użytkownik może obejrzeć definicję DTD, która jest używana do sprawdzenia poprawności pliku XML podczas wstawiania. Jedyną modyfikacją, jaką można wprowadzić w definicji DTD, jest dodanie deklaracji encji za pomocą opcji **-e**. Wszystkie zewnętrzne deklaracje DOCTYPE w pliku wejściowym XML zostaną zignorowane, a wewnętrzne deklaracje DOCTYPE mogą spowodować błąd. Reguły stosowane do analizowania pliku XML za pomocą deklaracji DTD są opisane w standardzie języka XML. W pliku `/usr/samples/ipsec` znajduje się przykład typowego pliku XML, który definiuje powszechne scenariusze tunelu. Szczegóły dotyczące składni komendy **ikedb** zawiera publikacja *Commands Reference*.

Komendy **ike** można używać do uruchamiania, zatrzymywania i monitorowania tuneli IKE. Ta komenda może być użyta także do aktywowania, usuwania lub pokazywania tuneli IKE i bezpieczeństwa IP. Szczegóły dotyczące składni komendy **ike** zawiera publikacja *Commands Reference*.

Poniższe przykłady pokazują, w jaki sposób można użyć komendy **ike**, **ikedb** i kilku innych, do konfigurowania i sprawdzania stanu tunelu IKE:

1. Aby uruchomić negocjację tunelu (*aktywować* tunel) lub zezwolić systemowi na działanie jako system odpowiadający (w zależności od określonej roli), należy użyć komendy **ike** z podanym numerem tunelu w następujący sposób:

   ```
   # ike cmd=activate numlist=1
   ```

   Można użyć także identyfikatora systemu zdalnego lub adresów IP, tak jak pokazano to w poniższych przykładach:

   ```
   # ike cmd=activate remid=9.3.97.256
   # ike cmd=activate ipaddr=9.3.97.100, 9.3.97.256
   ```

   Ponieważ zakończenie działania komend może potrwać kilka sekund, komenda zakończy się po rozpoczęciu negocjacji.
2. Aby wyświetlić status tunelu, komendy **ike** należy użyć w następujący sposób:

   ```
   # ike cmd=list
   ```

   Wyświetlone zostaną informacje podobne do poniższych:

   ```
   Phase 1 Tunnel ID       [1]
   Phase 2 Tunnel ID       [1]
   ```

   Informacje przedstawiają aktywne aktualnie tunele fazy 1 i 2.
3. Aby otrzymać szczegółową listę tuneli, komendy **ike** należy użyć w następujący sposób:

   ```
   # ike cmd=list verbose
   ```

   Wyświetlone zostaną informacje podobne do poniższych:

   ```
   Phase 1 Tunnel ID       1
   Local ID Type:          Fully_Qualified_Domain_Name
   Local ID:               bee.austin.ibm.com
   Remote ID Type:         Fully_Qualified_Domain_Name
   Remote ID:              ipsec.austin.ibm.com
   Mode:                   Aggressive
   Security Policy:        BOTH_AGGR_3DES_MD5
   Role:                   Initiator
   Encryption Alg:         3DES-CBC
   Auth Alg:               Preshared Key
   Hash Alg:               MD5
   Key Lifetime:           28800 Seconds
   Key Lifesize:           0 Kbytes
   Key Rem Lifetime:       28737 Seconds
   Key Rem Lifesize:       0 Kbytes
   Key Refresh Overlap:    5%
   Tunnel Lifetime:        2592000 Seconds
   Tunnel Lifesize:        0 Kbytes
   ```

```
Tun Rem Lifetime:       2591937 Seconds
Status:                 Active

Phase 2 Tunnel ID       1
Local ID Type:          IPv4_Address
Local ID:               10.10.10.1
Local Subnet Mask:      N/A
Local Port:             any
Local Protocol:         all
Remote ID Type:         IPv4_Address
Remote ID:              10.10.10.4
Remote Subnet Mask:     N/A
Remote Port:            any
Remote Portocol:        all
Mode:                   Oakley_quick
Security Policy:        ESP_3DES_MD5_SHA_TUNNEL_NO_PFS
Role:                   Initiator
Encryption Alg:         ESP_3DES
AH Transform:           N/A
Auth Alg:               HMAC-MD5
PFS:                    No
SA Lifetime:            600 Seconds
SA Lifesize:            0 Kbytes
SA Rem Lifetime:        562 Seconds
SA Rem Lifesize:        0 Kbytes
Key Refresh Overlap:    15%
Tunnel Lifetime:        2592000 Seconds
Tunnel Lifesize:        0 Kbytes
Tun Rem Lifetime:       2591962 Seconds
Assoc P1 Tunnel:        0
Encap Mode:             ESP_tunnel
Status:                 Active
```

4. Aby dla nowo aktywowanych tuneli IKE wyświetlić reguły filtrowania z tabeli filtrów dynamicznych, komendy **lsfilt** należy użyć w następujący sposób:

```
# lsfilt -d
```

Wyświetlone zostaną informacje podobne do poniższego przykładu:

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001 both both no all
  packets 0 all
2 *** Dynamic filter placement rule (Reguła rozmieszczania filtru dynamicznego) *** no
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 yes all any 0 any 0 both both no all
  packets 0 all

*** Dynamic table (Tabela dynamiczna) ***

0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 500 eq 500 local both no all
  packets 0
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both inbound no all
  packets 0
0 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both inbound no all
  packets 0
1 permit 10.10.10.1 255.255.255.255 10.10.10.4 255.255.255.255 no all any 0 any
  0 both outbound yes all packets 1
1 permit 10.10.10.4 255.255.255.255 10.10.10.1 255.255.255.255 no all any 0 any
  0 both inbound yes all packets 1
```

W tym przykładzie przedstawiono komputer mający tylko jeden tunel IKE. Reguła rozmieszczania filtrów dynamicznych (w tym przykładzie tabeli statycznej reguła nr 2) może być przeniesiona przez użytkownika, w celu sterowania rozmieszczeniem względem wszystkich pozostałych reguł zdefiniowanych przez użytkownika. Reguły tabeli dynamicznej są konstruowane automatycznie, podczas negocjacji tuneli, a odpowiadające im reguły są wstawiane do tabeli filtrów. Reguły te mogą być jedynie wyświetlane, nie mogą być natomiast modyfikowane.

5. Aby włączyć protokołowanie reguł filtrów dynamicznych, należy ustawić opcję protokołowania reguły nr 2 na Tak. W tym celu należy użyć komendy **chfilt** w następujący sposób:

```
# chfilt -v 4 -n 2 -l y
```

Więcej informacji na temat protokołowania komunikacji IKE zawiera sekcja “Narzędzia protokołowania” na stronie 266.

6. Aby dezaktywować tunel, komendy **ike** należy użyć w następujący sposób:

```
# ike cmd=remove numlist=1
```

7. Aby wyświetlić definicje tunelu, komendy **ikedb** należy użyć w następujący sposób:

```
# ikedb -g
```

8. Aby z pliku XML, który został wygenerowany na komputerze w jednym z węzłów sieci, wstawić definicje do bazy danych IKE i nadpisać wszystkie istniejące w bazie danych obiekty o tej samej nazwie, komendy **ikedb** należy użyć w następujący sposób:

```
# ikedb -pFs peer_tunnel_conf.xml
```

   Plik `peer_tunnel_conf.xml` jest plikiem XML wygenerowanym na komputerze w jednym z węzłów sieci.

9. Aby uzyskać definicje tunelu fazy 1 nazwanego *tunnel_sys1_and_sys2* , a także definicje wszystkich zależnych od niego tuneli fazy 2, razem z poszczególnymi kolekcjami propozycji i zabezpieczeniami, komendy **ikedb** należy użyć w następujący sposób:

```
# ikedb -gr -t IKETunnel -n tunnel_sys1_and_sys2
```

10. Aby z bazy danych usunąć wszystkie wstępne klucze wspólne, komendy **ikedb** należy użyć w następujący sposób:

```
# ikedb -d -t IKEPresharedKey
```

Informacje ogólne na temat obsługi grup tunelu IKE zawiera sekcja “Obsługa grupy” na stronie 243. Aby z poziomu wiersza komend zdefiniować grupy, można użyć komendy **ikedb**.

Tunele IKE systemu AIX a podobieństwa do systemu Linux
Tunel IKE systemu AIX można skonfigurować, korzystając z plików konfiguracyjnych systemu Linux.

Aby skonfigurować tunel IKE systemu AIX, korzystając z plików konfiguracyjnych systemu Linux, należy zastosować komendę **ikedb** z opcją **-c** (opcja konwersji), co umożliwi użycie plików konfiguracyjnych `/etc/ipsec.conf` i `/etc/ipsec.secrets` systemu Linux jako definicji tunelu IKE. Komenda **ikedb** analizuje pliki konfiguracyjne systemu Linux, tworzy plik XML i opcjonalnie dodaje definicje tunelu XML do bazy danych IKE. Definicje tunelu można później obejrzeć za pomocą komendy **ikedb -g**.

Obsługa grupy
Zabezpieczenie IP obsługuje grupowanie identyfikatorów IKE w definicji tunelu, aby powiązać wiele identyfikatorów z pojedynczą strategią bezpieczeństwa, bez konieczności tworzenia oddzielnych definicji tunelu.

Grupowanie jest pomocne szczególnie podczas konfigurowania połączeń z kilkoma zdalnymi hostami, ponieważ można wtedy uniknąć konfigurowania lub zarządzania wieloma definicjami tunelu. Także w przypadku zmian w strategii zabezpieczeń nie trzeba dokonywać zmian w wielu definicjach tunelu.

Przed użyciem nazwy grupy w definicji tunelu, należy zdefiniować grupę. Wielkość grupy jest ograniczona do 1 kB. Po stronie inicjatora negocjacji grup można używać jako identyfikatorów zdalnych tylko w definicjach tuneli zarządzania danymi. Po stronie odpowiadającego grup można używać jako identyfikatorów zdalnych w definicjach tuneli zarządzania danymi i zarządzania kluczami.

Grupa składa się z nazwy grupy i listy identyfikatorów IKE oraz z rodzajów identyfikatorów. Wszystkie identyfikatory mogą być tego samego rodzaju lub różnych rodzajów, ale spośród wymienionych poniżej:

- adresy protokołu IPv4,
- adresy protokołu IPv6,
- nazwa FQDN,
- użytkownik@FQDN,

- rodzaje X500 DN.

Podczas negocjacji powiązania bezpieczeństwa identyfikatory w grupie są przeszukiwane liniowo, aż do napotkania pierwszej zgodności.

Informacje na temat definiowania grup z poziomu wiersza komend zawiera sekcja “Użycie interfejsu wiersza komend do konfigurowania tunelu IKE” na stronie 240.

Scenariusze konfigurowania tunelu IKE
Poniższe scenariusze opisują sytuacje, jakie są napotykane przez większość klientów podczas konfigurowania tuneli. Można je podzielić na przypadki dotyczące biura oddziału, partnera handlowego i dostępu zdalnego.

- W przypadku biura oddziału klient ma dwie zaufane sieci, które chce połączyć razem - zespół projektowy z jednego miejsca z zespołem pracującym w innym miejscu. W tym przykładzie między grupami są bramy, a cały ruch danych między bramami korzysta z tego samego tunelu. Dane są na końcu tunelu dehermetyzowane i dopuszczane do ruchu w ramach sieci intranet przedsiębiorstwa.

  W pierwszej fazie negocjacji IKE, między dwoma bramami tworzone jest powiązanie bezpieczeństwa IKE. Ruch danych przez bezpieczny tunel IP jest ruchem między dwiema podsieciami, a więc podczas negocjacji fazy 2 używane są identyfikatory podsieci. Po wprowadzeniu strategii zabezpieczeń i parametrów tunelu, tunel jest tworzony. W celu jego uruchomienia należy użyć komendy **ike**.
- W przypadku partnerów handlowych sieci nie są zaufane, a więc administrator może chcieć ograniczyć dostęp do mniejszej liczby hostów, znajdujących się za bramą. W tym przypadku tunel między hostami zapewnia komunikację zabezpieczoną przez bezpieczeństwo IP dla dwóch konkretnych hostów. Protokołem wykorzystywanym w fazie 2 jest protokół AH lub ESP. Ten tunel, łączący host z hostem, jest chroniony przez tunel łączący bramę z bramą.
- W przypadku dostępu zdalnego tunele tworzone są na żądanie, a do ich zabezpieczenia stosowana jest ochrona wyższego poziomu. Adresy IP mogą nie być wystarczające, dlatego zalecane jest wykorzystanie pełnych nazw domen lub adresu *użytkownik@*. Opcjonalnie można wykorzystać KEYID, aby powiązać klucz z identyfikatorem hosta.

Pojęcia dotyczące certyfikatów cyfrowych i narzędzia Key Manager (Menedżer kluczy)
Certyfikaty cyfrowe wiążą tożsamość z kluczem publicznym, za pomocą którego można zidentyfikować nadawcę lub odbiorcę zaszyfrowanego przekazu.

Bezpieczeństwo IP korzysta z certyfikatów cyfrowych, aby włączyć *kryptografię klucza publicznego*, zwaną też *kryptografią asymetryczną*, która szyfruje dane za pomocą klucza prywatnego, znanego jedynie użytkownikowi i deszyfruje je za pomocą związanego z nim klucza publicznego (wspólnego) z danej pary kluczy publiczny-prywatny. *Pary kluczy* są długimi łańcuchami danych, które działają jako klucze schematu szyfrowania użytkownika.

W kryptografii opartej na kluczu publicznym, klucz ten jest rozdawany osobom, z którymi użytkownik chce się komunikować. Nadawca podpisuje cyfrowo całą chronioną komunikację za pomocą odpowiadającego mu klucza prywatnego z danej pary kluczy. Odbiorca korzysta z klucza publicznego, aby sprawdzić podpis nadawcy. Jeśli komunikat zostanie pomyślnie deszyfrowany za pomocą klucza publicznego, odbiorca może potwierdzić, że nadawca został uwierzytelniony.

Kryptografia oparta na kluczu publicznym w celu wystawienia wiarygodnych certyfikatów cyfrowych opiera się na innych zaufanych firmach, znanych jako *ośrodki certyfikacji* (Certification Authority - *CA*). Odbiorca określa, które organizacje lub władze uważa za zaufane. Certyfikat jest wystawiany na określony czas; po wygaśnięciu terminu ważności musi on być zastąpiony.

System AIX udostępnia narzędzie Key Manager (Menedżer kluczy), które pozwala zarządzać certyfikatami cyfrowymi. Poniższe sekcje zawierają informacje na temat samych certyfikatów.

Format certyfikatów cyfrowych
Certyfikat cyfrowy składa się z określonych fragmentów informacji na temat tożsamości właściciela oraz ośrodka certyfikacji. Na poniższym rysunku przedstawiono przykład certyfikatu cyfrowego.

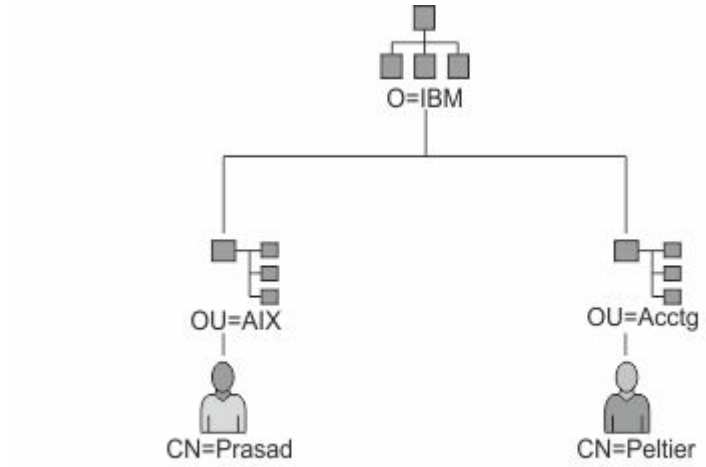
Rysunek 10. Elementy certyfikatu cyfrowego

Na ilustracji przedstawiono cztery jednostki certyfikatu cyfrowego. Są to (od góry): nazwa wyróżniająca właściciela, klucz publiczny właściciela, nazwa wyróżniająca wystawcy (CA) oraz podpis wystawcy.

Poniższa lista dokładniej opisuje budowę certyfikatu cyfrowego:

Nazwa wyróżniająca właściciela
Kombinacja powszechnej nazwy właściciela oraz kontekst (pozycja) w drzewie katalogów. W poniższym przykładzie prostego drzewa, Prasad jest powszechną nazwą właściciela, a kontekstem jest kraj=US, organizacja=ABC, podorganizacja=SERV; nazwą wyróżniającą jest więc:

```
/C=US/O=ABC/OU=SERV/CN=prasad.austin.ibm.com
```



Rysunek 11. Przykład pobierania nazwy wyróżniającej (DN) z drzewa katalogów

Na ilustracji przedstawiono drzewo katalogów z O=ABC na samym szczycie i odgałęzieniami na dwie jednostki znajdujące się na drugim poziomie. Poziom drugi składa się z OU=AIX i OU=Acctg na oddzielnych gałęziach; każda z nich ma gałąź prowadzącą do pojedynczej jednostki znajdującej się na ostatnim poziomie. Ostatni poziom zawiera odpowiednio CN=Prasad i CN=Peltier.

Klucz publiczny właściciela
Klucz używany przez odbiorcę do deszyfrowania danych.

Nazwa alternatywna podmiotu
Może to być identyfikator np. adres IP, adres poczty e-mail, pełna nazwa domeny itp.

Data wydania
Data wydania certyfikatu cyfrowego.

Data ważności
Data utraty ważności certyfikatu cyfrowego.

Nazwa wyróżniająca wystawcy
Nazwa wyróżniająca ośrodka certyfikacji.

Podpis cyfrowy wystawcy
Podpis cyfrowy używany w celu sprawdzania poprawności certyfikatu.

Uwagi na temat bezpieczeństwa certyfikatów cyfrowych
Sam certyfikat cyfrowy nie może być potwierdzeniem tożsamości.

Pozwala on jedynie sprawdzić tożsamość jego właściciela przez udostępnienie klucza publicznego, który jest potrzebny w celu sprawdzenia podpisu cyfrowego właściciela. Klucz publiczny można bezpiecznie przesłać innej osobie, ponieważ danych nie da się odszyfrować bez drugiej części pary kluczy – klucza prywatnego. Właściciel więc musi chronić klucz prywatny, który razem z kluczem publicznym tworzy parę kluczy w danym certyfikacie cyfrowym. Jeśli klucz prywatny jest znany, cała komunikacja właściciela certyfikatu cyfrowego może być deszyfrowana. Bez klucza prywatnego certyfikat cyfrowy nie może być źle użyty.

Ośrodki certyfikacji i hierarchie zaufania
Certyfikat cyfrowy jest pewny wtedy, gdy pewny jest ośrodek certyfikacji, który go wystawia.

Niezbędne jest zrozumienie strategii, według której wystawiane są certyfikaty. Każda organizacja lub użytkownik musi określić, które ośrodki certyfikacji mogą być zaakceptowane jako godne zaufania.

Narzędzie Key Manager (Menedżer kluczy) pozwala także tworzyć certyfikaty samopodpisane, które mogą być przydatne zarówno do testowania, jak i w środowiskach z niewielką liczbą użytkowników lub komputerów.

Użytkownik usługi bezpieczeństwa, aby otrzymywać i sprawdzać poprawność jakichkolwiek certyfikatów cyfrowych, musi znać swój klucz publiczny. Otrzymanie certyfikatu cyfrowego nie zapewnia jego autentyczności. Aby to sprawdzić, potrzebny jest klucz publiczny ośrodka certyfikacji, który wystawił dany certyfikat. Jeśli użytkownik nie ma jeszcze zabezpieczonej kopii klucza publicznego ośrodka certyfikacji, będzie musiał pobrać dodatkowy certyfikat cyfrowy, aby ten klucz otrzymać.

Listy odwołań certyfikatów
Certyfikat cyfrowy powinien być możliwy do wykorzystania przez cały jego okres ważności. Jeśli jednak zachodzi taka potrzeba, może on być unieważniony przed terminem.

Unieważnienie certyfikatu może być konieczne na przykład w przypadku, gdy pracownik opuszcza firmę lub jeśli klucz prywatny certyfikatu został przechwycony. Aby unieważnić certyfikat, należy powiadomić ośrodek certyfikacji o zaistniałych okolicznościach. Jeśli ośrodek certyfikacji odwoła certyfikat, jego numer seryjny zostaje dodany do listy odwołań certyfikatów (CRL).

Listy CRL są to podpisane struktury danych, które są wystawiane okresowo i oddawane do użytku publicznego. Można je pobrać z serwerów HTTP lub LDAP. Każda lista CRL zawiera aktualny datownik oraz datownik nextUpdate (następna aktualizacja). Każdy unieważniony certyfikat jest identyfikowany na liście przez swój numer seryjny.

Podczas konfigurowania tunelu IKE i korzystania z certyfikatów cyfrowych jako metody uwierzytelniania, za pomocą podpisu RSA wraz ze sprawdzaniem listy CRL można potwierdzić, że certyfikat nie został unieważniony. Jeśli opcja sprawdzania listy CRL jest włączona, to podczas procesu negocjacji do ustanowienia tunelu zarządzania kluczem, lista jest wyszukiwana i sprawdzana.

> **Uwaga:** Aby korzystać z tej opcji bezpieczeństwa IP, system musi być skonfigurowany do korzystania z serwera SOCKS (dla serwerów HTTP jest to wersja 4), serwera LDAP lub obu serwerów. Jeśli wiadomo, który serwer SOCKS lub LDAP jest używany do otrzymywania list CRL, można dodać je do pliku `/etc/isakmpd.conf`.

Używanie certyfikatów cyfrowych w aplikacjach internetowych

Aplikacje internetowe, które używają systemów kryptograficznych opartych na kluczu publicznym, muszą używać certyfikatów cyfrowych, aby te klucze uzyskać.

Istnieje wiele aplikacji, które korzystają z kryptografii opartej na kluczu publicznym. Są to na przykład:

Sieci VPN (Virtual Private Networks)
Sieci VPN, zwane również *bezpiecznymi tunelami* , które mogą być ustanowione między dwoma systemami, takimi jak firewalle, w celu zapewnienia zabezpieczonych połączeń między chronionymi sieciami przez niechronione łącza komunikacyjne. Wszelka komunikacja, przeznaczona dla tych sieci, jest szyfrowana między uczestniczącymi systemami.

Protokoły wykorzystywane w tunelach wynikają z bezpieczeństwa IP i standardów IKE, co pozwala na tworzenie bezpiecznych, szyfrowanych połączeń między klientem zdalnym (na przykład pracownikiem pracującym w domu), a bezpiecznym hostem lub siecią.

Warstwa SSL (Secure Sockets Layer)
Warstwa SSL jest protokołem, który zapewnia prywatność i integralność komunikacji. Jest on używany przez serwery WWW do chronionych połączeń między serwerami a przeglądarkami WWW, przez protokół LDAP (Lightweight Directory Access Protocol) do bezpiecznych połączeń między klientami a serwerami LDAP i przez systemy Host-on-Demand V.2 do połączeń między klientami a systemem hosta. Warstwa SSL używa certyfikatów cyfrowych do wymiany klucza, uwierzytelniania serwera i opcjonalnie do uwierzytelniania klienta.

Zabezpieczona poczta elektroniczna
Wiele systemów poczty elektronicznej, używających standardów, takich jak PEM lub S/MIME, w celu zapewnienia bezpiecznej poczty elektronicznej, korzysta z certyfikatów cyfrowych do podpisów cyfrowych i do wymiany kluczy szyfrujących i deszyfrujących wiadomości.

Certyfikaty cyfrowe a żądania certyfikatów

Aby zgłosić żądanie certyfikatu cyfrowego, należy utworzyć i wysłać do ośrodka CA *żądanie certyfikatu*.

Podpisany certyfikat cyfrowy zawiera pola z nazwą wyróżniającą właściciela, jego kluczem publicznym, nazwą wyróżniającą ośrodek certyfikacji i podpisem tego ośrodka. Samopodpisany certyfikat cyfrowy zawiera nazwę wyróżniającą jego właściciela, klucz publiczny i podpis.

Żądanie certyfikatu zawiera pola z nazwą wyróżniającą requestera, kluczem publicznym i podpisem. Ośrodek CA, za pomocą klucza publicznego w certyfikacie cyfrowym, sprawdza podpis requestera, aby upewnić się, że:

- żądanie certyfikatu nie zostało zmodyfikowane podczas przesyłania od requestera do ośrodka CA,
- requester posiada odpowiadający kluczowi publicznemu klucz prywatny, który został zawarty w żądaniu certyfikatu.

Ośrodek CA jest odpowiedzialny także za sprawdzenie do pewnego poziomu tożsamości requestera. Wymagania dotyczące weryfikacji mogą mieć zakres od bardzo małego dowodu do absolutnej pewności co do tożsamości właściciela.

Narzędzie Key Manager (Menedżer kluczy)

Narzędzie Key Manager (Menedżer kluczy) zarządza certyfikatami cyfrowymi. Znajduje się ono w zestawie plików `gskkm.rte` w pakiecie rozszerzenia.

Aby skonfigurować obsługę certyfikatów cyfrowych i podpisu, należy wykonać co najmniej zadania 1, 2, 3, 4, 6 i 7. Następnie należy utworzyć tunel IKE i powiązania z tunelem strategii, która wykorzystuje podpis RSA jako metodę uwierzytelniania.

Bazę danych kluczy można utworzyć i skonfigurować za pomocą komendy certmgr, służącej do uruchomienia narzędzia Key Manager (Menedżer kluczy) z poziomu wiersza komend.

W tej sekcji opisano, w jaki sposób korzystać z narzędzia Key Manager (Menedżer kluczy) w celu wykonania następujących zadań:

Tworzenie bazy danych kluczy
Baza danych kluczy umożliwia punktom końcowym sieci VPN nawiązywanie połączeń się przy wykorzystaniu poprawnych certyfikatów cyfrowych. W sieciach VPN bezpieczeństwa IP jest używany format bazy danych kluczy (*.kdb).

Narzędzie Key Manager (Menedżer kluczy) udostępnia następujące rodzaje certyfikatów cyfrowych:

- RSA Secure Server Certification Authority
- Thawte Personal Premium Certification Authority
- Thawte Personal Freemail Certification Authority
- Thawte Personal Basic Certification Authority
- Thawte Personal Server Certification Authority
- Thawte Server Certification Authority
- Verisign Class 1 Public Primary Certification Authority
- Verisign Class 2 Public Primary Certification Authority
- Verisign Class 3 Public Primary Certification Authority
- Verisign Class 4 Public Primary Certification Authority

Te podpisane certyfikaty cyfrowe umożliwiają klientom podłączanie do serwerów, które mają poprawne certyfikaty cyfrowe pochodzące od środków podpisujących. Po utworzeniu bazy danych kluczy, można ją używać w celu podłączania do serwera, który ma poprawny certyfikat cyfrowy, pochodzący od jednego z ośrodków podpisujących.

Aby korzystać z podpisanego certyfikatu cyfrowego, którego nie ma na liście, należy wysłać żądanie do ośrodka certyfikacji i dodać go do bazy danych kluczy. Więcej informacji na ten temat zawiera sekcja “Dodawanie głównego certyfikatu cyfrowego ośrodka CA” na stronie 249.

Aby korzystając z komendy **certmgr** utworzyć bazę danych kluczy, użyj następującej procedury:

1. Uruchom narzędzie Key Manager (Menedżer kluczy) wpisując:

   ```
   # certmgr
   ```

2. Z listy Key Database File (Plik bazy danych kluczy) wybierz polecenie **New** (Nowy).
3. Dla pola **Key database type** (Typ bazy danych) zaakceptuj wartość domyślną - CMS key database file (Plik CMS bazy danych kluczy).
4. W polu **File Name** (Nazwa pliku) wpisz następującą nazwę pliku:

   ```
   ikekey.kdb
   ```

5. W polu **Location** (Położenie) wpisz następującą ścieżkę do bazy danych:

   ```
   /etc/security
   ```

   Uwaga: Baza danych kluczy musi być nazwana `ikekey.kbd` i musi być umieszczona w katalogu `/etc/security`. W przeciwnym razie bezpieczeństwo IP nie będzie działać poprawnie.
6. Kliknij **OK**. Wyświetli się ekran **Password Prompt** (Podaj hasło).
7. W polu **Password** (Hasło) wpisz hasło i potwierdź je w polu **Confirm Password** (Potwierdzenie hasła).
8. Jeśli chcesz zmienić liczbę dni, po których hasło straci ważność, podaj żądaną liczbę dni w polu **Set expiration time?** (Ustaw datę ważności). Wartość domyślna dla tego pola to 60 dni. Jeśli nie chcesz, aby hasło utraciło ważność, anuluj zaznaczenie pola **Set expiration time?** (Ustaw datę ważności).
9. Aby zachować zaszyfrowaną wersję hasła w pliku ukrytych haseł, zaznacz pole **Stash the password to a file?** (Zeskładuj hasło do pliku) i wpisz Yes (Tak).

   Uwaga: Aby bezpieczeństwo IP mogło korzystać z certyfikatów cyfrowych, hasło trzeba zeskładować.
10. Kliknij **OK**. Pojawi się ekran potwierdzenia, informujący, że utworzona została baza danych kluczy.

11. Kliknij ponownie **OK**, aby powrócić do ekranu IBM Key Management (Zarządzanie kluczami IBM). Możesz wykonać inne zadania lub wyjść z narzędzia.

Dodawanie głównego certyfikatu cyfrowego ośrodka CA
Po zgłoszeniu żądania i otrzymaniu głównego certyfikatu cyfrowego z ośrodka CA, można go dodać do bazy danych.

Większość głównych certyfikatów cyfrowych jest w formacie *.arm, tak jak w następującym przykładzie:

```
cert.arm
```

Aby dodać główny certyfikat cyfrowy ośrodka CA do bazy danych, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

   ```
   # certmgr
   ```

2. Na głównym ekranie, z listy Key Database File (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy, do którego chcesz dodać główny certyfikat cyfrowy ośrodka CA, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu IBM Key Management (Zarządzanie kluczami IBM). Pasek tytułu pokazuje teraz nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty i można z nim pracować.
5. Z listy **Personal/Signer Certificates** (Certyfikaty osobiste/podpisującego) wybierz **Signer Certificates** (Certyfikaty podpisującego).
6. Kliknij **Add** (Dodaj).
7. Z listy **Data type** (Typ danych) wybierz typ danych, na przykład:

   ```
   Base64-encoded ASCII data (dane Base64-encoded ASCII)
   ```

8. Podaj nazwę pliku certyfikatu oraz położenie głównego certyfikatu cyfrowego ośrodka CA lub kliknij **Browse** (Przeglądaj), aby wybrać nazwę i położenie.
9. Kliknij **OK**.
10. Podaj etykietę dla głównego certyfikatu cyfrowego ośrodka CA, na przykład `Test głównego certyfikatu ośrodka CA` i kliknij **OK**. Program powróci do ekranu **Key Management** (Zarządzanie kluczami). Pole **Signer Certificates** (Certyfikaty podpisującego) pokazuje teraz etykietę dodanego głównego certyfikatu cyfrowego ośrodka CA. Możesz wykonać inne zadania lub wyjść z narzędzia.

Ustalanie ustawień zaufania
Domyślnie instalowane certyfikaty ośrodka CA są ustawiane jako zaufane. W razie potrzeby można zmienić ustawienia dotyczące relacji zaufania.

Aby zmienić ustawienia zaufania, wykonaj następujące czynności:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

   ```
   # certmgr
   ```

2. Na głównym ekranie, z listy **Key Database File** (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy, w którym chcesz zmienić domyślny certyfikat cyfrowy, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Pasek tytułu pokazuje nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty.
5. Z listy **Personal/Signer Certificates** (Certyfikaty osobiste/podpisującego) wybierz **Signer Certificates** (Certyfikaty podpisującego).

6. Zaznacz certyfikat, który chcesz zmienić, i kliknij **View/Edit** (Przeglądaj/Edytuj) lub kliknij dwukrotnie pozycję. Dla pozycji danego certyfikatu wyświetlony zostanie ekran **Key Information** (Informacje o kluczu).
7. Aby uczynić dany certyfikat głównym certyfikatem zaufanym, zaznacz pole **Set the certificate as a trusted root** (Ustaw certyfikat jako główny zaufany) i kliknij **OK**. Jeśli certyfikat nie ma być zaufany, anuluj zaznaczenie pola i kliknij **OK**.
8. Kliknij **OK** na ekranie **Signer Certificates** (Certyfikaty podpisującego). Program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Możesz wykonać inne zadania lub wyjść z narzędzia.

Usuwanie głównego certyfikatu cyfrowego ośrodka CA
Jeśli jeden z ośrodków CA nie ma być dłużej używany na liście podpisanych certyfikatów cyfrowych, należy usunąć główny certyfikat cyfrowy tego ośrodka CA.

Uwaga: Przed usunięciem głównego certyfikatu cyfrowego ośrodka CA należy utworzyć jego kopię zapasową, na wypadek gdyby zaszła potrzeba jego odtworzenia.

Aby usunąć główny certyfikat cyfrowy ośrodka CA z bazy danych, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

```
# certmgr
```

2. Na głównym ekranie, z listy **Key Database File** (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy, z którego chcesz usunąć główny certyfikat cyfrowy ośrodka CA, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu **Key Management** (Zarządzanie kluczami). Pasek tytułu pokazuje nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty i można go modyfikować.
5. Z listy **Personal/Signer Certificates** (Certyfikaty osobiste/podpisującego) wybierz **Signer Certificates** (Certyfikaty podpisującego).
6. Zaznacz certyfikat, który chcesz usunąć, i kliknij **Delete** (Usuń). Zostanie wyświetlony ekran **Confirm** (Potwierdź).
7. Kliknij **Yes** (Tak). Program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Etykieta głównego certyfikatu cyfrowego ośrodka CA nie będzie więcej widoczna w polu **Signer Certificates** (Certyfikaty podpisującego). Możesz wykonać inne zadania lub wyjść z narzędzia.

Żądanie certyfikatu cyfrowego
Aby uzyskać certyfikat cyfrowy, za pomocą narzędzia Key Manager (Menedżer kluczy) należy wygenerować żądanie i wysłać je do ośrodka CA. Wygenerowany plik żądania ma format PKCS#10. Ośrodek CA sprawdza tożsamość żądającego i wysyła mu certyfikat cyfrowy.

Aby zażądać certyfikatu cyfrowego, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

```
# certmgr
```

2. Na głównym ekranie, z listy **Key Database File** (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy `/etc/security/ikekey.kdb`, z którego chcesz wygenerować żądanie, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Pasek tytułu pokazuje nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty i można go modyfikować.
5. Wybierz kolejno opcje **Utwórz** > **Nowe żądanie certyfikatu**.
6. Kliknij **New** (Nowy).

7. Na następnym ekranie dla samopodpisanego certyfikatu cyfrowego podaj Key Label (etykietę klucza), taką jak:

```
test_klucza
```

8. Podaj common name (nazwę zwykłą - domyślnie jest to nazwa hosta) i organization (organizację), a następnie wybierz country (kraj). Dla pozostałych pól zaakceptuj wartości domyślne lub wybierz nowe.
9. Podaj subject alternate (nazwę alternatywną podmiotu). Polami opcjonalnymi, powiązanymi z subject alternate (nazwą alternatywną podmiotu) są: adres e-mail, adres IP i nazwa serwera DNS. W polu adresu IP - w przypadku identyfikatora tunelu typu adres IP - wpisz ten sam adres IP, który został skonfigurowany dla tunelu IKE. W przypadku identyfikatora tunelu typu *użytkownik@FQDN* wypełnij pole adresu e-mail. W przypadku identyfikatora tunelu typu nazwa FQDN, w polu nazwy serwera DNS wpisz pełną nazwę domeny (na przykład *nazwa_hosta*.*nazwa_firmy*.com).
10. U dołu ekranu wpisz nazwę pliku, na przykład:

```
certreq.arm
```

11. Kliknij **OK**. Pojawi się ekran potwierdzenia, informujący, że utworzone zostało żądanie nowego certyfikatu cyfrowego.
12. Kliknij **OK**. Program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). W polu **Personal Certificate Requests** (Żądanie certyfikatu cyfrowego) znajduje się teraz etykieta klucza utworzonego żądania nowego certyfikatu cyfrowego (PKCS#10).
13. Wyślij plik do ośrodka CA, aby zażądać nowego certyfikatu cyfrowego. Możesz wykonać inne zadania lub wyjść z narzędzia.

Dodawanie (pobieranie) nowego certyfikatu cyfrowego
Po otrzymaniu z ośrodka z CA nowego certyfikatu cyfrowego trzeba go dodać do bazy danych kluczy, z której zostało wygenerowane żądanie.

Aby dodać (pobrać) nowy certyfikat cyfrowy, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

```
# certmgr
```

2. Na głównym ekranie, z listy **Key Database File** (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy, z którego zostało wygenerowane żądanie certyfikatu, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu IBM Key Management (Zarządzanie kluczami IBM). Pasek tytułu pokazuje nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty i można go modyfikować.
5. Z listy **Personal/Signer Certificates** (Certyfikaty osobiste/podpisującego) wybierz **Personal Certificate Requests** (Żądania certyfikatu osobistego).
6. Kliknij **Receive** (Pobierz), aby do bazy danych dodać nowo pobrany certyfikat cyfrowy.
7. Z listy **Data type** (Typ danych) wybierz typ danych nowego certyfikatu cyfrowego. Domyślnie jest to typ **Base64-encoded ASCII data** (dane Base64-encoded ASCII).
8. Podaj nazwę pliku certyfikatu oraz położenie nowego certyfikatu cyfrowego lub kliknij **Browse** (Przeglądaj), aby wybrać nazwę i położenie.
9. Kliknij **OK**.
10. Dla nowego certyfikatu wpisz etykietę opisową, taką jak:

```
Certyfikat oddziału sieci VPN
```

11. Kliknij **OK**. Program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Pole **Personal Certificates** (Certyfikaty osobiste) pokazuje teraz etykietę dodanego nowego certyfikatu cyfrowego. Możesz wykonać inne zadania lub wyjść z narzędzia.

Jeśli podczas ładowania certyfikatu wystąpił błąd, sprawdź, czy plik certyfikatu zaczyna się od tekstu —-BEGIN CERTIFICATE—- i kończy się tekstem —-END CERTIFICATE—-.

Na przykład:

```
-----BEGIN CERTIFICATE-----
ajdkfjaldfwwwwwwwwwwadafdw
kajf;kdsajkflasasfkjafdaff
akdjf;ldasjkf;safdfdasfdas
kaj;fdljk98dafdas43adfadfa
-----END CERTIFICATE-----
```

Jeśli tak nie jest, zmień plik certyfikatu, tak aby odpowiednio się zaczynał i kończył.

Usuwanie certyfikatu cyfrowego
Czasami konieczne jest usunięcie certyfikatu cyfrowego.

Uwaga: Przed usunięciem certyfikatu cyfrowego należy utworzyć jego kopię zapasową, na wypadek gdyby zaszła potrzeba jego odtworzenia.

Aby usunąć certyfikat cyfrowy z bazy danych, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

   ```
   # certmgr
   ```

2. Na głównym ekranie, z listy **Key Database File** (Plik bazy danych kluczy) wybierz polecenie **Open** (Otwórz).
3. Zaznacz plik bazy danych kluczy, z którego chcesz usunąć certyfikat cyfrowy, i kliknij **Open** (Otwórz).
4. Podaj hasło i kliknij **OK**. Po zaakceptowaniu hasła program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Pasek tytułu pokazuje nazwę wybranego pliku bazy danych kluczy, wskazując, że plik jest otwarty i można go modyfikować.
5. Z listy **Personal/Signer Certificates** (Certyfikaty osobiste/podpisującego) wybierz **Personal Certificate Requests** (Żądania certyfikatu osobistego).
6. Zaznacz certyfikat cyfrowy, który chcesz usunąć, i kliknij **Delete** (Usuń). Zostanie wyświetlony ekran **Confirm** (Potwierdź).
7. Kliknij **Yes** (Tak). Program powróci do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Etykieta certyfikatu cyfrowego nie będzie więcej widoczna w polu **Personal Certificates** (Certyfikaty osobiste). Możesz wykonać inne zadania lub wyjść z narzędzia.

Zmiana hasła bazy danych
Czasami konieczna jest zmiana hasła bazy danych.

Aby zmienić bazę danych kluczy, użyj następującej procedury:

1. Jeśli narzędzie Key Manager (Menedżer kluczy) nie jest jeszcze uruchomione, uruchom je, wpisując:

   ```
   # certmgr
   ```

2. Na głównym ekranie wybierz polecenie **Change Password** (Zmień hasło) z listy **Key Database File** (Plik bazy danych).
3. W polu **Password** (Hasło) wpisz nowe hasło i potwierdź je w polu **Confirm Password** (Potwierdzenie hasła).
4. Jeśli chcesz zmienić liczbę dni, po których hasło straci ważność, podaj żądaną liczbę dni w polu **Set expiration time?** (Ustaw datę ważności). Wartość domyślna dla tego pola to 60 dni. Jeśli nie chcesz, aby hasło utraciło ważność, anuluj zaznaczenie pola **Set expiration time?** (Ustaw datę ważności).
5. Aby zachować zaszyfrowaną wersję hasła w pliku ukrytych haseł, zaznacz pole **Stash the password to a file?** (Zeskładuj hasło do pliku) i wpisz Yes (Tak).

   Uwaga: Aby bezpieczeństwo IP mogło korzystać z certyfikatów cyfrowych, hasło trzeba zeskładować.
6. Kliknij **OK**. Komunikat pojawiający się na pasku stanu informuje, że operacja zakończyła się pomyślnie.

7. Kliknij ponownie **OK**, aby powrócić do ekranu **IBM Key Management** (Zarządzanie kluczami IBM). Możesz wykonać inne zadania lub wyjść z narzędzia.

Tworzenie tuneli IKE wykorzystujących certyfikaty cyfrowe
Aby utworzyć tunele IKE, które wykorzystują certyfikaty cyfrowe, należy określić podpisy RSA jako tryb uwierzytelniania w pliku strategii transformacji tunelu IKE.

W poniższym przykładzie przedstawiono plik strategii XML określający podpisy RSA:

```
<!-- definiowanie strategii dla tunelu IKE -->
<IKEProtection
    IKE ProtectionName="ike_3des_sha">
    <IKETTransform
        IKE AuthenticationMethod="RSA_signatures"
        IKE Encryption="3DES-CBC"
        IKE Hash="SHA"
        IKE DHGroup="1"/>
</IKEProtection>
```

Bezpieczeństwo IP obsługuje następujące typy tożsamości hostów tuneli IKE:

- adres IP,
- pełna nazwa domeny (Fully Qualified Domain Name - FQDN),
- adres *użytkownik*@*FQDN*.
- nazwa wyróżniająca X.500,
- identyfikator klucza.

Gdy tunel IKE używa trybu podpisu RSA, w definicji tunelu IKE zwykle używane są nazwy wyróżniające X.500. Jeśli na przykład hosty lokalne i zdalne tunelu to **/C=US/O=ABC/OU=SERV/CN=localname.austin.ibm.com** i **/C=US/O=ABC/OU=SERV/CN=remotename.austin.ibm.com**, definicja tego tunelu IKE w pliku XML ma następującą treść:

```
<IKETunnel>
    IKE TunnelName="Key_Tunnel"
    IKE ProtectionRef="ike_3des_sha">
<IKELocalIdentity>
    <ASN1_DN Value="/C=US/O=ABC/OU=SERV/CN=localname.austin.ibm.com">
    </ASN1_DN>
</IKELocalIdentity>
<IKERemoteIdentity>
    <ASN1_DN Value="/C=US/O=ABC/OU=SERV/CN=remotename.austin.ibm.com">
    </ASN1_DN>
</IKERemoteIdentity>
</IKETunnel>
```

Aby uzyskać wymagany certyfikat z ośrodka certyfikacji (CA), należy użyć narzędzia Key Manager (Menedżer kluczy) do wygenerowania żądania certyfikatu. Jeśli na przykład nazwą wyróżniającą podmiotu w certyfikacie jest **/C=US/O=ABC/OU=SERV/CN=name.austin.ibm.com**, w narzędziu Key Manager podczas tworzenia żądania certyfikatu cyfrowego należy wprowadzić następujące wartości:

Nazwa zwykła
name.austin.ibm.com

Organizacja
ABC

Jednostka organizacyjna
SERV

Kraj
US

Wprowadzana nazwa wyróżniająca X.500 jest nazwą zwykle ustawioną przez system lub administratora LDAP. Wartość jednostki organizacyjnej jest opcjonalna.

Bezpieczeństwo IP obsługuje także wprowadzanie w certyfikacie cyfrowym innych typów tożsamości, takich jak alternatywne nazwy podmiotu. Jeśli na przykład adres IP 10.10.10.1 zostanie użyty jako alternatywna tożsamość hosta, w żądaniu certyfikatu cyfrowego należy wprowadzić następujące wartości:

Nazwa zwykła
name.austin.ibm.com

Organizacja
ABC

Jednostka organizacyjna
SERV

Kraj
US

Pole alternatywnego adresu IP podmiotu
10.10.10.1

Po utworzeniu za pomocą tych informacji żądania certyfikatu cyfrowego, ośrodek CA wykorzysta je do utworzenia osobistego certyfikatu cyfrowego.

Aby przyjąć żądanie osobistego certyfikatu cyfrowego, ośrodek CA wymaga następujących informacji:

- certyfikatu X.509,
- formatu podpisu MD5 z szyfrowaniem RSA,
- czy określana będzie nazwa alternatywna podmiotu; typy nazw alternatywnych to:
  - adres IP,
  - pełna nazwa domeny (Fully Qualified Domain Name - FQDN),
  - adres *użytkownik*@*FQDN*.

  W pliku żądania certyfikatu załączane są następujące informacje dotyczące nazwy alternatywnej podmiotu:
- użycie planowanego klucza (musi być wybrany bit podpisu cyfrowego),
- plik żądania certyfikatu cyfrowego narzędzia Key Manager (Menedżer kluczy) (w formacie PKCS#10).

Instrukcje dotyczące sposobu używania programu Key Manager (Menedżer kluczy) do tworzenia żądania certyfikatu zawiera sekcja “Żądanie certyfikatu cyfrowego” na stronie 250.

Przed aktywowaniem tunelu IKE należy dodać otrzymany z ośrodka CA osobisty certyfikat cyfrowy do bazy danych narzędzia Key Manager (Menedżer kluczy) `ikekey.kdb`. Więcej informacji na ten temat zawiera sekcja “Dodawanie (pobieranie) nowego certyfikatu cyfrowego” na stronie 251.

Bezpieczeństwo IP obsługuje następujące rodzaje osobistych certyfikatów cyfrowych:

Nazwa wyróżniająca podmiotu
Nazwa wyróżniająca podmiotu musi mieć następujący format:

```
/C=US/O=ABC/OU=SERV/CN=nazwa.austin.ibm.com
```

Narzędzie Key Manager (Menedżer kluczy) dopuszcza jedynie wartość **OU**.

Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu jako adres IP
Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu może być wskazana jako adres IP:

`/C=US/O=ABC/OU=SERV/CN=nazwa.austin.ibm.com` i `10.10.10.1`

Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu jako nazwa FQDN
Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu może być wskazana jako pełna nazwa domeny:

`/C=US/O=ABC/OU=SERV/CN=nazwa.austin.ibm.com` i `bell.austin.ibm.com`.

Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu jako adres *użytkownik*@*FQDN*
Nazwa wyróżniająca podmiotu i nazwa alternatywna podmiotu może być wskazana jako adres użytkownika (*ID_użytkownika*@*pełna_nazwa_domeny*):

`/C=US/O=ABC/OU=SERV/CN=nazwa.austin.ibm.com` i `nazwa@austin.ibm.com`.

Nazwa wyróżniająca podmiotu i wiele nazw alternatywnych podmiotu

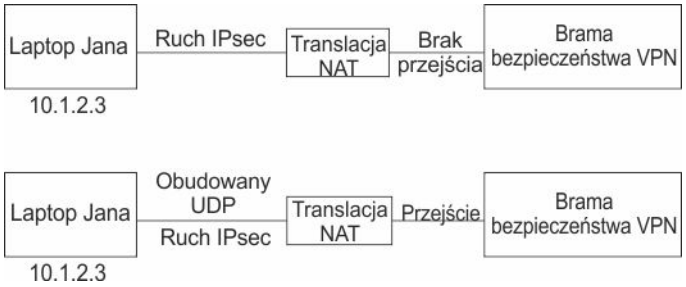
Nazwa wyróżniająca podmiotu może być powiązana z wieloma nazwami alternatywnymi podmiotu:

`/C=US/O=ABC/OU=SERV/CN=nazwa.austin.ibm.com` i `bell.austin.ibm.com`, `10.10.10.1` i `użytkownik@nazwa.austin.ibm.com`.

Translacja adresów sieciowych

Opcja bezpieczeństwa IP może korzystać z urządzeń, których adresy podlegają translacji adresów sieciowych (Network Address Translation - NAT).

Translacja NAT jest szeroko stosowana jako składnik technologii firewall udostępniania połączeń internetowych i jest standardowym elementem routerów oraz urządzeń granicznych. Protokół bezpieczeństwa IP jest uzależniony od identyfikowania komputerów końcowych oraz ich strategii opartej na zdalnym adresie IP. Podczas translacji prywatnego adresu na adres publiczny przez urządzenie pośrednie, takie jak router czy firewall, wymagane przetwarzanie uwierzytelniania w bezpieczeństwie IP może się nie powieść, ponieważ po obliczeniu skrótu uwierzytelniania został zmieniony adres w pakiecie IP. W nowej obsłudze bezpieczeństwa IP dla translacji NAT, skonfigurowane za węzłem urządzenia przeprowadzające translację adresu sieciowego są w stanie ustanowić bezpieczny tunel IP. Kod bezpieczeństwa IP jest w stanie wykryć translację zdalnego adresu. Używanie nowej implementacji bezpieczeństwa IP z obsługą translacji NAT umożliwia klientom sieci VPN łączenie się z biurem - przy użyciu połączenia internetowego z włączoną translacją NAT - z domu lub podczas podróży.



Rysunek 12. Bezpieczeństwo IP z włączoną translacją NAT

Diagram ten pokazuje różnicę pomiędzy implementacją bezpieczeństwa IP z włączoną translacją NAT wraz z ruchem obudowanym protokołem UDP, a implementacją bez włączonej translacji NAT.

Konfigurowanie bezpieczeństwa IP do pracy z translacją NAT

Aby używać translacji NAT w funkcji bezpieczeństwa IP, należy ustawić zmienną *ENABLE_IPSEC_NAT_TRAVERSAL* w pliku `/etc/isakmpd.conf`. Po ustawieniu tej zmiennej zostanie dodana reguła filtrowania, która powoduje wysyłanie i odbiór ruchu przez port 4500.

Następujący przykład pokazuje reguły filtrowania po ustawieniu zmiennej *ENABLE_IPSEC_NAT_TRAVERSAL* .

```
Dynamic rule 2:
Rule action          : permit
Source Address      : 0.0.0.0 (any)
Source Mask         : 0.0.0.0 (any)
Destination Address : 0.0.0.0 (any)
Destination Mask    : 0.0.0.0 (any)
Source Routing      : no
Protocol             : udp
Source Port         : 0 (any)
Destination Port    : 4500
Scope               : local
Direction            : inbound
Fragment control     : all packets
Tunnel ID number     : 0

Dynamic rule 3:
Rule action          : permit
Source Address      : 0.0.0.0 (any)
Source Mask         : 0.0.0.0 (any)
Destination Address : 0.0.0.0 (any)
Destination Mask    : 0.0.0.0 (any)
```

```
Source Routing      : no
Protocol             : udp
Source Port         : 4500
Destination Port    : 0 (any)
Scope               : local
Direction             : outbound
Fragment control     : all packets
Tunnel ID number     : 0
```

Ustawienie zmiennej *ENABLE_IPSEC_NAT_TRAVERSAL* powoduje także dodanie dodatkowych reguł filtrowania do tabeli filtru. Specjalne komunikaty bezpieczeństwa IP w translacji NAT używają hermetyzacji UDP i aby umożliwić przepływ ruchu, należy dodać pewne reguły filtrowania. Ponadto w fazie 1 wymagany jest tryb sygnatury. Jeśli w certyfikacie jako identyfikator używany jest adres IP, powinien on zawierać prywatny adres IP.

Bezpieczeństwo IP wymaga także wysyłania komunikatów sprawdzających połączenie translacji NAT, aby obsłużyć przypisanie oryginalnych adresów IP do adresów po translacji NAT. Odstęp czasu jest określony przez zmienną *NAT_KEEPALIVE_INTERVAL* w pliku `/etc/isakmpd.conf`. Zmienna ta określa w sekundach częstotliwość wysyłania pakietów sprawdzających połączenie translacji NAT. Jeśli wartość *NAT_KEEPALIVE_INTERVAL* nie zostanie podana, zostanie użyta wartość domyślna: 20 sekund.

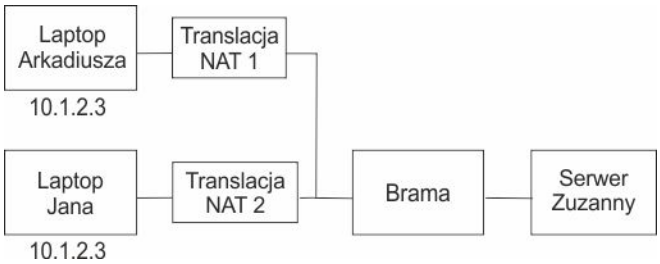
Ograniczenia podczas stosowania wymiany NAT
Komputery końcowe za urządzeniami NAT muszą chronić swój ruch, używając protokołu ESP.

ESP jest dominującym nagłówkiem wybranym dla bezpieczeństwa IP, który jest też używany przez większość aplikacji klienta. ESP wykonuje kodowanie mieszające danych użytkownika, lecz bez nagłówka IP. Sprawdzanie integralności w nagłówku AH włącza także źródłowe i docelowe adresy IP w proces sprawdzania integralności zaszyfrowanej wiadomości. Urządzenia translacji NAT lub translacji odwrotnej NAT, które zmieniają pola adresu, powodują błąd sprawdzania integralności komunikatu. Dlatego, jeśli w fazie 2 strategii dla tunelu zostanie zdefiniowany protokół AH i podczas wymiany fazy 1 zostanie wykryta translacja NAT, zostanie wysłane powiadomienie o treści `NO_PROPOSAL_CHOSEN`.

Ponadto połączenie używające translacji NAT musi wybrać tryb tunelu, tak aby oryginalne adresy IP zostały obudowane w pakiecie. Tryb transportu i adresy z translacją NAT nie są zgodne. Jeśli zostanie wykryta translacja NAT i w fazie 2 zostanie zadeklarowany tylko tryb transportu, zostanie wysłane powiadomienie o treści `NO_PROPOSAL_CHOSEN`.

Unikanie konfliktów trybu tunelu
Zdalny węzeł sieci może negocjować pozycje, które nakładają się na siebie w bramie. Nakładanie to może powodować konflikty trybu tunelu.

Poniższy rysunek ilustruje konflikt trybu tunelu.



Rysunek 13. Konflikt trybu tunelu

Dla adresu IP 10.1.2.3 brama ma dwa możliwe powiązania bezpieczeństwa (Security Association - SA). Istnienie dwóch zduplikowanych adresów zdalnych powoduje niejasność, dokąd mają być wysłane pakiety przychodzące do serwera. Jeśli zostanie skonfigurowany tunel pomiędzy serwerem Zuzanny a laptopem Arkadiusza, zostanie użyty adres IP, który z kolei nie może zostać użyty do skonfigurowania przez Zuzannę tunelu do Roberta. Aby uniknąć konfliktu trybu tunelu, nie należy definiować tunelu z tym samym adresem IP. Ponieważ zdalny adres nie jest kontrolowany przez zdalnego użytkownika, do identyfikacji zdalnego hosta należy użyć innego typu identyfikatora, takiego jak pełna nazwa domeny lub użytkownik z pełną nazwą domeny.

Konfigurowanie tuneli ręcznych
Tunele ręczne bezpieczeństwa IP można skonfigurować wtedy, gdy urządzenia nie obsługują metody z kluczami automatycznymi.

Tunele ręczne i filtry
Proces konfigurowania tunelu polega na zdefiniowaniu tunelu na jednym końcu, importowaniu definicji na drugi koniec i aktywowaniu tunelu oraz reguł filtrowania na obu końcach. Tunel jest wtedy gotowy do użycia.

Aby skonfigurować tunel ręczny, nie jest konieczne oddzielne konfigurowanie reguł filtrowania. Tak długo, jak cały ruch danych jest przesyłany między dwoma hostami przez tunel, niezbędne reguły filtrowania są generowane automatycznie.

Informacje po obu stronach muszą pasować do siebie, jeśli nie są przesyłane jawnie. Na przykład określone dla strony źródłowej algorytmy szyfrowania i uwierzytelniania będą używane dla strony docelowej, jeśli nie zostały określone wcześniej.

Tworzenie tunelu ręcznego na pierwszym hoście
Tunel można skonfigurować za pomocą krótkiej ścieżki programu SMIT `ips4_basic` (dla protokołu IP w wersji 4) lub krótkiej ścieżki programu SMIT `ips6_basic` (dla protokołu IP w wersji 6); można też utworzyć tunel ręcznie przy użyciu poniższej procedury.

Poniżej przedstawiony jest przykład użycia komendy **gentun** do tworzenia tunelu ręcznego:

```
gentun -v 4 -t manual -s 5.5.5.19 -d 5.5.5.8 \
   -a HMAC_MD5 -e DES_CBC_8 -N 23567
```

Za pomocą komendy **lstun -v 4** można przedstawić charakterystyki tunelu ręcznego, utworzonego w poprzednim przykładzie. Wyświetlone zostaną informacje podobne do poniższego przykładu:

```
Tunnel ID            : 1
IP Version           : IP Version 4
Source               : 5.5.5.19
Destination          : 5.5.5.8
Policy               : auth/encr
Tunnel Mode          : Tunnel
Send AH Algo         : HMAC_MD5
Send ESP Algo        : DES_CBC_8
Receive AH Algo      : HMAC_MD5
Receive ESP Algo     : DES_CBC_8
Source AH SPI        : 300
Source ESP SPI       : 300
Dest AH SPI          : 23576
Dest ESP SPI         : 23576
Tunnel Life Time     : 480
Status               : Inactive
Target               : -
Target Mask          : -
Replay               : No
New Header           : Yes
Snd ENC-MAC Algo     : -
Rcv ENC-MAC Algo     : -
```

Aby aktywować tunel, należy wpisać następujący kod:

```
mktun -v 4 -t1
```

Reguły filtrowania związane z tym tunelem zostaną wygenerowane automatycznie.

Aby obejrzeć reguły filtrowania, należy wpisać komendę **lsfilt -v 4**. Wyświetlone zostaną informacje podobne do poniższego przykładu:

```

Rule 4:
Rule action          : permit
Source Address        : 5.5.5.19
Source Mask           : 255.255.255.255
Destination Address   : 5.5.5.8
Destination Mask      : 255.255.255.255
```

```
Source Routing       : yes
Protocol              : all
Source Port           : any 0
Destination Port      : any 0
Scope                : both
Direction             : outbound
Logging control      : no
Fragment control     : all packets
Tunnel ID number      : 1
Interface            : all
Auto-Generated        : yes

Rule 5:
Rule action          : permit
Source Address        : 5.5.5.8
Source Mask           : 255.255.255.255
Destination Address   : 5.5.5.19
Destination Mask      : 255.255.255.255
Source Routing       : yes
Protocol              : all
Source Port           : any 0
Destination Port      : any 0
Scope                : both
Direction             : inbound
Logging control      : no
Fragment control     : all packets
Tunnel ID number      : 1
Interface            : all
Auto-Generated        : yes
```

Aby aktywować reguły filtrowania, także domyślne, należy użyć komendy **mktun -v 4 -t 1**.

Aby skonfigurować drugą stronę (jeśli jest to inny komputer używający tego systemu operacyjnego), definicja tunelu może być eksportowana na hosta A, a następnie importowana na hosta B.

Poniższa komenda eksportuje definicję tunelu do pliku nazwanego **ipsec_tun_manu.exp**, a wszystkie związane z nim reguły filtrowania do pliku **ipsec_fltr_rule.exp**, do katalogu podanego w opcji **-f**:

```
exptun -v 4 -t 1 -f /tmp
```

Tworzenie tunelu ręcznego na drugim hoście
Aby utworzyć odpowiedni koniec tunelu, pliki eksportu są kopiowane, a następnie importowane na komputer zdalny.

Aby utworzyć odpowiedni koniec tunelu, należy użyć komendy:

```
imptun -v 4 -t 1 -f /tmp
```

gdzie

1
jest tunelem, który ma być importowany

/tmp
jest katalogiem, w którym znajdują się pliki importu

Numer tunelu generowany jest przez system. Można go uzyskać z danych wyjściowych komendy **gentun** lub używając komendy **lstun** w celu pokazania listy tuneli, a następnie określając poprawny numer tunelu do importowania. Jeśli w pliku importu jest tylko jeden tunel lub zaimportowane mają być wszystkie tunele, opcja **-t** nie jest potrzebna.

Jeśli komputer zdalny działa pod kontrolą innego systemu, plik eksportu może być wykorzystany jako odniesienie do ustawienia algorytmu, kluczy i wartości interfejsu SPI dla drugiego końca tunelu.

W celu utworzenia tuneli mogą być importowane pliki eksportu spoza firewalla. Aby to zrobić, podczas importowania pliku należy użyć opcji **-n**:

```
imptun -v 4 -f /tmp -n
```

Usuwanie filtrów
Do całkowitego usunięcia filtrów i zatrzymania bezpieczeństwa IP można użyć komendy **rmdev**.

Domyślna reguła filtrowania pozostanie aktywna nawet wtedy, gdy filtrowanie zostanie wyłączone komendą **mkfilt -d**. Komenda ta umożliwia zawieszanie lub usuwanie wszystkich reguł filtrowania oraz ładowanie nowych reguł w czasie, gdy obowiązuje ochrona przy użyciu reguły domyślnej. Domyślną regułą filtrowania jest *DENY*. Gdy filtrowanie zostanie zdezaktywowane komendą **mkfilt -d**, raporty komendy **lsfilt** będą informować, że filtrowanie jest wyłączone, ale ruch pakietów jest niedozwolony ani na zewnątrz, ani do wewnątrz. Aby całkowicie zatrzymać działanie bezpieczeństwa IP, należy użyć komendy **rmdev**.

Konfiguracja filtrów bezpieczeństwa IP
Można skonfigurować filtrowanie proste, używające głównie automatycznie generowanych reguł filtrowania lub można je dostosować przez zdefiniowanie bardzo specyficznych funkcji filtrowania opartych na właściwościach pakietów IP.

Każdy wiersz tabeli filtrowania jest traktowany jako *reguła*. Zbiór reguł określa, które pakiety są akceptowane przez komputer i w jaki sposób są kierowane. Zgodność pakietów przychodzących z regułami filtrowania jest ustalana przez porównywanie adresu źródłowego i wartości interfejsu SPI z informacjami wymienionymi w tabeli filtrowania. Dlatego pary te muszą być unikalne. Reguły filtrowania mogą kontrolować wiele aspektów komunikacji, w tym: adresy oraz maski źródłowe i docelowe, protokół, numer portu, kierunek, kontrolę fragmentu, routing źródłowy, tunel, a także rodzaj interfejsu.

Istnieją następujące rodzaje reguł filtrowania:

- Statyczne reguły filtrowania są tworzone w tabeli filtrowania na potrzeby ogólnego filtrowania ruchu danych lub tworzenia powiązań z tunelami ręcznymi. Mogą być dodawane, usuwane, modyfikowane lub przenoszone. W celu identyfikowania określonej reguły można dodać pole tekstowe z opisem.
- Automatycznie generowane reguły filtrowania oraz reguły filtrowania określone przez użytkownika (zwane również *automatycznie wygenerowanymi* regułami filtrowania) stanowią określony zestaw reguł utworzonych w celu wykorzystania przez tunele IKE. Zarówno statyczne, jak i dynamiczne reguły filtrowania są tworzone w oparciu o informacje tunelu zarządzania danymi i negocjację tunelu zarządzania danymi.
- Predefiniowane reguły filtrowania są ogólnymi regułami filtrowania, które nie mogą być modyfikowane, przenoszone ani usuwane. Są to takie reguły, jak reguła `całej komunikacji` , reguła ah i reguła esp. Odnoszą się one do całej komunikacji.

Opcja kierunku (**-w**) komendy **genfilt** umożliwia określenie, kiedy dana reguła ma być stosowana; podczas przetwarzania pakietów wejściowych, czy też przetwarzania pakietów wyjściowych. Wartość **both** (obydwa kierunki) wskazuje, że reguła ta jest wykorzystywana podczas przetwarzania pakietów wejściowych i wyjściowych. Kiedy włączone jest filtrowanie w bezpieczeństwie IP systemu AIX, przynajmniej jedna reguła określa los każdego pakietu sieciowego (zarówno wejściowego, jak i wyjściowego). Jeśli pewna reguła powinna być stosowana wyłącznie podczas przetwarzania pakietu przychodzącego (lub wychodzącego), można w tym celu użyć przełącznika **-w** komendy **genfilt**. Na przykład, kiedy pakiet jest wysyłany z hosta A do hosta B, wychodzący pakiet IP zawiera adres źródłowy *A* oraz adres docelowy *B*. Na hoście A pakiet ten zostaje przetworzony przez filtr IPsec podczas przetwarzania wyjściowego, a na hoście B podczas przetwarzania wejściowego. Jeśli pomiędzy hostem A i hostem B znajduje się brama G, na bramie tej ten sam pakiet (w którym wszystkie niezmienne pola mają te same wartości) zostaje przetworzony dwukrotnie: raz podczas przetwarzania wejściowego i raz podczas wyjściowego (jeśli ustawiona jest opcja **ipforwarding**). Aby umożliwić pakietowi pokonanie trasy od hosta A do hosta B przez bramę G, należy określić regułę zezwalającą:

- Na hoście A – **src addr** (adres źródłowy) ustawiony na A, **dest addr** (adres docelowy) ustawiony na B, kierunek wychodzący
- Na hoście B – **src addr** ustawiony na A, **dest addr** ustawiony na B, kierunek przychodzący

Jednakże na bramie G potrzebne są dwie reguły filtrowania:

1. **src addr** ustawiony na A, **dest addr** ustawiony na B, kierunek wychodzący
2. **src addr** ustawiony na A, **dest addr** ustawiony na B, kierunek przychodzący

Powyższe reguły można zastąpić jedną: **src addr** ustawiony na A, **dest addr** ustawiony na B i kierunek w obydwie strony. Dlatego wartość określająca kierunek **both** (w obie strony) jest zwykle stosowana na bramach, na których opcja **ipforwarding** (przekazywanie IP) jest ustawiona na wartość no (nie). Omówiona powyżej konfiguracja stosowana jest wyłącznie w przypadku pakietów pokonujących drogę od hosta A do hosta B przez bramę G. W przypadku pakietów przemieszczających się w przeciwnym kierunku (z hosta B do hosta A przez bramę G) potrzebna jest inna reguła.

Uwaga: Kierunek **both** wskazuje, że powiązana z nim reguła stosowana jest zarówno wobec pakietów przychodzących, jak i wychodzących. Jednak nie oznacza, że regułę tę można stosować, kiedy adresy źródłowy i docelowy zostają zamienione miejscami. Na przykład, kiedy serwer A dysponuje regułą, w której *A* jest adresem źródłowym, *B* - adresem docelowym, a opcja kierunku ma wartość **both**, wtedy *A* jako pakiet przychodzący z adresem źródłowym *B* i docelowym *A* nie jest zgodny z tą regułą. Opcja **both** jest zwykle używana w bramach przekazujących pakiety.

Z tymi regułami filtrowania związane są Maski podsieci, których identyfikatory grupy są związane z regułą filtrowania i opcją konfigurowania host-firewall-host. Poniższe sekcje opisują różne rodzaje reguł filtrowania i związane z nimi opcje.

Filtry IP dla systemu AIX

IPFilter jest pakietem oprogramowania, którego można użyć do zapewnienia translacji adresów sieciowych (translacji NAT) lub usług firewalla.

Oprogramowanie Open Source IPFilter w wersji 4.1.13 zostało przeniesione na platformę systemu AIX i pozostaje spójne z zasadami licencjonowania podanymi w serwisie WWW IP Filter (http://coombs.anu.edu.au/~avalon/). Oprogramowanie IPFilter jest dostarczane w pakiecie rozszerzeń systemu AIX. Pakiet installp o nazwie ipfl zawiera stronę podręcznika i licencję.

W systemie operacyjnym AIX produkt IPFilter jest ładowany jako rozszerzenie jądra, `/usr/lib/drivers/ipf`. W tym pakiecie dostarczane są także pliki binarne **ipf**, **ipfs**, **ipfstat**, **ipmon** i **ipnat**.

Po zainstalowaniu tego pakietu należy uruchomić poniższą komendę, aby załadować rozszerzenie jądra:

```
/usr/lib/methods/cfg_ipf -l
```

Aby usunąć rozszerzenie jądra z pamięci, należy uruchomić następującą komendę:

```
/usr/lib/methods/cfg_ipf -u
```

Jeśli potrzebne jest przekazywanie pakietów, należy pamiętać o włączeniu przekazywania IP (opcja network). Więcej informacji na temat programu IPFilter, w tym strony podręcznika i często zadawane pytania (FAQ), zawiera serwis WWW programu IPFilter dostępny pod adresem http://coombs.anu.edu.au/~avalon/.

Uwaga: >|Komend **ipfilter** i **ipsec** nie można uruchamiać jednocześnie. Gdy trwa działanie komendy **ipfilter**, podczas uruchamiania i konfigurowania urządzeń `ipsec_v4` mogą występować problemy. |<

Reguły filtrowania statycznego

Każda reguła filtrowania statycznego zawiera pola oddzielone spacjami.

Poniższa lista zawiera nazwy wszystkich pól w regule filtrowania statycznego (w nawiasach znajdują się przykładowe wartości z pierwszej reguły):

- Rule_number (1)
- Action (`permit`)
- Source_addr (`0.0.0.0`)
- Source_mask (`0.0.0.0`)
- Dest_addr (`0.0.0.0`)
- Dest_mask (`0.0.0.0`)
- Source_routing (no)
- Protocol (udp)

- Src_prt_operator (eq)
- Src_prt_value (4001)
- Dst_prt_operator (eq)
- Dst_prt_value (4001)
- Scope (both)
- Direction (both)
- Logging (no)
- Fragment (all packets)
- Tunnel (0)
- Interface (all).

Przykład reguł filtrowania statycznego

```
1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no udp eq 4001 eq 4001 both both no all
   packets 0 all

2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no ah any 0 any 0 both both no all packets
   0 all

3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no esp any 0 any 0 both both no all packets
   0 all

4 permit 10.0.0.1 255.255.255.255 10.0.0.2 255.255.255.255 no all any 0 any 0 both
   outbound no all packets 1 all outbound traffic

5 permit 10.0.0.2 255.255.255.255 10.0.0.1 255.255.255.255 no all any 0 any 0 both
   inbound no all packets 1 all


6 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no tcp lt 1024 eq 514 local
   outbound yes all packets 2 all


7 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack eq 514 lt 1024
   local inbound yes all packets 2 all


8 permit 10.0.0.1 255.255.255.255 10.0.0.3 255.255.255.255 no tcp/ack lt 1024 lt 1024
   local outbound yes all packets 2 all


9 permit 10.0.0.3 255.255.255.255 10.0.0.1 255.255.255.255 no tcp lt 1024 lt 1024 local
   inbound yes all packets 2 all


10 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 0 any 0 local
   outbound yes all packets 3 all


11 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 0 any 0 local
   inbound yes all packets 3 all


12 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp gt 1023 eq 21 local
   outbound yes all packets 4 all


13 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack eq 21 gt 1023 local
   inbound yes all packets 4 all


14 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp eq 20 gt 1023 local
   inbound yes all packets 4 all


15 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp/ack gt 1023 eq 20 local
   outbound yes all packets 4 all


16 permit 10.0.0.1 255.255.255.255 10.0.0.5 255.255.255.255 no tcp gt 1023 gt 1023 local
   outbound yes all packets 4 all
```

```
17 permit 10.0.0.5 255.255.255.255 10.0.0.1 255.255.255.255 no tcp/ack gt 1023 gt 1023 local
   inbound yes all packets 4 all


18 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 no all any 0 any 0 both both yes all
   packets
```

Każda reguła z poprzedniego przykładu opisana jest w następujący sposób:

Reguła 1
Dla demona **Session Key** (Klucz sesji). Ta reguła pojawia się jedynie w tabelach filtrowania dla protokołu IP w wersji 4. W celu sterowania pakietami odświeżania sesji korzysta ona z portu o numerze 4001. Reguła 1 jest przykładem wykorzystania numeru portu do określonego celu.

Uwaga: Tej reguły filtrowania nie należy modyfikować, chyba że jest to potrzebne do celów protokołowania.

Reguły 2 i 3
Umożliwiają przetwarzanie nagłówków protokołu AH (authentication headers) i protokołu ESP (encapsulating security payload).

Uwaga: Reguł 2 i 3 nie należy modyfikować, chyba że jest to potrzebne do celów protokołowania.

Reguły 4 i 5
Zestaw automatycznie generowanych reguł, które filtrują komunikację między adresami 10.0.0.1 i 10.0.0.2 w tunelu 1. Reguła 4 dotyczy ruchu wychodzącego, a reguła 5 - przychodzącego.

Uwaga: Reguła 4 ma zdefiniowany przez użytkownika opis *ruchu wychodzącego*.

Reguły od 6 do 9
Zestaw reguł zdefiniowanych przez użytkownika, które filtrują wychodzące usługi rsh, rcp, rdump, rrestore i rdist między adresami 10.0.0.1 i 10.0.0.3 w tunelu 2. W tym przykładzie protokołowanie jest ustawione na Yes (tak), więc administrator może monitorować ten rodzaj komunikacji.

Reguły 10 i 11
Zestaw reguł zdefiniowanych przez użytkownika, które filtrują przychodzące i wychodzące usługi icmp każdego rodzaju między adresami 10.0.0.1 i 10.0.0.4 w tunelu 3.

Reguły od 12 do 17
Są to reguły zdefiniowane przez użytkownika, które filtrują wychodzącą usługę protokołu FTP między adresami 10.0.0.1 i 10.0.0.5 w tunelu 4.

Reguła 18
Automatycznie generowana reguła, która jest umieszczana zawsze na końcu tabeli. W tym przykładzie dopuszcza ona wszystkie pakiety, które nie pasują do pozostałych reguł filtrowania. Może być ustawiona na odrzucanie całego ruchu, który nie pasuje do pozostałych reguł filtrowania.

Każdą regułę można obejrzeć oddzielnie (za pomocą komendy **lsfilt**), aby wyświetlić każde pole oraz jego wartość. Na przykład:

```
Rule 1:
Rule action          : permit
Source Address       : 0.0.0.0
Source Mask          : 0.0.0.0
Destination Address  : 0.0.0.0
Destination Mask     : 0.0.0.0
Source Routing       : yes
Protocol             : udp
Source Port          : eq  4001
Destination Port     : eq  4001
Scope                : both
Direction            : both
Logging control      : no
Fragment control     : all packets
Tunnel ID number     : 0
Interface            : all
Auto-Generated       : yes
```

Poniższa lista zawiera wszystkie parametry, które można określić dla reguły filtrowania:

-v
protokół IP, wersja: 4 lub 6

-a
Działanie:

d
odmowa

p
zezwolenie

-s
adres źródłowy; może to być adres IP lub nazwa hosta

-m
maska podsieci źródła

-d
adres docelowy, może to być adres IP lub nazwa hosta

-M
maska podsieci miejsca docelowego

-g
kontrola routingu źródła: y lub n

-c
protokół; wartościami mogą być: udp, `icmp`, `tcp`, `tcp/ack`, `ospf`, `pip`, `esp`, `ah` i `all`

-o
port źródłowy lub działanie rodzaju ICMP

-p
port źródłowy lub wartość rodzaju ICMP

-O
port docelowy lub działanie kodu ICMP

-P
port docelowy lub wartość kodu ICMP

-r
Routing:

r
pakiety przekazane dalej

l
pakiety przeznaczenia/pochodzenia lokalnego

b
oba rodzaje pakietów

-l
Kontrola protokołowania

y
włączanie do protokołu

n
niewłączanie do protokołu

-f
Fragmentacja

y
stosowanie dla nagłówków fragmentów, fragmentów i niefragmentów

o
stosowanie tylko dla fragmentów i nagłówków fragmentów

n
stosowanie tylko dla niefragmentów

h
stosowanie tylko dla niefragmentów i nagłówków fragmentów

-t
identyfikator tunelu

-i
interfejs, taki jak `tr0` lub `en0`

Więcej informacji na ten temat zawiera opis komend **genfilt** i **chfilt**.

Reguły filtrowania wygenerowane automatycznie i określone przez użytkownika
Niektóre reguły, wykorzystywane przez filtry bezpieczeństwa IP i kod tunelu, są generowane automatycznie.

Reguły wygenerowane automatycznie zawierają następujące zestawy reguł:

- reguły dla demona klucza sesji, który odświeża w tunelu IKE klucze protokołu IP w wersji 4,
- reguły do przetwarzania pakietów protokołu AH i ESP.

Reguły filtrowania są generowane automatycznie także podczas definiowania tunelu. W przypadku tuneli ręcznych, generowane automatycznie reguły określają adresy źródła i miejsca docelowego, wartości maski, a także identyfikator tunelu. Cały ruch danych między tymi adresami przepływa przez tunel.

W przypadku tuneli IKE, generowane automatycznie reguły filtrowania określają protokół i numery portów podczas negocjacji IKE. Reguły filtrowania IKE są przechowywane w oddzielnej tabeli, która jest przeszukiwana po regułach filtrowania statycznego, a przed regułami wygenerowanymi automatycznie. Reguły filtrowania IKE są wstawiane na domyślną pozycję wewnątrz tabeli filtrów statycznych, ale mogą być przenoszone przez użytkownika.

Reguły wygenerowane automatycznie zezwalają na wszelki ruch danych przez tunel. Reguły zdefiniowane przez użytkownika mogą wprowadzić ograniczenia na niektóre rodzaje ruchu danych. Reguły te należy umieścić przed regułami wygenerowanymi automatycznie, ponieważ bezpieczeństwo IP używa pierwszej napotkanej reguły. Poniżej przedstawiono przykład reguł filtrowania zdefiniowanych przez użytkownika, które filtrują ruch danych oparciu o działanie ICMP.

```
1 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 8 any 0
   local outbound no all packets 3 all
2 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 0 any 0 local
   inbound no all packets 3 all
3 permit 10.0.0.4 255.255.255.255 10.0.0.1 255.255.255.255 no icmp any 8 any 0 local
   inbound no all packets 3 all
4 permit 10.0.0.1 255.255.255.255 10.0.0.4 255.255.255.255 no icmp any 0 any 0 local
   outbound no all packets 3 all
```

Aby uprościć konfigurowanie pojedynczego tunelu, podczas jego definiowania reguły filtrowania są generowane automatycznie. Funkcję tę można wyłączyć przez podanie opcji **-g** dla komendy **gentun**. W katalogu `/usr/samples/ipsec/filter.sample` dostępny jest przykładowy plik filtru, którego można użyć z komendą **genfilt**, aby wygenerować reguły filtrowania dla różnych usług protokołu TCP/IP.

Predefiniowane reguły filtrowania
Dla pewnych zdarzeń automatycznie generowane są predefiniowane reguły filtrowania.

Kiedy załadowane jest urządzenie `ipsec_v4` lub `ipsec_v6` , do tabeli filtrów wstawiana jest predefiniowana reguła, a następnie jest ona aktywowana. Domyślnie reguła ta zezwala na przepływ wszystkich pakietów, ale istnieje możliwość konfigurowania jej przez użytkownika, tak aby odmawiała przepływu wszystkich pakietów.

Uwaga: Podczas konfigurowania zdalnego, aby zapobiec zablokowaniu sesji, należy się upewnić, że reguła odmowy nie została włączona przed zakończeniem konfigurowania. Tej sytuacji można uniknąć ustawiając działanie domyślne, które będzie zezwalało na przepływ lub skonfigurowanie tunelu na komputerze zdalnym, przed aktywowaniem bezpieczeństwa IP.

Protokół IP w wersji 4 i 6 mają predefiniowane reguły filtrowania. Każda z nich może być niezależnie zmieniona, aby blokować cały przepływ. Pozwoli to zablokować ruch danych, dopóki nie zostanie on zdefiniowany za pomocą dodatkowych reguł filtrowania. Jedyną opcją, którą można zmienić w predefiniowanych regułach, jest opcja **chfilt** z argumentem **-l**, pozwalająca na protokołowanie pakietów odpowiadających tej regule.

Aby obsługiwać tunele IKE, w tabeli filtrowania protokołu IP w wersji 4 umieszczana jest reguła filtrowania dynamicznego. Jest to pozycja, na której w tabeli filtrowania wstawiane są reguły filtrowania dynamicznego. Użytkownik może nią sterować, przenosząc ją w górę lub w dół tabeli filtrowania. Po zainicjowaniu demona zarządzania tunelem i demona **isakmpd**, służących do negocjowania tuneli IKE, w tabeli filtrowania dynamicznego reguły są tworzone automatycznie, aby obsłużyć komunikaty IKE, a także pakiety AH i ESP.

Maski podsieci
Maski podsieci używane są w celu grupowania zestawu identyfikatorów, który powiązany jest z regułą filtrowania. Wartość maski jest łączona z identyfikatorem za pomocą operacji logicznej AND, dodawana do reguł filtrowania i porównywana z identyfikatorem określonym w pakiecie.

Na przykład reguła filtrowania ze źródłowym adresem IP `10.10.10.4` i maską podsieci `255.255.255.255` określa, że musi wystąpić dokładne dopasowanie dziesiętnego adresu IP, tak jak pokazano poniżej:

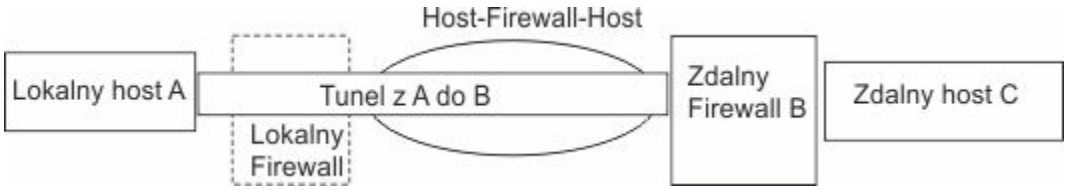
	Binarny	**Dziesiętny**
Źródłowy adres IP	`1010.1010.1010.0100`	`10.10.10.4`
Maska podsieci	`11111111.11111111.11111111.111111 11`	`255.255.255.255`

Podsieć `10.10.10.`x jest określana jako `11111111.11111111.11111111.0` lub jako `255.255.255.0`. Jeśli dla adresu przychodzącego zastosowano maskę podsieci, ta kombinacja może być porównana z identyfikatorem w regule filtrowania. Na przykład adres `10.10.10.100` po zastosowaniu maski podsieci ma postać `10.10.10.0`, co odpowiada regule filtrowania.

Maska podsieci `255.255.255.240` zezwala na dowolną wartość ostatnich czterech bitów adresu.

Konfiguracja host-firewall-host
Opcja konfiguracji host-firewall-host dla tuneli umożliwia utworzenie tunelu między hostem a firewallem, a następnie automatyczne wygenerowanie niezbędnych reguł filtrowania, służących do poprawnej komunikacji między hostem użytkownika a hostem znajdującym się za firewallem.

Reguły filtrowania wygenerowane automatycznie akceptują wszystkie reguły przez tunel określony między dwoma hostami, nie będącymi firewallami. Reguły domyślne - dla nagłówków protokołów UDP, AH i ESP - powinny od razu obsługiwać komunikację między hostem a firewallem. Aby zakończyć konfigurowanie, należy poprawnie skonfigurować firewall. Z utworzonego tunelu należy użyć pliku eksportu, aby wprowadzić wartości interfejsu SPI oraz klucze, których firewall potrzebuje.



Rysunek 14. Host-Firewall-Host

Na ilustracji przedstawiono konfigurację Host-Firewall-Host. Host A ma tunel, łączący z lokalnym firewallem i dalej z siecią Internet. Następnie dochodzi on do zdalnego firewalla B i do zdalnego hosta C.

Narzędzia protokołowania
Kiedy hosty komunikują się ze sobą, przesyłane pakiety mogą być protokołowane w systemowym demonie protokołowania, `syslogd`. Wyświetlane mogą być także inne ważne komunikaty dotyczące bezpieczeństwa IP.

Administrator może monitorować protokołowane informacje, aby analizować ruch danych i uzyskać pomoc przy debugowaniu. Poniżej przedstawione są kolejne kroki konfigurowania narzędzi protokołowania.

1. Zmodyfikuj plik `/etc/syslog.conf`, aby dodać następującą pozycję:

   ```
   local4.debug var/adm/ipsec.log
   ```

   Użyj narzędzia `local4`, aby zapisywać zdarzenia dotyczące ruchu danych i bezpieczeństwa IP. Stosowane są standardowe poziomy priorytetu systemu operacyjnego. Poziom priorytetu powinien być ustawiony na `debug`, dopóki ruch danych przez tunele bezpieczeństwa IP i filtry nie będzie stabilny i poprawny.

   Uwaga: Protokołowanie zdarzeń filtrowania może spowodować znaczącą aktywność hosta bezpieczeństwa IP i zająć dużą ilość pamięci.
2. Zapisz plik `/etc/syslog.conf`.
3. Przejdź do katalogu określonego dla pliku protokołu i utwórz pusty plik o tej samej nazwie. Dla powyższego przypadku można zmienić katalog na `/var/adm` i wprowadzić komendę:

   ```
   touch ipsec.log
   ```
4. W podsystemie `syslogd` wprowadź komendę **refresh**:

   ```
   refresh -s syslogd
   ```
5. Jeśli używane są tunele IKE, upewnij się, że w pliku `/etc/isakmpd.conf` określono wymagany poziom protokołowania **isakmpd**. (Więcej informacji na temat protokołowania IKE zawiera sekcja “Diagnozowanie problemów dotyczących protokołu IP” na stronie 271).
6. Podczas tworzenia reguł filtrowania dla hosta za pomocą komendy **genfilt** lub **chfilt** można ustawić dla reguły parametr *-l* na **Y** (tak), aby protokołowane były pakiety jej odpowiadające.
7. Włącz protokołowanie pakietów i uruchom demon **ipsec_logd** za pomocą komendy:

   ```
   mkfilt -g start
   ```

   Protokołowanie pakietów można zatrzymać za pomocą następującej komendy:

   ```
   mkfilt -g stop
   ```

Poniższy przykładowy plik protokołu zawiera pozycje dotyczące ruchu danych oraz inne pozycje protokołowania bezpieczeństwa IP:

```
1. Aug 27 08:08:40 host1 : Filter logging daemon ipsec_logd (level 2.20)
   initialized at 08:08:40 on 08/27/97A
2. Aug 27 08:08:46 host1 : mkfilt: Status of packet logging set to Start
   at 08:08:46 on 08/27/97
3. Aug 27 08:08:47 host1 : mktun: Manual tunnel 2 for IPv4, 9.3.97.244, 9.3.97.130
   activated.
4. Aug 27 08:08:47 host1 : mkfilt: #:1 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   udp eq  4001 eq  4001  both both l=n f=y t=0 e= a=
5. Aug 27 08:08:47 host1 : mkfilt: #:2 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   ah any 0 any 0  both both l=n f=y t=0 e= a=
6. Aug 27 08:08:47 host1 : mkfilt: #:3 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
   esp any 0 any 0  both both l=n f=y t=0 e= a=
7. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.1 255.255.255.255 10.0.0.2
   255.255.255.255 icmp any 0 any 0  local outbound l=y f=y t=1 e= a=
8. Aug 27 08:08:47 host1 : mkfilt: #:4 permit 10.0.0.2 255.255.255.255 10.0.0.1
   255.255.255.255 icmp any 0 any 0  local inbound l=y f=y t=1 e= a=
9. Aug 27 08:08:47 host1 : mkfilt: #:6 permit 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
    all any 0 any 0  both both l=y f=y t=0 e= a=
10. Aug 27 08:08:47 host1 : mkfilt: Filter support (level 1.00) initialized at
```

```
    08:08:47 on 08/27/97
11. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.20 p:udp
    sp:3327 dp:53 r:l a:n f:n T:0 e:n l:67
12. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.20 d:10.0.0.1 p:udp
    sp:53 dp:3327 r:l a:n f:n T:0 e:n l:133
13. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15 d:10.0.0.1 p:tcp
    sp:4649 dp:23 r:l a:n f:n T:0 e:n l:43
14. Aug 27 08:08:48 host1 : #:6 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.15 p:tcp
    sp:23 dp:4649 r:l a:n f:n T:0 e:n l:41
15. Aug 27 08:08:48 host1 : #:6 R:p  i:10.0.0.1 s:10.0.0.15 d:10.0.0.1 p:tcp
    sp:4649 dp:23 r:l a:n f:n T:0 e:n l:40
16. Aug 27 08:08:51 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.2 p:icmp
    t:8 c:0 r:l a:n f:n T:1 e:n l:84
17. Aug 27 08:08:51 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2 d:10.0.0.1 p:icmp
    t:0 c:0 r:l a:n f:n T:1 e:n l:84
18. Aug 27 08:08:52 host1 : #:4 R:p  o:10.0.0.1 s:10.0.0.1 d:10.0.0.2 p:icmp
    t:8 c:0 r:l a:n f:n T:1 e:n l:84
19. Aug 27 08:08:52 host1 : #:5 R:p  i:10.0.0.1 s:10.0.0.2 d:10.0.0.1 p:icmp
    t:0 c:0 r:l a:n f:n T:1 e:n l:84
20. Aug 27 08:32:27 host1 : Filter logging daemon terminating at 08:32:27 on
    08/27/97l
```

Poniższe akapity wyjaśniają pozycje w protokole.

1
Włączenie demona protokołującego filtrowanie.

2
Protokołowanie filtrowania pakietu zostało ustawione za pomocą komendy **mkfilt -g start**.

3
Nastąpiła aktywacja tunelu, przedstawienie identyfikatora tunelu, adresu źródłowego, adresu docelowego oraz ustawienie daty i godziny.

4-9
Filtry zostały aktywowane; protokołowanie pokazuje wszystkie załadowane reguły filtrowania.

10
Komunikat przedstawiający aktywację filtrów.

11-12
Te pozycje pokazują wyszukiwanie przez serwer DNS hosta.

13-15
Te pozycje pokazują częściowe połączenie Telnet (z powodu oszczędności miejsca, pozostałe pozycje zostały usunięte z przykładu).

16-19
Te pozycje pokazują dwie komendy ping.

20
Wyłączenie demona protokołującego filtrowanie.

Poniższy przykład przedstawia dwa hosty negocjujące tunel, fazy 1 i 2, z punktu widzenia hosta inicjującego. (Poziom protokołowania **isakmpd** został określony jako **isakmp_events**).

```
1. Dec  6 14:34:42 host1 Tunnel Manager: 0: TM is processing a
    Connection_request_msg
 2. Dec  6 14:34:42 host1 Tunnel Manager: 1: Creating new P1 tunnel object (tid)
 3. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( SA PROPOSAL
    TRANSFORM  )
 4. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 ( SA
    PROPOSAL TRANSFORM  )
 5. Dec  6 14:34:42 host1 isakmpd: Phase I SA Negotiated
 6. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( KE NONCE  )
 7. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 ( KE
    NONCE  )
 8. Dec  6 14:34:42 host1 isakmpd: Encrypting the following msg to send: ( ID HASH
     )
 9. Dec  6 14:34:42 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
10. Dec  6 14:34:42 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 (
    Encrypted Payloads )
11. Dec  6 14:34:42 host1 Tunnel Manager: 1: TM is processing a P1_sa_created_msg
    (tid)
12. Dec  6 14:34:42 host1 Tunnel Manager: 1:   Received good P1 SA, updating P1
```

```
    tunnel (tid)
13. Dec  6 14:34:42 host1 Tunnel Manager: 0: Checking to see if any P2 tunnels need
    to start
14. Dec  6 14:34:42 host1 isakmpd: Decrypted the following received msg: ( ID HASH
     )
15. Dec  6 14:34:42 host1 isakmpd:  Phase I Done !!!
16. Dec  6 14:34:42 host1 isakmpd: Phase I negotiation authenticated
17. Dec  6 14:34:44 host1 Tunnel Manager: 0: TM is processing a
    Connection_request_msg
18. Dec  6 14:34:44 host1 Tunnel Manager: 0: Received a connection object for an
    active P1 tunnel
19. Dec  6 14:34:44 host1 Tunnel Manager: 1: Created blank P2 tunnel (tid)
20. Dec  6 14:34:44 host1 Tunnel Manager: 0: Checking to see if any P2 tunnels need
    to start
21. Dec  6 14:34:44 host1 Tunnel Manager: 1: Starting negotiations for P2 (P2 tid)
22. Dec  6 14:34:45 host1 isakmpd: Encrypting the following msg to send: ( HASH SA
    PROPOSAL TRANSFORM NONCE ID ID  )
23. Dec  6 14:34:45 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
24. Dec  6 14:34:45 host1 isakmpd: ::ffff:192.168.100.103 <<< 192.168.100.104 (
    Encrypted Payloads )
25. Dec  6 14:34:45 host1 isakmpd: Decrypted the following received msg: ( HASH SA
    PROPOSAL TRANSFORM NONCE ID ID  )
26. Dec  6 14:34:45 host1 isakmpd: Encrypting the following msg to send: ( HASH  )
27. Dec  6 14:34:45 host1 isakmpd: 192.168.100.103 >>> 192.168.100.104 ( Encrypted
    Payloads )
28. Dec  6 14:34:45 host1 isakmpd: Phase II SA Negotiated
29. Dec  6 14:34:45 host1 isakmpd: PhaseII negotiation complete.
30. Dec  6 14:34:45 host1 Tunnel Manager: 0: TM is processing a P2_sa_created_msg
31. Dec  6 14:34:45 host1 Tunnel Manager: 1: received p2_sa_created for an existing
    tunnel as initiator (tid)
32. Dec  6 14:34:45 host1 Tunnel Manager: 1: Filter::AddFilterRules: Created filter
    rules for tunnel
33. Dec  6 14:34:45 host1 Tunnel Manager: 0: TM is processing a List_tunnels_msg
```

Poniższe akapity wyjaśniają pozycje w protokole.

1-2
Komenda **ike cmd=activate phase=1** inicjuje połączenie.

3-10
Demon **isakmpd** negocjuje tunel, faza 1.

11-12
Menedżer tunelu pobiera od odpowiadającego poprawne powiązanie bezpieczeństwa fazy 1.

13
Menedżer tunelu sprawdza, czy **ike cmd=activate** ma wartość fazy 2 do dalszej pracy; nie ma.

14-16
Demon **isakmpd** kończy negocjację fazy 1.

17-21
Komenda **ike cmd=activate phase=2** inicjuje tunel, faza 2.

22-29
Demon **isakmpd** negocjuje tunel, faza 2.

30-31
Menedżer tunelu pobiera od odpowiadającego poprawne powiązanie bezpieczeństwa fazy 2.

32
Menedżer tunelu zapisuje reguły filtrowania dynamicznego.

33
Komenda **ike cmd=list** przegląda tunele IKE.

Etykiety na pozycjach pola
Pola pozycji protokołowania zostały skrócone w celu zredukowania wymagań przestrzeni DASD.

Pole	Znaczenie
#	Numer reguły, która spowodowała protokołowanie tego pakietu.

Pole **Znaczenie**

R Rodzaj reguły

p
zezwolenie

d
odmowa

i/**o** Kierunek ruchu pakietu w momencie przechwycenia przez kod obsługi filtru. Identyfikuje adres IP adaptera związanego z pakietem:

- dla pakietów przychodzących (inbound - i), jest to adapter, z którego przybył pakiet,
- dla pakietów wychodzących (outbound - o), jest to adapter, który warstwa IP wyznaczyła do obsługi transmisji pakietu.

s Określa adres IP nadawcy pakietu (wyodrębniony z nagłówka IP).

d Określa adres IP zamierzonego odbiorcy pakietu (wyodrębniony z nagłówka IP).

p Określa protokół wyższego poziomu, który został użyty do utworzenia komunikatu w części danych pakietu. Może to być numer lub nazwa, na przykład: udp, `icmp`, `tcp`, `tcp/ack`, `ospf`, `pip`, `esp`, ah lub `all`.

sp/**t** Określa numer portu protokołu związanego z nadawcą pakietu (wyodrębniony z nagłówka TCP/UDP). Jeśli protokołem jest ICMP lub OSPF, to pole zastępowane jest wartością **t**, która określa rodzaj IP.

dp/**c** Określa numer portu protokołu związanego z zamierzonym odbiorcą pakietu (wyodrębniony z nagłówka TCP/UDP). Jeśli protokołem jest ICMP lub OSPF, to pole zastępowane jest wartością **c**, która określa kod IP.

- Określa, że nie są dostępne żadne informacje.

r Oznacza, czy pakiet ma jakąkolwiek lokalną przynależność.

f
pakiety przekazane dalej

l
pakiety lokalne

o
wychodzące

b
oba

l Określa długość poszczególnych pakietów w bajtach.

f Informuje, czy pakiet jest pofragmentowany.

T Wskazuje identyfikator tunelu.

i Określa, z jakiego interfejsu pakiet pochodzi.

Protokołowanie IKE (Internet Key-Exchange)
Istnieje możliwość włączenia protokołowania zdarzeń związanych z protokołem IKE w narzędziu SYSLOG przy użyciu demona **isakmpd**.

Dla demona **isakmpd** protokołowanie włącza się za pomocą komendy **`ike cmd=log`**. Poziom protokołowania można ustawić w pliku konfiguracyjnym `/etc/isakmpd.conf` przy pomocy parametru **log_level**. Zależnie od ilości informacji, które mają być protokołowane, można ustawić poziom *none* (żaden), *errors* (błędy), *isakmp_events* (zdarzenia isakmp) lub *information* (informacje).

Na przykład, aby określić, że mają być protokołowane informacje dotyczące protokołu i implementacji, należy parametr poziomu protokołowania określić następująco:

```
log_level=INFORMATION
```

Demon **isakmpd** uruchamia jeden z dwóch procesów: wysyła kolekcję propozycji lub ocenia kolekcję propozycji. Jeśli kolekcja propozycji zostanie zaakceptowana, tworzone jest powiązanie bezpieczeństwa i konfigurowany jest tunel. Jeśli kolekcja propozycji nie zostanie zaakceptowana lub połączenie zakończy się przed zakończeniem negocjacji, demon **isakmpd** wykaże błąd. Pozycje demona **tmd** w narzędziu SYSLOG wskazują, czy negocjacja zakończyła się powodzeniem. Niepowodzenie spowodowane przez niepoprawny certyfikat jest protokołowane w narzędziu SYSLOG. Aby określić dokładną przyczynę niepowodzenia negocjacji, należy przejrzeć dane w pliku protokołu określonym w pliku `/etc/syslog.conf`.

Narzędzie SYSLOG dodaje do każdego wiersza protokołu przedrostek, informujący o dacie i godzinie, komputerze oraz programie. W poniższym przykładzie nazwą komputera jest `googly`, a nazwą programu `isakmpd`:

```
Nov 20 09:53:50 googly isakmpd: ISAKMP_MSG_HEADER
Nov 20 09:53:50 googly isakmpd:  Icookie : 0xef06a77488f25315, Rcookie :0x0000000000000000
Nov 20 09:53:51 googly isakmpd:  Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
Nov 20 09:53:51 googly isakmpd:  Xchg Type : 2 (ID protected), Flag= 0, Encr : No,COMMIT : No
Nov 20 09:53:51 googly isakmpd:  Msg ID  : 0x00000000
```

W celu zwiększenia czytelności protokołu należy użyć komendy **grep**, aby wyodrębnić interesujące wiersze protokołu (na przykład wszystkie zapisy do protokołu demona **isakmpd**) oraz komendy **cut**, aby z każdego wiersza usunąć przedrostek.

Plik /etc/isakmpd.conf
Opcje demona **isakmpd** można skonfigurować w pliku `/etc/isakmpd.conf`.

W pliku `/etc/isakmpd.conf` dostępne są następujące opcje:

Konfiguracja protokołu
Należy określić ilość protokołowanych informacji, a następnie ustawić poziom. Demony IKE korzystają z tej opcji w celu określenia poziomu protokołowania.

Składnia: `none | error | isakmp_events | information`

gdzie poszczególne poziomy mają następujące znaczenia:

none
Brak protokołowania. Jest to wartość domyślna.

error
Protokołowanie błędów protokołu lub błędów funkcji API.

isakmp_events
Protokołowanie zdarzeń lub błędów IKE. Z tego poziomu należy korzystać podczas debugowania problemu.

information
Protokołowanie informacji o protokole i implementacji.

Negocjacja nieznanego adresu IP
Tej opcji można przypisać wartość TAK lub NIE. W przypadku ustawienia wartości TAK, lokalna baza danych IKE musi zawierać adresy IP dla obu punktów końcowych tunelu fazy 1. Aby host akceptował przychodzący tunel w trybie głównym, opcja ta musi być ustawiona na TAK. Adres IP może być podstawowym identyfikatorem lub opcjonalnym adresem IP powiązanym z innym typem identyfikatora.

Aby akceptować przychodzące połączenie w trybie głównym, należy ustawić tę opcję na NIE. Przy takim ustawieniu host może akceptować połączenie, nawet jeśli w bazie danych IKE nie ma określonych adresów dla punktów końcowych fazy 1. Jednak aby host mógł akceptować połączenie,

trzeba używać uwierzytelniania na podstawie certyfikatów. Dzięki temu host z dynamicznie przypisanym adresem IP może inicjować tunel do komputera w trybie głównym.

Jeśli parametr ten nie zostanie określony, wartością domyślną będzie NIE.

Składnia: MAIN_MODE_REQUIRES_IP= YES | NO

Konfiguracja serwera SOCKS4
Ustawienie opcji SOCKS4_PORTNUM jest opcjonalne. Jeśli nie zostanie określona, zostanie użyta domyślna wartość portu serwera SOCKS równa 1080. Wartość portu jest używana podczas komunikacji serwera SOCKS z serwerem HTTP.

Składnia: *mnemonik* = *wartość*

gdzie *mnemonik* i *wartość* mogą mieć następujące wartości:

SOCKS4_SERVER= nazwa serwera,
SOCKS4_PORTNUM= numer portu serwera SOCKS,
SOCKS4_USERID= identyfikator użytkownika.

Konfiguracja serwera LDAP

Składnia: *mnemonik* = *wartość*

gdzie *mnemonik* i *wartość* mogą mieć następujące wartości:

LDAP_SERVER= nazwa serwera LDAP,
LDAP_VERSION= wersja serwera LDAP (może być 2 lub 3),
LDAP_SERVERPORT= numer portu serwera LDAP,
LDAP_SEARCHTIME= wartość limitu czasu szukania klienta.

Kolejność pobierania listy CRL
Ta opcja określa, czy zapytania kierowane są najpierw do serwera HTTP, czy do serwera LDAP (jeśli skonfigurowane są oba serwery). Ustawienie opcji CRL_FETCH_ORDER jest opcjonalne. Jeśli skonfigurowane są oba serwery, domyślnie najpierw pobierany jest serwer HTTP, a następnie serwer LDAP.

Składnia: CRL_FETCH_ORDER= *numer protokołu*, *protokół*

gdzie *numer protokołu* może mieć wartość HTTP lub LDAP.

Specyfikacja portów IKEv1 i IKEv2
Ten łańcuch określa porty używane przez demon **isakmpd** (IKEv1) i demon **ikev2d** (IKEv2). Demon **iked** (demon brokera wiadomości IKE) wyszukuje tę pozycję i uruchamia demon **isakmpd** oraz demon **ikev2d** z użyciem odpowiednich portów.

Składnia: v1=port-natport,v2=port-natport

Diagnozowanie problemów dotyczących protokołu IP
Poniżej przedstawiono kilka wskazówek, które mogą być pomocne w przypadku wystąpienia problemów.

Podczas pierwszego konfigurowania bezpieczeństwa IP należy skonfigurować protokołowanie. Protokoły są bardzo przydatne przy określaniu, co się przydarzyło filtrom i tunelom. (Szczegółowe informacje na temat protokołowania zawiera sekcja “Narzędzia protokołowania” na stronie 266).

Aby określić, które demony bezpieczeństwa IP są uruchomione, wprowadź następującą komendę:

```
ps -ef
```

Z bezpieczeństwem IP powiązane są następujące demony: **tmd**, **iked**, **isakmpd**, **ikev2d** i **cpsd**.

Uwaga: Jeśli skonfigurowano zarówno IKEv1, jak i IKEv2, uruchomiony jest demon **iked**. W przeciwnym razie uruchomiony jest demon **iskmpd** albo demon **ikev2d**. Ta konfiguracja jest określona w pliku **/etc/isakmpd.conf**.

Rozwiązywanie problemów związanych z błędami tuneli ręcznych
Poniżej podano opisy kilku możliwych błędów tuneli oraz odpowiednich sposobów postępowania.

Błąd	Możliwy problem i jego rozwiązanie
Wywoływanie komendy **mktun** zwraca następujący błąd: `insert_tun_man4(): write failed : The requested resource is busy (zapis nie powiódł się: żądany zasób jest zajęty)`	Problem: żądany tunel jest już aktywny lub nastąpiła kolizja z wartościami interfejsu SPI. Rozwiązanie: należy wywołać komendę **rmtun**, aby dezaktywować tunel, a następnie komendę mktun, aby go ponownie aktywować. Należy sprawdzić, czy wartości interfejsu SPI tunelu odpowiadają innym aktywnym tunelom. Każdy tunel powinien mieć unikalne wartości interfejsu SPI.

Wywoływanie komendy **mktun** zwraca następujący błąd:
`Device ipsec_v4 is in Defined status.`
`Tunnel activation for IP Version 4 not performed (Urządzenie ipsec_v4 ma status Defined. Nie aktywowano tunelu protokołu IP w wersji 4).`
	Problem: urządzenie bezpieczeństwa IP nie jest dostępne.
	Rozwiązanie: należy wywołać następującą komendę:
	`mkdev -l ipsec -t 4`
	Jeśli ten sam błąd występuje w przypadku aktywowania tunelu protokołu IP w wersji 6, opcję **-t** trzeba zmienić na 6. Urządzenia muszą być w stanie dostępności. Aby sprawdzić stan urządzenia bezpieczeństwa IP, należy wywołać następującą komendę:
	`lsdev -Cc ipsec`

Wywoływanie komendy **gentun** zwraca następujący błąd: `Invalid Source IP address (Błędny źródłowy adres IP)`	Problem: dla adresu źródłowego podano błędny adres IP. Rozwiązanie: w przypadku tuneli protokołu IP w wersji 4 należy sprawdzić, czy dla komputera lokalnego wprowadzony został dostępny adres IP w wersji 4. Podczas generowania tuneli nie można podawać nazw hosta jako adresu źródłowego, można to zrobić tylko dla adresu docelowego. W przypadku tuneli protokołu IP w wersji 6 należy sprawdzić, czy wprowadzony został dostępny adres IP w wersji 6. Jeśli wpisana zostanie komenda `netstat -in` i nie istnieją żadne adresy IP w wersji 6, należy uruchomić interfejs `/usr/sbin/autoconf6` w celu dowiązania adresu wygenerowanego lokalnie (korzystającego z adresu MAC) lub komendę **ifconfig**, aby adres przypisać ręcznie.
Wywoływanie komendy **gentun** zwraca następujący błąd: `Invalid Source IP address (Błędny źródłowy adres IP)`	Problem: dla adresu źródłowego podano błędny adres IP. Rozwiązanie: w przypadku tuneli protokołu IP w wersji 4 należy sprawdzić, czy dla komputera lokalnego wprowadzony został dostępny adres IP w wersji 4. Podczas generowania tuneli nie można podawać nazw hosta jako adresu źródłowego, można to zrobić tylko dla adresu docelowego. W przypadku tuneli protokołu IP w wersji 6 należy sprawdzić, czy wprowadzony został dostępny adres IP w wersji 6. Jeśli wpisana zostanie komenda `netstat -in` i nie istnieją żadne adresy IP w wersji 6, należy uruchomić interfejs `/usr/sbin/autoconf6` w celu dowiązania adresu wygenerowanego lokalnie (korzystającego z adresu MAC) lub komendę **ifconfig**, aby adres przypisać ręcznie.

Błąd	Możliwy problem i jego rozwiązanie
Wywoływanie komendy **mktun** zwraca następujący błąd: `insert_tun_man4(): write failed : A system call received a parameter that is not valid. (zapis nie powiódł się: wywołanie systemu otrzymało parametr, który jest błędny).`	Problem: miało miejsce generowanie tunelu z błędną kombinacją protokołów ESP i AH lub bez użycia koniecznego nowego formatu nagłówka. Rozwiązanie: należy sprawdzić, które algorytmy uwierzytelniania są używane przez poszczególne tunele. Należy pamiętać, że algorytmy HMAC_MD5 i HMAC_SHA wymagają nowego formatu nagłówka. Nowy format nagłówka można zmienić za pomocą krótkiej ścieżki programu SMIT **ips4_basic** lub parametru *-z* komendy **chtun**. Należy także pamiętać, że algorytm DES_CBC_4 nie może być używany z nowym formatem nagłówka.
Próba użycia bezpieczeństwa IP powoduje następujący błąd: `The installed bos.crypto is back level and must be updated. (Zainstalowany zestaw plików bos.crypto jest nieaktualny i musi zostać zaktualizowany).`	Problem: pliki `bos.net.ipsec.*` zostały zaktualizowane do nowszej wersji, a odpowiadające im pliki `bos.crypto.*` nie. Rozwiązanie: pliki `bos.crypto.*` należy zaktualizować do wersji, która będzie odpowiadać zaktualizowanym plikom `bos.net.ipsec.*`.

Rozwiązywanie problemów związanych z błędami tuneli IKE (Internet Key Exchange)
Poniższe sekcje opisują błędy, które mogą wystąpić podczas korzystania z tuneli IKE (Internet Key Exchange).

Przebieg procesu tunelu IKE (Internet Key Exchange)
W tej sekcji opisano przebieg procesu tunelu IKE.

Tunele IKE są konfigurowane przez komunikację komendy **ike** z następującymi demonami:

tmd
Demon zarządzania tunelem

iked
Demon brokera IKE (jest aktywny tylko wtedy, gdy oba demony IKEv1 i IKEv2 są skonfigurowane w systemie)

isakmpd
Demon IKEv1

ikev2d
Demon IKEv2

cpsd
Certyfikowany demon proxy

Aby tunele IKE zostały skonfigurowane poprawnie, muszą być uruchomione demony **tmd** i **isakmpd**. Jeśli bezpieczeństwo IP jest ustawione na uruchamianie podczas restartowania, demony te są uruchamiane automatycznie. W przeciwnym razie należy je uruchomić, wprowadzając następującą komendę:

```
startsrc -g ike
```

Menedżer tunelu, aby uruchomić tunel, wysyła żądania do komendy **isakmpd**. Jeśli tunel już istnieje lub nie jest poprawny (na przykład ma niepoprawny adres zdalny), raportowany jest błąd. Jeśli negocjacja została rozpoczęta, jej zakończenie może zająć trochę czasu, w zależności od opóźnień sieci. Za pomocą komendy **ike cmd=list** można pokazać stan tunelu, aby określić, czy negocjacja zakończyła się sukcesem. Menedżer tunelu w pliku `syslog` protokołuje zdarzenia do poziomów debug (debugowanie), event (zdarzenie) i information (informacje), co można wykorzystać, aby monitorować postęp negocjacji.

Sekwencja postępowania jest następująca:

1. W celu zainicjowania tunelu należy użyć komendy **ike**.
2. Demon **tmd** wysyła żądanie połączenia dla tunelu zarządzania kluczem (faza 1) do demona **isakmpd** .
3. Demon **isakmpd** odpowiada SA `created` (powiązanie bezpieczeństwa SA zostało utworzone) lub zwraca komunikat o błędzie.
4. Demon **tmd** wysyła żądanie połączenia dla tunelu zarządzania danymi (faza 2) do demona **isakmpd** .
5. Demon **isakmpd** odpowiada SA `created` (powiązanie bezpieczeństwa SA zostało utworzone) lub zwraca komunikat o błędzie.
6. Do pamięci podręcznej jądra tunelu wstawiane są parametry tunelu.
7. Do tabeli filtrowania dynamicznego dodawane są reguły filtrowania.

Jeśli komputer działa jako komputer odpowiadający, demon **isakmpd** powiadomi demon zarządzania tunelem **tmd**, że tunel został wynegocjowany pomyślnie, a do jądra wstawiany jest nowy tunel. W takich przypadkach proces zaczyna się od kroku 3 i jest kontynuowany do kroku 7, z pominięciem wywoływania przez demon **tmd** żądań połączenia.

Funkcja protokołowania Parse Payload
Powiązanie bezpieczeństwa (Security Association - SA) między dwoma punktami końcowymi jest ustanawiane przez wymianę komunikatów IKE. Funkcja Parse Payload (Analiza ładunku) analizuje komunikaty w formacie czytelnym dla użytkownika.

Protokołowanie funkcji Parse Payload (Analiza ładunku) można włączyć, modyfikując plik `/etc/isakmpd.conf`. Pozycja protokołowania w pliku `/etc/isakmpd.conf` wygląda podobnie do następującej:

```
information
```

Rodzaj ładunków IKE, które protokołuje funkcja Parse Payload (Analiza ładunku), zależy od zawartości komunikatu IKE. Przykłady obejmują SA Payload (ładunek powiązania bezpieczeństwa), Key Exchange Payload (ładunek wymiany klucza), Certificate Request Payload (ładunek żądania certyfikatu), Certificate Payload (ładunek certyfikatu) i Signature Payload (ładunek podpisu). Poniżej przedstawiony jest przykład protokołowania funkcji Parse Payload, w którym po ISAKMP_MSG_HEADER następuje pięć ładunków:

```
ISAKMP_MSG_HEADER
        Icookie : 0x9e539a6fd4540990, Rcookie : 0x0000000000000000
        Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
        Xchg Type : 4 (Aggressive), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x10e(270)
SA Payload:
        Next Payload : 4(Key Exchange), Payload len : 0x34(52)
        DOI          : 0x1(INTERNET)
        bitmask      : 1(SIT_IDENTITY_ONLY
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x28(40)
        Proposal #  : 0x1(1), Protocol-ID : 1(ISAKMP)
        SPI size : 0x0(0), # of Trans : 0x1(1)
   Transform Payload:
        Next Payload : 0(NONE), Payload len : 0x20(32)
        Trans #  : 0x1(1), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x1(1),(DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x3(3),(RSA Signature)
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
Key Payload:
        Next Payload : 10(Nonce), Payload len : 0x64(100)

        Key Data :
```

```
        33 17 68 10 91 1f ea da 38 a0 22 2d 84 a3 5d 5d
        a0 e1 1f 42 c2 10 aa 8d 9d 14 0f 58 3e c4 ec a3
        9f 13 62 aa 27 d8 e5 52 8d 5c c3 cf d5 45 1a 79
        8a 59 97 1f 3b 1c 08 3e 2a 55 9b 3c 50 cc 82 2c
        d9 8b 39 d1 cb 39 c2 a4 05 8d 2d a1 98 74 7d 95
        ab d3 5a 39 7d 67 5b a6 2e 37 d3 07 e6 98 1a 6b

Nonce Payload:
        Next Payload : 5(ID), Payload len : 0xc(12)

        Nonce Data:
        6d 21 73 1d dc 60 49 93
ID Payload:
        Next Payload : 7(Cert.Req), Payload len : 0x49(73)
        ID type      : 9(DER_DN), Protocol : 0, Port = 0x0(0)
Certificate Request Payload:
        Next Payload : 0(NONE), Payload len : 0x5(5)
        Certificate Encoding Type: 4(X.509 Certificate - Signature)
```

W ramach każdego ładunku pole **Next Payload** (Następny ładunek) wskazuje na następujący po nim ładunek. Jeśli bieżący ładunek jest ostatnim ładunkiem komunikatu IKE, pole **Next Payload** (Następny ładunek) ma wartość zero (None).

Każdy ładunek w tym przykładzie zawiera informacje odnoszące się do przeprowadzanych negocjacji. Na przykład ładunek powiązania bezpieczeństwa ma ładunki Proposal and Transform Payloads (Ładunki transformowania i kolekcji propozycji), które pokazują algorytm szyfrowania, tryb uwierzytelniania, algorytm mieszający, rodzaj czasu życia powiązania bezpieczeństwa oraz przedział czasu powiązania bezpieczeństwa, które inicjator proponuje odpowiadającemu.

Ładunek powiązania bezpieczeństwa zawiera także jeden lub więcej ładunków Proposal Payloads (Ładunki kolekcji propozycji) i Transform Payloads (Ładunki transformacji). Pole **Next Payload** (Następny ładunek) dla ładunku Proposal Payload (Ładunek kolekcji propozycji) ma wartość 0, jeśli jest to jedyny ładunek, lub wartość 2, jeśli następuje po nim jeszcze jeden ładunek. Podobnie pole **Next Payload** (Następny ładunek) dla ładunku Transform Payload (Ładunek transformacji) ma wartość 0, jeśli jest to jedyny ładunek, lub 3, jeśli następuje po nim jeszcze jeden ładunek, tak jak przedstawiono to w poniższym przykładzie:

```
ISAKMP_MSG_HEADER
        Icookie : 0xa764fab442b463c6, Rcookie : 0x0000000000000000
        Next Payload : 1(SA), Maj Ver : 1, Min Ver : 0
        Xchg Type : 2 (ID protected), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x70(112)
SA Payload:
        Next Payload : 0(NONE), Payload len : 0x54(84)
        DOI          : 0x1(INTERNET)
        bitmask      : 1(SIT_IDENTITY_ONLY
   Proposal Payload:
        Next Payload : 0(NONE), Payload len : 0x48(72)
        Proposal # : 0x1(1), Protocol-ID : 1(ISAKMP)
        SPI size : 0x0(0), # of Trans : 0x2(2)
   Transform Payload:
        Next Payload : 3(Transform), Payload len : 0x20(32)
        Trans # : 0x1(1), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x5(5),(3DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x1(1),(Pre-shared Key)
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
   Transform Payload:
        Next Payload : 0(NONE), Payload len : 0x20(32)
        Trans # : 0x2(2), Trans.ID : 1(KEY_IKE)
        Attr : 1(Encr.Alg     ), len=0x2(2)
        Value=0x1(1),(DES-cbc)
        Attr : 2(Hash Alg     ), len=0x2(2)
        Value=0x1(1),(MD5)
        Attr : 3(Auth Method  ), len=0x2(2)
        Value=0x1(1),(Pre-shared Key)
```

```
        Attr : 4(Group Desc   ), len=0x2(2)
        Value=0x1(1),(default 768-bit MODP group)
        Attr : 11(Life Type    ), len=0x2(2)
        Value=0x1(1),(seconds)
        Attr : 12(Life Duration), len=0x2(2)
        Value=0x7080(28800)
```

Nagłówek komunikatu IKE protokołu funkcji Parse Payload (Analiza ładunku) przedstawia rodzaj wymiany (Tryb główny lub tryb agresywny), długość całego komunikatu, jego identyfikator itp.

Ładunek Certificate Request Payload (Ładunek żądania certyfikatu) żąda certyfikatu od odpowiadającego. Odpowiadający wysyła certyfikat w osobnym komunikacie. Poniższy przykład przedstawia ładunki Certificate Payload (Ładunek certyfikatu) i Signature Payload (Ładunek podpisu), które są wysyłane do węzła sieci jako część negocjacji powiązania bezpieczeństwa. Dane certyfikatu i podpisu wydrukowane są w formacie szesnastkowym.

```
ISAKMP_MSG_HEADER
        Icookie : 0x9e539a6fd4540990, Rcookie : 0xc7e0a8d937a8f13e
        Next Payload : 6(Certificate), Maj Ver : 1, Min Ver : 0
        Xchg Type : 4 (Aggressive), Flag= 0, Encr : No,COMMIT : No
        Msg ID  : 0x00000000
        len     : 0x2cd(717)
Certificate Payload:

        Next Payload : 9(Signature), Payload len : 0x22d(557)
        Certificate Encoding Type: 4(X.509 Certificate - Signature)
        Certificate: (len 0x227(551) in bytes
        82 02 24 30 82 01 8d a0 03 02 01 02 02 05 05 8e
        fb 3e ce 30 0d 06 09 2a 86 48 86 f7 0d 01 01 04
        05 00 30 5c 31 0b 30 09 06 03 55 04 06 13 02 46
        49 31 24 30 22 06 03 55 04 0a 13 1b 53 53 48 20
        43 6f 6d 6d 75 6e 69 63 61 74 69 6f 6e 73 20 53
        65 63 75 72 69 74 79 31 11 30 0f 06 03 55 04 0b
        13 08 57 65 62 20 74 65 73 74 31 14 30 12 06 03
        55 04 03 13 0b 54 65 73 74 20 52 53 41 20 43 41
        30 1e 17 0d 39 39 30 39 32 31 30 30 30 30 30 30
        5a 17 0d 39 39 31 30 32 31 32 33 35 39 35 39 5a
        30 3f 31 0b 30 09 06 03 55 04 06 13 02 55 53 31
        10 30 0e 06 03 55 04 0a 13 07 49 42 4d 2f 41 49
        58 31 1e 30 1c 06 03 55 04 03 13 15 62 61 72 6e
        65 79 2e 61 75 73 74 69 6e 2e 69 62 6d 2e 63 6f
        6d 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01 01
        01 05 00 03 81 8d 00 30 81 89 02 81 81 00 b2 ef
        48 16 86 04 7e ed ba 4c 14 d7 83 cb 18 40 0a 3f
        55 e9 ad 8f 0f be c5 b6 6d 19 ec de 9b f5 01 a6
        b9 dd 64 52 34 ad 3d cd 0d 8e 82 6a 85 a3 a8 1c
        37 e4 00 59 ce aa 62 24 b5 a2 ea 8d 82 a3 0c 6f
        b4 07 ad 8a 02 3b 19 92 51 88 fb 2c 44 29 da 72
        41 ef 35 72 79 d3 e9 67 02 b2 71 fa 1b 78 13 be
        f3 05 6d 10 4a c7 d5 fc fe f4 c0 b8 b8 fb 23 70
        a6 4e 16 5f d4 b1 9e 21 18 82 64 6d 17 3b 02 03
        01 00 01 a3 0f 30 0d 30 0b 06 03 55 1d 0f 04 04
        03 02 07 80 30 0d 06 09 2a 86 48 86 f7 0d 01 01
        04 05 00 03 81 81 00 75 a4 ee 9c 3a 18 f2 de 5d
        67 d4 1c e4 04 b4 e5 b8 5e 9f 56 e4 ea f0 76 4a
        d0 e4 ee 20 42 3f 20 19 d4 25 57 25 70 0a ea 41
        81 3b 0b 50 79 b5 fd 1e b6 0f bc 2f 3f 73 7d dd
        90 d4 08 17 85 d6 da e7 c5 a4 d6 9a 2e 8a e8 51
        7e 59 68 21 55 4c 96 4d 5a 70 7a 50 c1 68 b0 cf
        5f 1f 85 d0 12 a4 c2 d3 97 bf a5 42 59 37 be fe
        9e 75 23 84 19 14 28 ae c4 c0 63 22 89 47 b1 b6
        f4 c7 5d 79 9d ca d0
Signature Payload:
        Next Payload : 0(NONE), Payload len : 0x84(132)

        Signature: len 0x80(128) in bytes
        9d 1b 0d 90 be aa dc 43 95 ba 65 09 b9 00 6d 67
        b4 ca a2 85 0f 15 9e 3e 8d 5f e1 f0 43 98 69 d8
        5c b6 9c e2 a5 64 f4 ef 0b 31 c3 cb 48 7c d8 30
        e3 a2 87 f4 7c 9d 20 49 b2 39 00 fa 8e bf d9 b0
        7d b4 8c 4e 19 3a b8 70 90 88 2c cf 89 69 5d 07
        f0 5a 81 58 2e 15 40 37 b7 c8 d6 8c 5c e2 50 c3
        4d 19 7e e0 e7 c7 c2 93 42 89 46 6b 5f f8 8b 7d
        5b cb 07 ea 36 e5 82 9d 70 79 9a fe bd 6c 86 36
```

Problemy związane z certyfikatami cyfrowymi i trybami podpisu
Poniżej wymienione zostały rozwiązania możliwych problemów związanych z certyfikatami cyfrowymi i trybami podpisu:

Błąd	**Możliwy problem i jego rozwiązanie**
Błąd: nie uruchamia się demon **cpsd** (Certificate Proxy Server daemon). W pliku protokołu pojawia się pozycja podobna do następującej: `Sep 21 6:02:00 ripple CPS[19950]: Init():LoadCaCerts() nie powiodło się, rc =-12`	Problem: nie otworzyła się baza danych certyfikatów lub nie została ona znaleziona. Rozwiązanie: należy się upewnić, że w katalogu `/etc/security` obecne są bazy danych certyfikatów narzędzia Key Manager (Menedżer kluczy). Bazę danych tworzą następujące pliki: `ikekey.crl`, `ikekey.kdb`, `ikekey.rdb`, `ikekey.sth`. Jeśli brakuje jedynie pliku `ikekey.sth`, oznacza to, że podczas tworzenia bazy danych w narzędziu Key Manager (Menedżer kluczy) nie wybrano opcji `stash password` (składowanie hasła). Aby umożliwić korzystanie z certyfikatów cyfrowych razem z zabezpieczeniem IP, hasło musi być zeskładowane. (Więcej informacji na ten temat zawiera sekcja Tworzenie bazy danych kluczy).

Błąd: podczas pobierania certyfikatu narzędzie Key Manager (Menedżer kluczy) pokazuje następujący błąd:
`Invalid Base64-encoded data was found (Znaleziono nieprawidłowe dane Base64-encoded)`
	Problem: w pliku certyfikatu znaleziono niepotrzebne dane albo dane zostały utracone lub uszkodzone.
	Rozwiązanie: zakodowany certyfikat 'DER' powinien zawierać się między dwoma łańcuchami (przedstawionymi poniżej). W pliku nie powinny znajdować się żadne inne znaki, które poprzedzałyby lub następowałyby po łańcuchach BEGIN (początek) i END CERTIFICATE (koniec certyfikatu).
	`-----BEGIN CERTIFICATE-----`
	`MIICMTCCAZqgAwIBAgIFFKZtANowDQYJKoZIhvcNAQEFBQAwXDELMAkGA1UEBhMC`
	`RkkxJDAiBgNVBAoTG1NTSCBDb21tdW5pY2F0aW9ucyBTZWN1cml0eTERMA8GA1UE`
	`CxMIV2ViIHRlc3QxFDASBgNVBAMTC1Rlc3QgUlNBIENBMB4XDTk5MDkyMTAwMDAw`
	`MFoXDTk5MTAyMTIzNTk1OVowOzELMAkGA1UEBhMCVVMxDDAKBgNVBAoTA0lCTTEe`
	`MBwGA1UEAxMVcmlwcGxlLmF1c3Rpbi5pYm0uY29tMIGfMA0GCSqGSIb3DQEBAQUA`
	`A4GNADCBiQKBgQC5EZqo6n7tZrpAL6X4L7mf4yXQSm+m/NsJLhp6afbFpPvXgYWC`
	`wq4pvOtvxgum+FHrE0gysNjbKkE4Y6ixC9PGGAKHnhM3vrmvFjnl1G6KtyEz58Lz`
	`BWW39QS6NJ1LqqP1nT+y3+Xzvfv8Eonqzno8mglCWMX09SguLmWoU1PcZQIDAQAB`
	`oyAwHjALBgNVHQ8EBAMCBaAwDwYDVR0RBAgwBocECQNhhzANBgkqhkiG9w0BAQUF`
	`AOBgQA6bgp4Zay34/fyAlyCkNNAYJRrN3Vc4NHN7IGjUziN6jK5UyB5zL37FERW`
	`hT9ArPLzK7yEZs+MDNvB0bosyGWEDYPZr7EZHhYcoBP4/cd0V5rBFmA8Y2gUthPi`
	`Ioxpi4+KZGHYyLqTrm+8Is/DVJaQmCGRPynHK35xjT6WuQtiYg==`
	`-----END CERTIFICATE-----`
	Poniższe opcje mogą pomóc przy diagnozowaniu i rozwiązywaniu tego problemu:
	• jeśli dane zostały utracone lub uszkodzone, certyfikat należy utworzyć ponownie,
	• aby sprawdzić, czy certyfikat jest poprawny, należy użyć analizatora składni ASN.1 (dostępnego w sieci Internet).

Błąd: podczas pobierania certyfikatu osobistego narzędzie Key Manager (Menedżer kluczy) pokazuje następujący błąd: `No request key was found for the certificate (Nie znaleziono żądania klucza dla certyfikatu)`	Problem: dla pobieranego certyfikatu osobistego nie istnieje żądanie certyfikatu osobistego. Rozwiązanie: należy ponownie utworzyć żądanie certyfikatu osobistego i zażądać nowego certyfikatu.

Błąd	Możliwy problem i jego rozwiązanie
Błąd: negocjacja tunelu IKE nie powiodła się, a w pliku protokołu pojawia się pozycja podobna do następującej: `inet_cert_service:: channelOpen(): clientInitIPC():error,rc =2 (Brak pliku lub katalogu)`	Problem: demon **cpsd** nie działa lub został zatrzymany. Rozwiązanie: uruchom bezpieczeństwo IP, które uruchamia odpowiednie demony.
Błąd: negocjacja tunelu IKE nie powiodła się, a w pliku protokołu pojawia się pozycja podobna do następującej: `CertRepo::GetCertObj: DN Does Not Match: ("/C=US/O=IBM/CN=ripple.austin.ibm.com") (Niezgodna nazwa wyróżniająca)`	Problem: nazwa wyróżniająca X.500, podana podczas definiowania tunelu IKE, nie odpowiada nazwie X.500 w certyfikacie osobistym. Rozwiązanie: zmień definicję tunelu IKE, tak aby odpowiadała nazwie wyróżniającej w certyfikacie.

Narzędzia śledzenia

Śledzenie jest narzędziem debugowania, służącym do śledzenia zdarzeń jądra. Narzędzia śledzenia mogą być używane w celu uzyskania bardziej szczegółowych informacji na temat zdarzeń lub błędów występujących w filtrze jądra lub kodzie tunelu.

Narzędzie śledzenia bezpieczeństwa IP programu SMIT jest dostępne z poziomu menu Zaawansowana konfiguracja bezpieczeństwa IP. Informacje, przechwycone przez to narzędzie, obejmują dane dotyczące: błędów, filtru, informacji o filtrze, tunelu, informacji o tunelu, hermetyzowania/dehermetyzowania, informacji o hermetyzowaniu, szyfrowania i informacji o szyfrowaniu. W zamyśle, śledzenie błędów udostępnia najbardziej krytyczne informacje. Śledzenie może generować krytyczne informacje i może wpływać wpływ na wydajność systemu. Śledzenie udostępnia wskazówki na temat problemu i jest wymagane podczas zgłaszania problemu do serwisu.

Aby włączyć śledzenie, skonfiguruj urządzenia IPSec i ustaw poziom śledzenia dla każdego podkomponentu IPSec na 7, aby wygenerować użyteczne dane śledzenia jądra. Jeśli urządzenia IPSec nie są skonfigurowane, komendy kontrolne śledzenia nie będą zawierać powiązanych pozycji IPSec. Aby uruchomić śledzenie IPSec, użyj krótkiej ścieżki SMIT **smit ips4_start** (dla IPv4) lub **smit ips6_start** (dla IPv6).

Uwaga: Jeśli śledzenie komponentu IPSec nie jest poprawnie ustawione, pliki śledzenia będą puste.

Aby przechwycić dane śledzenia jądra, wykonaj następujące kroki:

1. Sprawdź bieżący stan ustawień śledzenia wszystkich komponentów:

   ```
   # ctctrl -q
   ```

2. Sprawdź komponent IPSec i podkomponenty. Komponenty początkowo mają ustawiony poziom śledzenia 3. Aby wyświetlić domyślny, początkowy poziom śledzenia komponentów:

   ```
   # ctctrl -q -c ipsec -r
   ```

Nazwa komponentu	Ma alias	Pamięć śledzenia/poziom	Śledzenie systemowe/ poziom	Wielkość buforu/ przydzielone
ipsec	NIE	ON/3	ON/3	40960/TAK
.capsulate	NIE	ON/3	ON/3	10240/TAK
.filter	NIE	ON/3	ON/3	10240/TAK
.tunnel	NIE	ON/3	ON/3	10240/TAK

3. Zwiększ poziom śledzenia IPSec i podkomponentów na 7, aby umożliwić śledzenie jądra:

```
# ctctrl systracelevel=7 -c ipsec -r
```

4. Potwierdź zmianę poziomów śledzenia, wpisując komendę:

```
# ctctrl -q -c ipsec -r
```

Nazwa komponentu	Ma alias	Pamięć śledzenia/poziom	Śledzenie systemowe/ poziom	Wielkość buforu/ przydzielone
ipsec	NIE	ON/3	ON/7	40960/TAK
.capsulate	NIE	ON/3	ON/7	10240/TAK
.filter	NIE	ON/3	ON/7	10240/TAK
.tunnel	NIE	ON/3	ON/7	10240/TAK

Aby uzyskać dostęp do narzędzia śledzenia, należy użyć krótkiej ścieżki programu SMIT **smit ips4_tracing** (dla protokołu IP w wersji 4) lub **smit ips6_tracing** (dla protokołu IP w wersji 6). Śledzenie jądra zebrane za pomocą komend **smit ips4_tracing**, **smit ips6_tracing** lub w wierszu komend generuje poprawne dane śledzenia IPSec.

Komenda ipsecstat

Komenda **ipsecstat** umożliwia wyświetlenie statusu urządzeń bezpieczeństwa IP, algorytmów szyfrowania bezpieczeństwa IP i statystyk pakietów bezpieczeństwa IP.

Wydanie komendy **ipsecstat** powoduje wygenerowanie poniższego przykładowego raportu, który pokazuje, że urządzenia bezpieczeństwa IP są w stanie dostępności, że zainstalowane są trzy algorytmy uwierzytelniające i trzy algorytmy szyfrowania i że istnieje bieżący raport aktywności pakietu. Informacje te mogą być przydatne przy określaniu problemu podczas rozwiązywania problemów dotyczących komunikacji bezpieczeństwa IP.

```
IP Security Devices:
ipsec_v4 Available
ipsec_v6 Available

Authentication Algorithm:
HMAC_MD5 -- Hashed MAC MD5 Authentication Module
HMAC_SHA -- Hashed MAC SHA Hash Authentication Module
KEYED_MD5 -- Keyed MD5 Hash Authentication Module

Encryption Algorithm:
CDMF -- CDMF Encryption Module
DES_CBC_4 -- DES CBC 4 Encryption Module
DES_CBC_8 -- DES CBC 8 Encryption Module
3DES_CBC -- Triple DES CBC Encryption Module

IP Security Statistics -
Total incoming packets:  1106
Incoming AH packets:326
Incoming ESP packets:  326
Srcrte packets allowed:  0
Total outgoing packets:844
Outgoing AH packets:527
```

```
Outgoing ESP packets:  527
Total incoming packets dropped:  12
  Filter denies on input:  12
  AH did not compute: 0
  ESP did not compute:0
  AH replay violation:0
  ESP replay violation:  0
Total outgoing packets dropped:0
  Filter denies on input:0
Tunnel cache entries added: 7
Tunnel cache entries expired:  0
Tunnel cache entries deleted:  6
```

Uwaga: Nie ma potrzeby korzystania z algorytmu CDMF, ponieważ algorytm szyfrowania DES jest teraz ogólnie dostępny. Należy przekonfigurować wszystkie tunele, które korzystają z algorytmu CDMF, aby używały one algorytmu DES lub potrójnego DES.

Informacje dodatkowe o bezpieczeństwie IP
Bezpieczeństwo IP obejmuje komendy i metody. Istnieje także możliwość przeprowadzenia migracji tuneli, filtrów i wstępnych kluczy wspólnych IKE.

Lista komend
Poniższa tabela zawiera listę komend.

Komenda	Działanie
ike cmd=activate	Uruchamia negocjację IKE (Internet Key Exchange).
ike cmd=remove	Dezaktywuje tunele IKE
ike cmd=list	Wyświetla listę tuneli IKE
ikedb	Udostępnia interfejs bazie danych tunelu IKE
gentun	Tworzy definicję tunelu
mktun	Aktywuje definicje tunelu
chtun	Zmienia definicję tunelu
rmtun	Usuwa definicję tunelu
lstun	Wyświetla definicje tunelu
exptun	Eksportuje definicje tunelu
imptun	Importuje definicje tunelu
genfilt	Tworzy definicję filtrowania
mkfilt	Aktywuje definicje filtrowania
mvfilt	Przenosi reguły filtrowania
chfilt	Zmienia definicję filtrowania
rmfilt	Usuwa definicję filtrowania
lsfilt	Pokazuje definicje filtrowania
expfilt	Eksportuje definicje filtrowania
impfilt	Importuje definicje filtrowania
ipsec_convert	Pokazuje status bezpieczeństwa IP
Komenda ipsecstat	Pokazuje status bezpieczeństwa IP
ipsectrcbuf	Pokazuje zawartość buforu śledzenia bezpieczeństwa IP
unloadipsec	Rozładowuje moduł szyfrowania

Lista metod
Poniżej znajduje się lista metod.

defipsec
Definiuje instancję bezpieczeństwa IP dla protokołu IP w wersji 4 lub 6

cfgipsec
Konfiguruje i ładuje **ipsec_v4** lub **ipsec_v6**

ucfgipsec
Dekonfiguruje **ipsec_v4** lub **ipsec_v6**

Migracja bezpieczeństwa IP
Istnieje możliwość przeprowadzenia migracji tuneli, filtrów i wstępnych kluczy wspólnych IKE z wcześniejszych wersji systemu operacyjnego AIX.

Migracja tuneli IKE
Aby przeprowadzić migrację tuneli:

1. Uruchom skrypt `bos.net.ipsec.keymgt.pre_rm.sh`. Po uruchomieniu tego skryptu w katalogu `/tmp` zostaną utworzone następujące pliki:
   a. `p2proposal.bos.net.ipsec.keymgt`
   b. `p1proposal.bos.net.ipsec.keymgt`
   c. `p1policy.bos.net.ipsec.keymgt`
   d. `p2policy.bos.net.ipsec.keymgt`
   e. `p1tunnel.bos.net.ipsec.keymgt`
   f. `p2tunnel.bos.net.ipsec.keymgt`

   Ostrzeżenie: Skrypt ten należy uruchomić tylko jeden raz. Po zaktualizowaniu bazy danych i ponownym uruchomieniu tego skryptu, wszystkie pliki zostaną utracone i nie będzie możliwe ich odtworzenie. Przed migracją tuneli należy przeczytać skrypt “Skrypt bos.net.ipsec.keymgt.pre_rm.sh” na stronie 282.
2. Zapisz pliki utworzone przy pomocy skryptu oraz plik `/tmp/lpplevel` na nośniku zewnętrznym, takim jak dysk CD lub dyskietka.

Migracja wstępnych kluczy wspólnych
Niżej wymienione czynności umożliwiają zaktualizowanie formatu wstępnego klucza wspólnego.

Baza danych wstępnych kluczy wspólnych tunelu IKE również ulega uszkodzeniu podczas migracji. Aby zaktualizować format wstępnych kluczy wspólnych w systemie, w którym przeprowadzono migrację:

1. Zapisz dane wyjściowe komendy **ikedb -g**, uruchamiając następującą komendę:
   ```
   ikedb -g > out.keys
   ```
2. W pliku `out.keys` zamień wyrażenie formatu wstępnych kluczy wspólnych FORMAT=ASCII na FORMAT=HEX.
3. Wprowadź plik XML, uruchamiając następującą komendę:
   ```
   ikedb -pF out.keys
   ```

Migracja filtrów
Aby przeprowadzić migrację filtrów:

1. Wyeksportuj pliki reguł filtrowania do katalogu `/tmp` za pomocą programu SMIT, wykonując następujące kroki:
   a. Uruchom komendę **smitty ipsec4**.

b. Wybierz opcję Zaawansowana konfiguracja IPsec—>Konfiguruj reguły filtru IPsec->Eksportuj reguły filtrowania IPsec.

c. Wpisz nazwę katalogu /tmp.

d. W opcji Reguły filtrowania naciśnij klawisz F4 i z listy wybierz **wszystkie**.

e. Naciśnij klawisz Enter, aby zapisać regułę filtrowania w pliku /tmp/ipsec_fltr_rule.exp na nośniku zewnętrznym.

Przeprowadź ten proces dla wszystkich systemów, na których przeprowadzana jest migracja z wcześniejszych wersji systemu operacyjnego AIX.

2. Skopiuj sześć plików tunelu utworzonych za pomocą skryptu, plik /tmp/lpplevel oraz plik /tmp/ipsec_fltr_rule.exp do katalogu /tmp w systemie, w którym przeprowadzana jest migracja.
3. Uruchom skrypt bos.net.ipsec.keymgt.post_i.sh, aby ponownie umieścić konfiguracje tuneli w bazie danych.
4. Uruchom komendę **ikedb -g**, aby sprawdzić, czy tunele znajdują się w bazie danych.

   Uwaga: Jeśli w bazie danych nie widać informacji o tunelach, należy ponownie uruchomić skrypt, zmieniając wcześniej nazwy plików *.loaded w katalogu /tmp na ich nazwy początkowe.

W systemie, w którym przeprowadzono migrację, baza danych filtrów jest uszkodzona. Jeśli komenda **lsfilt** zostanie uruchomiona w systemie, w którym została przeprowadzona migracja, zostanie wyświetlony następujący błąd:

```
Cannot get ipv4 default filter rule (Nie można pobrać domyślnej reguły filtrowania ipv4)
```

Aby zaktualizować bazę danych filtrów:

1. Zastąp pliki ipsec_filter i ipsec_filter.vc w katalogu /etc/security plikami nie uszkodzonymi, pobranymi z nowo zmigrowanego systemu. Jeśli nie masz tych plików, możesz je zamówić w serwisie IBM.
2. Zaimportuj pliki reguł filtrowania do katalogu /tmp za pomocą programu SMIT, wykonując następujące kroki:

   a. Uruchom komendę **smitty ipsec4**.

   b. Wybierz opcję Zaawansowana konfiguracja IPsec—>Konfiguruj reguły filtru IPsec->Eksportuj reguły filtrowania IPsec.

   c. Wpisz nazwę katalogu /tmp.

   d. W opcji **Reguły filtrowania** naciśnij klawisz **F4** i z listy wybierz **wszystkie**.

   e. Naciśnij klawisz Enter, aby ponownie utworzyć reguły filtrowania. Listę reguł filtrowania można wyświetlić za pomocą programu SMIT lub komendy **lsfilt**.

Skrypt bos.net.ipsec.keymgt.pre_rm.sh
Skrypt bos.net.ipsec.keymgt.pre_rm.sh zapisuje zawartość bazy danych tuneli w systemie operacyjnym AIX.

```
#!/usr/bin/ksh
keymgt_installed=`lslpp -Lqc bos.net.ipsec.keymgt 2>/dev/null | awk -F: '{print $6}' | head -1`

if [ ! "$keymgt_installed" ]
then
  exit 0
fi


#  Kopiuje bazę danych do katalogu serwera w przypadku, gdy zmiany nie powiodą się.
if [ -d /etc/ipsec/inet/DB ]
then
  cp -R /etc/ipsec/inet/DB /etc/ipsec/inet/DB.sav || exit $?
fi

#  Zapamiętuje poziom, z którego wykonywana jest migracja.
VRM=$(LANG=C lslpp -Lqc bos.net.ipsec.keymgt 2>/dev/null | awk -F: '{print $3}' | \
awk -F. '{print $1"."$2"."$3}')
```

```
VR=${VRM%.*}
echo $VRM > /tmp/lpplevel

IKEDB=$(which ikedb) || IKEDB=/usr/sbin/ikedb

XMLFILE=/tmp/full_ike_database.bos.net.ipsec.keymgt
PSKXMLFILE=/tmp/psk_ike_database.bos.net.ipsec.keymgt

#  Sprawdza, czy istnieje baza kluczy ikedb.
if [ -f $IKEDB ]
then

  # Jeśli oba wywołania ikedb nie powiodą się, nie ma problemu. Po prostu usuń
  # plik wynikowy (który może zawierać błąd) i kontynuuj wykonywanie skryptu. Skrypt post_i
  # po prostu nie zaimportuje pliku, który nie istnieje. Oznacza to, że
  # część lub cała baza danych IKE została utracona. W takim przypadku najlepiej
  # wyjść ze skryptu z kodem błędu, co spowoduje niepowodzenie
  # wykonywania migracji.

  $IKEDB -g > $XMLFILE
  if [ $? -ne 0 ]
  then
    rm -f $XMLFILE  || exit $?
  fi

  if [[ $VR = "5.1" ]]; then
    # To jest przypadek specjalny. Wersja 5.1 bazy danych kluczy ikedb jest jedyną,
    # która nie włącza wstępnych kluczy wspólnych w pełnych danych wyjściowych
    # bazy danych. Dlatego należy je odtworzyć oddzielnie.
    $IKEDB -g -t IKEPresharedKey > $PSKXMLFILE
    if [ $? -ne 0 ]
    then
     rm -f $PSKXMLFILE  || exit $?
    fi
  fi

#  Należy się upewnić, czy komenda ikegui została zainstalowana.
elif [ -f /usr/sbin/ikegui ]
then

  #  Pobiera informacje bazy danych i zapisuje je do pliku /tmp
  /usr/sbin/ikegui 0 1 0 0 > /tmp/p1proposal.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p1proposal.bos.net.ipsec.keymgt || exit $?
  fi

  /usr/sbin/ikegui 0 1 1 0 > /tmp/p1policy.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p1policy.bos.net.ipsec.keymgt || exit $?
  fi

  /usr/sbin/ikegui 0 2 0 0 > /tmp/p2proposal.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p2proposal.bos.net.ipsec.keymgt || exit $?
  fi

  /usr/sbin/ikegui 0 2 1 0 > /tmp/p2policy.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p2policy.bos.net.ipsec.keymgt || exit $?
  fi

  /usr/sbin/ikegui 0 1 2 0 > /tmp/p1tunnel.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p1tunnel.bos.net.ipsec.keymgt || exit $?
  fi

  /usr/sbin/ikegui 0 2 2 0 > /tmp/p2tunnel.bos.net.ipsec.keymgt 2>/dev/null
  RC=$?
  if [[ $RC -ne 0 ]]
  then
    rm -f /tmp/p2tunnel.bos.net.ipsec.keymgt || exit $?
  fi
```

```
fi
```

Skrypt bos.net.ipsec.keymgt.post_i.sh
Skrypt `bos.net.ipsec.keymgt.post_i.sh` ładuje zawartość bazy danych tuneli do systemu operacyjnego AIX, na którym przeprowadzana jest migracja.

```
#!/usr/bin/ksh

function PrintDot {
    echo "echo \c"
    echo "\".\c"
    echo "\\\c\c"
    echo "\"\c"
    echo
}

function P1PropRestore {
    while :
    do
        read NAME
        read MODE
        if [[ $? = 0 ]]; then
            echo "ikegui 1 1 0 $NAME $MODE \c"
            MORE=1
            while [[ $MORE = 1 ]];
            do
                read AUTH
                read HASH
                read ENCRYPT
                read GROUP
                read TIME
                read SIZE
                read MORE
                echo "$AUTH $HASH $ENCRYPT $GROUP $TIME $SIZE $MORE \c"
            done
            echo " > /dev/null 2>&1"
            PrintDot
        else
            return 0
        fi
    done
}

function P2PropRestore {
    while :
    do
        read NAME
        FIRST=yes
        MORE=1
        while [[ $MORE = 1 ]];
        do
            read PROT
            if [[ $? = 0 ]]; then
                read AH_AUTH
                read ESP_ENCR
                read ESP_AUTH
                read ENCAP
                read TIME
                read SIZE
                read MORE
                if [[ $FIRST = "yes" ]]; then
                    echo "ikegui 1 2 0 $NAME $MODE \c"
                fi
                echo "$PROT $AH_AUTH $ESP_ENCR $ESP_AUTH $ENCAP $TIME $SIZE $MORE \c"
                FIRST=no
            else
                return 0
            fi
        done
        echo " > /dev/null 2>&1"
        PrintDot
    done
}

function P1PolRestore {
    while :
    do
        read NAME
```

```
        read ROLE
        if [[ $? = 0 ]]; then
            read TIME
            read SIZE
            read OVERLAP
            read TTIME
            read TSIZE
            read MIN
            read MAX
            read PROPOSAL
            echo "ikegui 1 1 1 $NAME $ROLE $OVERLAP $TTIME $TSIZE $MIN $MAX 1 0 0 $PROPOSAL > \
/dev/null 2>&1"
            PrintDot
        else
            return 0
        fi
    done
}

function P2PolRestore {
    while :
    do
        read NAME
        read ROLE
        if [[ $? = 0 ]]; then
            read IPFS
            read RPFS
            read TIME
            read SIZE
            read OVERLAP
            read TTIME
            read TSIZE
            read MIN
            read MAX
            echo "ikegui 1 2 1 $NAME $ROLE $IPFS $RPFS $OVERLAP $TTIME $TSIZE $MIN $MAX 1 0 0
\c"
            MORE=1
            while [[ $MORE = 1 ]];
            do
                read PROPOSAL
                read MORE
                echo "$PROPOSAL $MORE \c"
                FIRST=no
            done
        else
            return 0
        fi
        echo " > /dev/null 2>&1"
        PrintDot
    done
}

function P1TunRestore {
    while :
    do
        read TUNID
        read NAME
        if [[ $? = 0 ]]; then
            read LID_TYPE
            read LID
            if [[ $LPPLEVEL = "4.3.3" ]]; then
                read LIP
            fi
            read RID_TYPE
            read RID
            read RIP
            read POLICY
            read KEY
            read AUTOSTART
            echo "ikegui 1 1 2 0 $NAME $LID_TYPE \"$LID\" $LIP $RID_TYPE \"$RID\" \
$RIP $POLICY $KEY $AUTOSTART > /dev/null 2>&1"
            PrintDot
        else
            return 0
        fi
    done
}

function P2TunRestore {
    while :
    do
        read TUNID
```

```
        read NAME
        if [[ $? = 0 ]]; then
            read P1TUN
            read LTYPE
            read LID
            read LMASK
            read LPROT
            read LPORT
            read RTYPE
            read RID
            read RMASK
            read RPROT
            read RPORT
            read POLICY
            read AUTOSTART
            echo "ikegui 1 2 2 0 $NAME $P1TUN $LTYPE $LID $LMASK $LPROT $LPORT $RTYPE
              \$RID $RMASK $RPROT $RPORT $POLICY $AUTOSTART > /dev/null 2>&1"
            PrintDot
        else
            return 0
        fi
    done
}

function allRestoreWithIkedb {

    ERRORS=/tmp/ikedb_msgs.bos.net.ipsec.keymgt
    echo > $ERRORS
    $IKEDB -p $XMLFILE 2>> $ERRORS
    if [ -f $PSKXMLFILE ]
    then
        $IKEDB -p $PSKXMLFILE 2>> $ERRORS
    fi

}

P1PROPFILE=/tmp/p1proposal.bos.net.ipsec.keymgt
P2PROPFILE=/tmp/p2proposal.bos.net.ipsec.keymgt
P1POLFILE=/tmp/p1policy.bos.net.ipsec.keymgt
P2POLFILE=/tmp/p2policy.bos.net.ipsec.keymgt
P1TUNFILE=/tmp/p1tunnel.bos.net.ipsec.keymgt
P2TUNFILE=/tmp/p2tunnel.bos.net.ipsec.keymgt
XMLFILE=/tmp/full_ike_database.bos.net.ipsec.keymgt
PSKXMLFILE=/tmp/psk_ike_database.bos.net.ipsec.keymgt
CMD_FILE=/tmp/commands
IKEDB=$(which ikedb) || IKEDB=/usr/sbin/ikedb

echo "Budowanie bazy danych ISAKMP\n"
$IKEDB -x || exit $?

if [ -f $XMLFILE ]; then
    echo "\nOdtwarzanie pozycji bazy danych\c"
    allRestoreWithIkedb
    echo "\ngotowe\n"

elif [ -f /tmp/*.bos.net.ipsec.keymgt ]; then
    echo "\nOdtwarzanie pozycji bazy danych\c"

    LPPLEVEL=`cat /tmp/lpplevel`

    echo > $CMD_FILE
    touch $P1PROPFILE; P1PropRestore < $P1PROPFILE >> $CMD_FILE
    touch $P2PROPFILE; P2PropRestore < $P2PROPFILE >> $CMD_FILE
    touch $P1POLFILE; P1PolRestore < $P1POLFILE >> $CMD_FILE
    touch $P2POLFILE; P2PolRestore < $P2POLFILE >> $CMD_FILE
    touch $P1TUNFILE; P1TunRestore < $P1TUNFILE >> $CMD_FILE
    touch $P2TUNFILE; P2TunRestore < $P2TUNFILE >> $CMD_FILE

    mv $P1PROPFILE ${P1PROPFILE}.loaded
    mv $P2PROPFILE ${P2PROPFILE}.loaded
    mv $P1POLFILE ${P1POLFILE}.loaded
    mv $P2POLFILE ${P2POLFILE}.loaded
    mv $P1TUNFILE ${P1TUNFILE}.loaded
    mv $P2TUNFILE ${P2TUNFILE}.loaded

    ksh $CMD_FILE

    echo "\ngotowe\n"
fi
```

Bezpieczeństwo sieciowego systemu plików (NFS)

System plików NFS jest powszechnie stosowaną technologią pozwalającą na udostępnianie zasobów między różnymi hostami w sieci.

System plików NFS oprócz algorytmu DES obsługuje także użycie uwierzytelniania Kerberos 5. Protokół Kerberos 5 jest dostarczany z użyciem mechanizmu RPCSEC_GSS.

Oprócz standardowego mechanizmu uwierzytelniania w systemie UNIX, system plików NFS umożliwia uwierzytelnianie użytkowników i komputerów w sieciach na poziomie pojedynczych komunikatów. Ten dodatkowy mechanizm uwierzytelniania wykorzystuje szyfrowanie algorytmem DES oraz kryptografię z kluczem publicznym.

System plików NFS oprócz algorytmu DES obsługuje także użycie uwierzytelniania Kerberos 5. Protokół Kerberos 5 jest dostarczany z użyciem mechanizmu RPCSEC_GSS. Opis administrowania i używania uwierzytelniania Kerberos w protokole NFS zawiera publikacja *NFS Administration Guide*.

Ogólne wskazówki na temat bezpieczeństwa systemu plików NFS

Istnieje kilka wytycznych ułatwiających zapewnienie bezpieczeństwa systemu plików NFS (Network File System).

- Należy się upewnić, że zostały zainstalowane najnowsze poprawki programowe. Poprawki dotyczące zagadnień bezpieczeństwa powinny być traktowane ze szczególną uwagą. Dla całego oprogramowania w danej infrastrukturze powinny być zainstalowane najnowsze poprawki. Na przykład zainstalowanie poprawek w systemie operacyjnym: ich brak na serwerze WWW może spowodować otwarcie drogi do środowiska sieciowego dla włamywaczy komputerowych. Można tego uniknąć, instalując wszystkie poprawki także na serwerze WWW. Aby zasubskrybować alerty bezpieczeństwa systemu IBM System p zawierające informacje na temat najnowszych zagadnień związanych z bezpieczeństwem, należy odwiedzić stronę WWW pod adresem: http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd.
- Należy skonfigurować serwer NFS, tak aby wyeksportować systemy plików z możliwie najmniejszymi niezbędnymi uprawnieniami. Jeśli użytkownikom potrzebny jest tylko odczyt z systemu plików, nie powinni mieć uprawnień do zapisu. Może to zmniejszyć ryzyko wymazania ważnych danych, zmiany plików konfiguracyjnych lub zapisania niebezpiecznych plików wykonywalnych do eksportowanego systemu plików. Uprawnienia można określić przy pomocy programu SMIT lub bezpośrednio edytując plik `/etc/exports`.
- Należy skonfigurować serwer NFS, tak aby wyeksportować systemy plików wyłącznie dla użytkowników, który powinni mieć do nich dostęp. Większość implementacji systemu plików NFS umożliwia określenie, które klienty NFS powinny mieć dostęp do danego systemu plików. Zmniejszy to ryzyko dostępu do systemu plików przez nieuprawnionych użytkowników. W szczególności nie należy konfigurować serwera NFS w celu eksportowania systemu plików do siebie samego.
- Wyeksportowane systemy plików powinny się znajdować w swoich własnych partycjach. Włamywacz komputerowy może spowodować uszkodzenie systemu, zapisując do pełna wyeksportowany system plików. Może to spowodować niewydolność systemu dla innych aplikacji lub użytkowników, którzy go potrzebują.
- Nie należy zezwalać klientom NFS na dostęp do systemu plików z wiarygodnością użytkownika root lub z nieznaną wiarygodnością. Większość implementacji systemu plików NFS może być tak skonfigurowana, aby przypisywać żądania przychodzące od uprawnionego lub nieznanego użytkownika do użytkownika nieuprawnionego. Zapobiegnie to sytuacji, w której włamywacz komputerowy próbuje uzyskać dostęp do plików i wykonać operacje na plikach jako uprawniony użytkownik.
- Nie należy zezwalać klientom systemu plików NFS na wykonywanie programów suid i sgid na wyeksportowanych systemach plików. Zapobiegnie to sytuacji, w której klienty systemu plików NFS mogą uruchamiać niebezpieczne programy. Jeśli włamywacz komputerowy jest stanie uruchomić program, którego właścicielem jest uprawniony użytkownik lub grupa, to może spowodować duże szkody na serwerze NFS. Jest to możliwe po podaniu opcji komendy **mknfsmnt -y**.
- Należy używać zabezpieczeń systemu plików NFS. Zabezpieczenia systemu plików NFS używają algorytmu szyfrowania DES do uwierzytelniania hostów uczestniczących w transakcjach RPC. RPC jest protokołem używanym przez system plików NFS do wymiany żądań pomiędzy hostami. Zabezpieczenia

systemu plików NFS zmniejszają ryzyko podjęcia przez włamywacza komputerowego próby sfałszowania żądań RPC poprzez zaszyfrowanie datownika w żądaniach RPC. Odbiorca deszyfruje pomyślnie datownik i potwierdza, że jest on poprawny, co oznacza, że żądanie RPC nadeszło z zaufanego hosta.

- Jeśli system plików NFS nie jest potrzebny, należy go wyłączyć. Zmniejszy to liczbę możliwych ataków pochodzących od intruzów.

System plików NFS oprócz algorytmu szyfrowania Triple DES i Single DES obsługuje również użycie typu szyfrowania AES z uwierzytelnianiem Kerberos 5. Opis konfigurowania protokołu Kerberos 5 pod kątem użycia szyfrowania typu AES zawiera podręcznik zarządzania systemem plików NFS.

Pojęcia pokrewne

“Bezpieczeństwo sieciowego systemu plików (NFS)” na stronie 287 text="System plików NFS jest powszechnie stosowaną technologią pozwalającą na udostępnianie zasobów między różnymi hostami w sieci."

Informacje pokrewne

Lista kontrolna konfigurowania NFS
Uruchomienie demonów NFS podczas uruchomienia systemu
Skonfigurowanie serwera NFS
Skonfigurowanie klienta NFS
Odwzorowywanie tożsamości
Wyeksportowanie systemu plików NFS
Skonfigurowanie sieci dla RPCSEC-GSS
Anulowanie eksportu systemu plików NFS
Zmiana wyeksportowanego systemu plików
Dostęp użytkownika root do wyeksportowanego systemu plików
Jawne podłączenie systemu plików NFS
Automatyczne podłączenie podsystemu
Ustanowienie predefiniowanych podłączeń NFS
Usunięcie predefiniowanych podłączeń NFS
Plik eksportów dla NFS
Komenda mknfsmnt

Uwierzytelnianie w sieciowym systemie plików (NFS)

System plików NFS używa algorytmu szyfrowania DES w różnych celach, między innymi w celu szyfrowania datownika w komunikatach zdalnego wywołania procedury (Remote Procedure Call - RPC) wysyłanych pomiędzy serwerami i klientami NFS. Szyfrowany datownik uwierzytelnia komputer w taki sam sposób, w jaki token uwierzytelnia nadawcę.

System plików NFS może uwierzytelnić każdy komunikat RPC wysyłany pomiędzy klientami i serwerami NFS, więc stanowi to dodatkowy, opcjonalny poziom bezpieczeństwa dla każdego systemu plików. Domyślnie systemy plików są eksportowane ze standardowym uwierzytelnianiem systemu UNIX. Aby wykorzystać ten dodatkowy poziom bezpieczeństwa, należy przy eksportowaniu systemu plików podać opcję secure.

Szyfrowanie klucza publicznego dla bezpiecznego systemu plików NFS

Zarówno klucz publiczny, jak i klucz tajny użytkownika są przechowywane i indeksowane według nazwy sieciowej w odwzorowaniu `publickey.byname`.

Klucz tajny jest szyfrowany algorytmem DES z hasłem logowania. Komenda **keylogin** używa zaszyfrowanego klucza tajnego, deszyfruje go za pomocą hasła logowania, a następnie umieszcza w zabezpieczonym lokalnym serwerze kluczy w celu późniejszego wykorzystania w transakcjach RPC. Użytkownicy nie muszą być świadomi istnienia swoich kluczy publicznych i tajnych, gdyż komenda **yppasswd** w momencie zmiany hasła logowania użytkownika generuje automatycznie oba klucze.

Demon keyserv jest usługą RPC działającą na każdym komputerze z NIS i NIS+. Więcej informacji o tym, w jaki sposób NIS+ używa komendy **keyserv**, zawiera publikacja *Network Information Services (NIS and*

NIS+) Guide. W systemie NIS komenda **keyserv** wykonuje następujące podprocedury klucza publicznego:

- **key_setsecret**,
- **key_encryptsession**,
- **key_decryptsession**.

Podprocedura **key_setsecret** nakazuje serwerowi kluczy przechowanie klucza tajnego użytkownika (SK_A) w celu jego późniejszego wykorzystania; zazwyczaj jest wywoływana przez komendę **keylogin**. Program klient wywołuje podprocedurę **key_encryptsession**, aby wygenerować zaszyfrowany klucz konwersacji, przekazywany do serwera w pierwszej transakcji RPC. Serwer kluczy sprawdza klucz publiczny serwera i łączy go z kluczem tajnym klienta (skonfigurowanym przez poprzednią podprocedurę **key_setsecret**) aby wygenerować klucz wspólny. Serwer prosi serwer kluczy o deszyfrowanie klucza, wywołując w tym celu podprocedurę **key_decryptsession**.

W tych wywołaniach podprocedur niejawna jest nazwa wywołującego, która musi być w jakiś sposób uwierzytelniona. Serwer kluczy nie może w tym celu użyć uwierzytelniania DES, gdyż mogłoby to spowodować zakleszczenie. Serwer kluczy rozwiązuje ten problem, przechowując klucze tajne według ID użytkownika i dopuszcza jedynie żądania do lokalnych procesów działających z prawami użytkownika root. Proces klienta wykonuje następnie podprocedurę **setuid** użytkownika root, która wykonuje żądanie w imieniu klienta i zwraca do serwera kluczy jego rzeczywisty identyfikator użytkownika.

Wymagania dotyczące uwierzytelniania w systemie plików NFS
Uwierzytelnianie w bezpiecznym systemie plików NFS działa w oparciu o możliwość szyfrowania przez nadawcę bieżącego czasu, który odbiorca następnie deszyfruje i sprawdza własny zegar.

Proces ten ma następujące wymagania:

- oba agenty muszą uzgodnić bieżący czas,
- nadawca i odbiorca muszą korzystać z tego samego klucza szyfrowania DES.

Uzgadnianie bieżącego czasu
Jeśli sieć korzysta z synchronizacji czasu, demon timed synchronizuje zegary klienta i serwera. Jeśli nie, klient oblicza poprawny datownik według zegara serwera.

W tym celu klient przed rozpoczęciem sesji RPC określa czas serwera, a następnie oblicza różnicę czasu pomiędzy własnym zegarem a tym na serwerze. Następnie klient dopasowuje odpowiednio swój datownik. Jeśli w trakcie trwania sesji RPC zegary klienta i serwera zaczną się desynchronizować, w momencie, gdy serwer zacznie odrzucać żądania klienta, ten powinien ponownie określić czas serwera.

Korzystanie z tego samego klucza DES
Klient i serwer obliczają ten sam klucz szyfrowania DES za pomocą szyfrowania z kluczem publicznym.

Dla dowolnego klienta A i serwera B istnieje klucz o nazwie *klucz wspólny*, który tylko A i B są w stanie wywnioskować. Klient oblicza klucz wspólny za pomocą następującego wzoru:

$$K_{AB} = PK_B^{SK}A$$

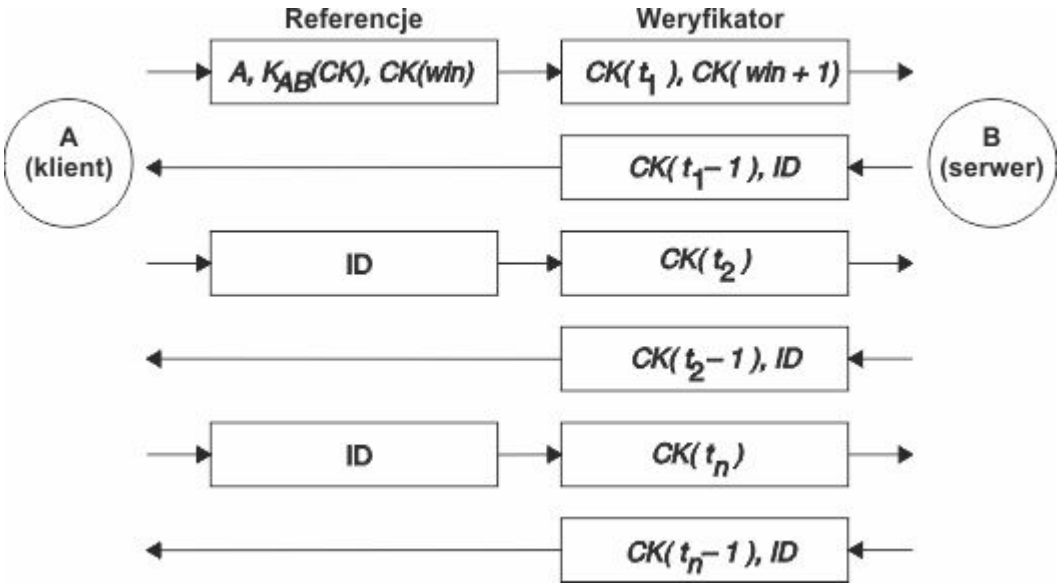
gdzie *K* jest kluczem wspólnym, *PK* jest kluczem publicznym, a *SK* jest kluczem tajnym. Wszystkie klucze są liczbami 128-bitowymi. Serwer oblicza klucz wspólny za pomocą następującego wzoru:

$$K_{AB} = PK_A^{SK}B$$

Tylko serwer i klient mogą obliczyć ten klucz wspólny, gdyż w tym celu potrzebna jest znajomość jednego z kluczy tajnych. Ponieważ klucz wspólny ma 128 bitów, a DES używa 56-bitowego klucza, klient i serwer wyodrębniają 56 bitów z klucza wspólnego, aby utworzyć klucz DES.

Proces uwierzytelniania w sieciowym systemie plików
Gdy klient chce rozmawiać z serwerem, generuje losowo klucz służący do szyfrowania datownika. Klucz ten jest nazywany *kluczem konwersacji* (*Conversation Key - CK*).

Klient szyfruje klucz konwersacji za pomocą klucza wspólnego DES (opisanego w sekcji Wymagania dotyczące uwierzytelniania) i wysyła go do serwera w pierwszej transakcji RPC. Proces ten ilustruje poniższy rysunek.



Rysunek 15. Proces uwierzytelniania

Rysunek przedstawia połączenie klienta A z serwerem B. Litera *K*(*CK*) oznacza *CK* i jest szyfrowana kluczem wspólnym DES *K*. W pierwszym żądaniu referencje RPC klienta zawierają nazwę klienta (*A*), klucz konwersacji (*CK*) i zmienną nazywaną *win* (window - okno) szyfrowaną za pomocą *CK*. (Domyślna wielkość okna wynosi 30 minut). Weryfikacja klienta w pierwszym żądaniu zawiera szyfrowany datownik i szyfrowaną weryfikację podanego okna *win* + 1. Weryfikacja okna powoduje, że odgadywanie referencji jest znacznie utrudnione, dzięki czemu zwiększone zostaje bezpieczeństwo.

Po uwierzytelnieni klienta serwer zapisuje w tabeli referencji następujące elementy:

- nazwę klienta, *A*,
- klucz konwersacji, *CK*,
- okno,
- datownik.

Serwer akceptuje datowniki tylko chronologicznie późniejsze od ostatnio widzianych, gwarantowane jest więc odrzucenie powtórzonych transakcji. Serwer podczas weryfikacji zwraca do klienta ID indeksu do tabeli referencji oraz datownik klienta pomniejszony o 1, wszystko szyfrowane kluczem *CK*. Klient wie, że tylko serwer może wysłać taką weryfikację, gdyż tylko serwer zna datownik wysłany przez klienta. Powodem pomniejszenia datownika o 1 jest zapewnienie, że nie będzie on poprawny i nie będzie mógł zostać wykorzystany ponownie jako weryfikacja klienta. Po tej pierwszej transakcji RPC klient wysyła po prostu do serwera własny identyfikator i szyfrowany datownik, a serwer odsyła datownik pomniejszony o 1, wszystko szyfrowane kluczem *CK*.

Nazewnictwo jednostek sieciowych dla uwierzytelniania DES
Uwierzytelnianie DES wykorzystuje we własnym nazewnictwie nazwy sieciowe. Informacje dotyczące obsługi przez system NIS+ uwierzytelniania DES zawiera publikacja *Network Information Services (NIS and NIS+) Guide*.

Nazwa sieciowa to łańcuch drukowalnych znaków używanych do uwierzytelniania. Klucze publiczne i tajne są zapisywane zwykle według nazwy sieciowej, a nie według nazwy użytkownika. Odwzorowanie `netid.byname` systemu NIS odwzorowuje nazwę sieciową na lokalny identyfikator użytkownika i listę dostępu grupy.

Nazwy użytkowników są unikalne w ramach każdej domeny, uzyskiwane są z konkatenacji systemu operacyjnego i ID użytkownika z nazwami domen systemu NIS i Internetu. Dobrą konwencją przy

nazywaniu domen jest dodanie nazwy domeny w Internecie (com, edu, gov, mil) do nazwy domeny lokalnej.

Nazwy sieciowe przypisywane są do komputerów i do użytkowników. Nazwa sieciowa komputera jest utworzona w podobny sposób co nazwa użytkownika. Na przykład komputer o nazwie `hal` w domenie `eng.xyz.com` ma nazwę sieciową `unix.hal@eng.xyz.com`. Prawidłowe uwierzytelnianie komputerów jest ważne w przypadku maszyn bezdyskowych, które potrzebują pełnego dostępu przez sieć do katalogów osobistych.

Aby uwierzytelnić użytkowników z dowolnej zdalnej domeny, należy dokonać dla nich wpisów do dwóch baz danych systemu NIS. Jeden wpis jest dla klucza publicznego i tajnego, drugi dla lokalnego numeru UID i odwzorowania listy dostępu grupy. Użytkownicy ze zdalnej domeny mają wtedy dostęp do wszystkich zdalnych usług sieciowych, takich jak system plików NFS czy zdalne logowanie.

Plik /etc/publickey
Plik `/etc/publickey` zawiera nazwy i klucze publiczne, z których korzystają systemy NIS i NIS+ w celu utworzenia odwzorowania publickey.

Odwzorowanie publickey używane jest w celu zapewnienia bezpiecznego działania sieci. Każdy wpis w pliku składa się z nazwy sieciowej użytkownika (odnoszącej się do nazwy użytkownika lub nazwy hosta), następnie z klucza publicznego użytkownika (w zapisie szesnastkowym), przecinka i szyfrowanego klucza tajnego użytkownika (także w zapisie szesnastkowym). Domyślnie w pliku `/etc/publickey` jedynym użytkownikiem jest użytkownik nobody.

Nie należy używać edytora tekstu w celu wprowadzania zmian w pliku `/etc/publickey`, gdyż plik ten zawiera klucze szyfrowania. Aby zmodyfikować plik `/etc/publickey`, należy użyć komendy **chkey** albo **newkey**.

Uwagi dotyczące uruchamiania systemów klucza publicznego
Gdy nastąpi awaria zasilania komputera i związany z tym restart, wszystkie zapisane klucze tajne giną i żaden proces nie ma dostępu do bezpiecznych usług sieciowych, takich jak podłączenie systemu plików NFS. Procesy użytkownika root mogą nadal działać, jeśli znajdzie się ktoś, kto wpisze hasło, które deszyfruje klucz tajny użytkownika root. Rozwiązaniem jest zapisanie deszyfrowanego klucza tajnego użytkownika root w pliku, który serwer kluczy będzie mógł odczytać.

Nie wszystkie wywołania podprocedury **setuid** działają poprawnie. Na przykład, jeśli podprocedura **setuid** jest wywoływana przez właściciela A, który nie zalogował się do komputera od momentu jego uruchomienia, to podprocedura nie ma dostępu do żadnych bezpiecznych usług sieciowych jako A. Jednak większość wywołań podprocedur **setuid** należy do użytkownika root, którego klucz tajny jest zapisywany podczas uruchamiania systemu.

Uwagi dotyczące wydajności bezpiecznego systemu plików NFS
Bezpieczny system plików NFS wpływa na wydajność systemu na kilka sposobów.

- Klient i serwer muszą obliczyć klucz wspólny. Czas takiego obliczenia wynosi około 1 sekundy. W wyniku tego, początkowe nawiązanie połączenia RPC zajmuje około 2 sekund, gdyż operację tę musi wykonać i klient i serwer. Po początkowym połączeniu RPC serwer kluczy przechowa w pamięci podręcznej wynik poprzednich obliczeń, aby za każdym razem nie obliczać klucza wspólnego.
- Każda transakcja RPC wymaga następującego szyfrowania algorytmem DES:
  1. Klient szyfruje datownik żądania.
  2. Serwer go deszyfruje.
  3. Serwer szyfruje datownik odpowiedzi.
  4. Klient go deszyfruje.

Stosowanie bezpiecznego systemu plików NFS powoduje zmniejszenie wydajności systemu, dlatego należy wyważyć zalety zwiększonego bezpieczeństwa wraz z wymaganiami dotyczącymi wydajności systemu.

Lista kontrolna bezpiecznego systemu plików NFS
Ta lista kontrolna ułatwia zapewnienie poprawnego działania bezpiecznego systemu plików NFS.

- Podczas podłączania na kliencie systemu plików z opcją **-secure**, nazwa serwera musi być zgodna z nazwą hosta serwera z pliku `/etc/hosts`. Jeśli do tłumaczenia nazw używany jest serwer nazw, należy się upewnić, że informacje o hoście zwracane przez serwer nazw są zgodne z wpisem w pliku `/etc/hosts`. Jeśli nazwy te nie są zgodne, gdyż nazwy sieciowe komputerów bazują na pierwszych wpisach w pliku `/etc/hosts` a klucze w odwzorowaniu **publickey** są dostępne po nazwie sieciowej, to spowoduje to błędy uwierzytelniania.
- Nie należy łączyć chronionych i niechronionych eksportów i podłączeń. W przeciwnym razie dostęp do pliku może być określony niepoprawnie. Na przykład, jeśli klient podłącza bezpieczny system plików bez opcji **-secure** lub niezabezpieczony system z opcją **-secure**, użytkownicy mają dostęp jako użytkownik nobody, a nie z własnymi identyfikatorami. Warunek ten występuje także, jeśli użytkownik nieznany w systemie NIS lub NIS+ próbuje utworzyć lub zmienić pliki w bezpiecznym systemie plików.
- System NIS musi propagować nowe odwzorowanie po każdym użyciu komendy **chkey** i **newkey**, dlatego należy używać tych komend tylko wtedy, gdy sieć jest mało obciążona.
- Nie należy usuwać pliku `/etc/keystore` ani `/etc/.rootkey`. Podczas reinstalacji, przenoszenia lub aktualizacji systemu należy zapisać pliki `/etc/keystore` i `/etc/.rootkey`.
- Należy poinstruować użytkowników, aby do zmiany hasła używali komendy **yppasswd**, zamiast komendy **passwd**. Wtedy hasła i klucze prywatne będą zsynchronizowane.
- Komenda **login** nie odczytuje kluczy z odwzorowania publickey dla demona **keyserv**, dlatego użytkownik musi wykonać komendę **keylogin**. Można umieścić komendę **keylogin** w pliku `profile` każdego użytkownika, aby wykonywała się automatycznie podczas jego logowania w systemie. Komenda **keylogin** wymaga dwukrotnego wprowadzenia hasła.
- Podczas generowania - na każdym hoście - kluczy dla użytkownika root za pomocą komendy **newkey -h** lub **chkey**, trzeba uruchomić komendę **keylogin**, aby przesłać nowe klucze do demona **keyserv**. Klucze są przechowywane w pliku `/etc/.rootkey` odczytywanym przez demon **keyserv** po każdym jego uruchomieniu.
- Okresowo należy sprawdzać, czy demony **yppasswdd** i **ypupdated** działają na serwerze nadrzędnym NIS. Są one niezbędne do obsługi odwzorowania publickey.
- Okresowo należy sprawdzać, czy na wszystkich komputerach używających bezpiecznego systemu plików NFS jest uruchomiony demon **keyserv**.

Konfigurowanie bezpiecznego systemu plików NFS
Aby skonfigurować bezpieczny system plików NFS na serwerze głównym i na serwerach podrzędnych NIS, należy wykonać poniższą procedurę.

Więcej informacji na temat używania systemu plików NFS z systemem NIS+ zawiera książka *Network Information Services (NIS and NIS+) Guide*.

1. Na serwerze głównym NIS utwórz w pliku `/etc/publickey` systemu NIS pozycję dla każdego użytkownika; w tym celu użyj komendy **newkey** w następujący sposób:
   - dla zwykłego użytkownika wpisz:

     ```
     smit newkey
     ```

     LUB

     ```
     newkey -u nazwa użytkownika
     ```

     dla użytkownika root na hoście wpisz:

     ```
     newkey -h nazwa hosta
     ```

   - Użytkownicy mogą także ustanowić własne klucze publiczne za pomocą komendy **chkey** lub **newkey**.
2.

Utwórz odwzorowanie publickey systemu NIS, wykonując instrukcje opisane w podręczniku *Network Information Services (NIS and NIS+) Guide*. Odpowiadające mu odwzorowanie `publickey.byname` systemu NIS rezyduje tylko na serwerach NIS.

3. W pliku `/etc/rc.nfs` usuń komentarz z następujących sekcji:

```
#if [ -x /usr/sbin/keyserv ]; then
#  startsrc -s keyserv
#fi
#if [ -x /usr/lib/netsvc/yp/rpc.ypupdated -a -d /etc/yp/`domainname` ]; then
#  startsrc -s ypupdated
#fi
#DIR=/etc/passwd
#if [ -x /usr/lib/netsvc/yp/rpc.yppasswdd -a -f $DIR/passwd ]; then
#  startsrc -s yppasswdd
#fi
```

4. Uruchom demony **keyserv**, **ypupdated** i **yppasswdd** za pomocą komendy **startsrc**.

Aby skonfigurować bezpieczny system plików NFS na klientach NIS, uruchom demon **keyserv** za pomocą komendy **startsrc**.

Eksportowanie systemu plików za pomocą bezpiecznego systemu plików NFS
Bezpieczny system plików NFS można wyeksportować, wykonując poniższe procedury.

- Aby eksportować bezpieczny system plików NFS za pomocą programu SMIT, wykonaj następujące czynności:
  1. Sprawdź, czy system plików NFS jest uruchomiony. W tym celu wpisz komendę **lssrc -g nfs**. Dane wyjściowe wskazują, że demony nfsd i rpc.mountd są aktywne.
  2. Sprawdź, czy istnieje odwzorowanie publickey i czy uruchomiony jest demon keyserv. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie bezpiecznego systemu plików NFS” na stronie 292.
  3. Uruchom krótką ścieżkę **mknfsexp** programu **smit**.
  4. Podaj odpowiednie wartości pól: ŚCIEŻKA katalogu, który należy wyeksportować, TRYB eksportu katalogu i EKSPORTOWAĆ katalog teraz, przy ponownym uruchomieniu systemu czy jedno i drugie. W polu Użyć opcji BEZPIECZNIE? podaj wartość tak.
  5. Podaj inne parametry opcjonalne lub akceptuj wartości domyślne.
  6. Zamknij program SMIT. Jeśli plik `/etc/exports` nie istnieje, zostanie utworzony.
  7. Dla każdego katalogu, który chcesz eksportować, powtórz punkty od 3 do 6.
- Aby eksportować bezpieczny system plików NFS za pomocą edytora tekstu, wykonaj następujące czynności:
  1. W dowolnym edytorze tekstu otwórz plik `/etc/exports`.
  2. Utwórz wpis dla każdego katalogu, który ma być eksportowany. Użyj pełnej nazwy ścieżki tego katalogu. Począwszy od lewego marginesu wylicz każdy katalog, który ma być eksportowany. Żaden katalog nie powinien zawierać innego katalogu, który już został eksportowany. Dokumentacja pliku `/etc/exports` zawiera opis pełnej składni dla wpisów w pliku `/etc/exports`, włącznie z informacją o sposobie używania opcji secure.
  3. Zapisz i zamknij plik `/etc/exports`.
  4. Jeśli system plików NFS jest uruchomiony, wpisz:

     ```
     /usr/sbin/exportfs -a
     ```

     Użycie opcji **-a** w komendzie **exportfs** powoduje wysłanie do jądra wszystkich informacji zawartych w pliku `/etc/exports`.

- Aby tymczasowo eksportować system plików NFS (bez zmieniania pliku /etc/exports), należy wpisać:

```
exportfs -i -o secure /
nazwa_katalogu
```

  gdzie nazwa_katalogu jest nazwą eksportowanego systemu plików. Komenda **exportfs -i** określa, że podany katalog nie będzie szukany w pliku /etc/exports i że wszystkie opcje będą brane bezpośrednio z wiersza komend.

Podłączanie systemu plików za pomocą bezpiecznego systemu plików NFS
Bezpieczny katalog NFS można podłączyć w sposób jawny.

Aby jawnie podłączyć katalog bezpiecznego systemu plików NFS, wykonaj następujące czynności:

1. Sprawdź, czy serwer NFS wyeksportował katalog. W tym celu wpisz komendę:

   ```
   showmount -e NazwaSerwera
   ```

   gdzie NazwaSerwera jest nazwą serwera NFS. Komenda ta wyświetli nazwy katalogów wyeksportowanych przez serwer NFS. Jeśli na liście nie ma katalogu, który chcesz podłączyć, wyeksportuj go z serwera.
2. Ustanów lokalny punkt podłączenia za pomocą komendy **mkdir**. Aby system plików NFS wykonał podłączenie pomyślnie, katalog służący jako punkt podłączenia (lub uchwyt) dla podłączenia NFS musi istnieć. Katalog ten powinien być pusty, można go utworzyć tak samo jak każdy inny katalog, nie są potrzebne żadne atrybuty specjalne.
3. Sprawdź, czy istnieje odwzorowanie publickey i czy uruchomiony jest demon keyserv. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie bezpiecznego systemu plików NFS” na stronie 292.
4. Wpisz:

   ```
   mount -o secure NazwaSerwera:/zdalny/katalog /lokalny/katalog
   ```

   gdzie NazwaSerwera to nazwa serwera NFS, /zdalny/katalog to katalog na serwerze NFS, który chcesz podłączyć, a /lokalny/katalog to punkt podłączenia na kliencie NFS.

   Uwaga: Tylko użytkownik root może podłączyć bezpieczny system plików NFS.

Odwzorowanie tożsamości dla przedsiębiorstwa - architektura EIM

Nowoczesne środowisko sieciowe składa się ze złożonej grupy systemów i aplikacji, wymagającej zarządzania rejestrami wielu użytkowników. Radzenie sobie z rejestrami wielu użytkowników szybko zmienia się w duży problem administracyjny, który dotyczy użytkowników, administratorów i twórców aplikacji. Odwzorowanie tożsamości dla przedsiębiorstwa pozwala administratorom i twórcom aplikacji łatwiej podejść to tego problemu.

Ta sekcja opisuje problemy, przedstawia w skrócie istniejące rozwiązania i wyjaśnia rozwiązanie z użyciem architektury EIM.

Zarządzanie wieloma rejestrami użytkowników
Wielu administratorów zarządza sieciami zawierającymi różne systemy i serwery, z różnymi, unikalnymi metodami zarządzania użytkownikami poprzez różne rejestry użytkowników.

W takiej złożonej sieci administratorzy są odpowiedzialni za zarządzanie każdym identyfikatorem i hasłem użytkownika w wielu systemach. Ponadto administratorzy muszą często synchronizować te identyfikatory i hasła. Użytkownicy są obciążeni pamiętaniem wielu identyfikatorów i haseł oraz ich synchronizacją. Nakład pracy użytkowników i administratorów w takim środowisku jest kosztowny, administratorzy często spędzają dużo czasu, rozwiązując problemy z nieudanymi próbami zalogowania się do systemu i zerując zapomniane hasła, zamiast zarządzać siecią przedsiębiorstwa.

Problem zarządzania rejestrami wielu użytkowników dotyczy także twórców aplikacji, którzy chcą dostarczyć wielowarstwowe lub heterogeniczne aplikacje. Użytkownicy mają ważne dane biznesowe na wielu różnych typach systemów, każdy z tych systemów ma własne rejestry użytkowników. W wyniku tego programiści muszą tworzyć własne rejestry użytkowników i powiązane z tym mechanizmy zabezpieczeń dla swojej aplikacji. Rozwiązuje to wprawdzie problem twórcy aplikacji, ale zwiększa nakład pracy dla użytkowników i administratorów.

Bieżące rozwiązania dotyczące odwzorowywania tożsamości dla przedsiębiorstwa
Istnieje obecnie kilka przemysłowych metod rozwiązania problemu zarządzania rejestrami wielu użytkowników, ale dostarczają one niekompletnych rozwiązań. Na przykład protokół LDAP udostępnia rozproszone rejestry użytkowników. Jednak aby skorzystać z takiego rozwiązania jak LDAP, administratorzy muszą zarządzać jeszcze jednym rejestrem użytkowników i innymi metodami zabezpieczeń lub wymienić istniejące aplikacje, korzystające z tych rejestrów.

Skorzystanie z tego rozwiązania zmusza administratorów do zarządzania wieloma mechanizmami zabezpieczeń dla pojedynczych zasobów, zwiększając ich nakład pracy i potencjalnie zwiększając ryzyko naruszenia bezpieczeństwa. Gdy wiele mechanizmów obsługuje pojedynczy zasób, prawdopodobieństwo zmiany uprawnień za pomocą jednego mechanizmu i zapomnienia zmiany uprawnień dla jednego lub większej liczby mechanizmów jest znacznie większe. Na przykład ryzyko naruszenia bezpieczeństwa może zaistnieć, gdy użytkownik ma odpowiednio zabroniony dostęp poprzez jeden interfejs, ale dozwolony poprzez jeden lub większą liczbę innych interfejsów.

Po zakończeniu tego zadania administratorzy odkrywają, że rozwiązanie problemu nie jest kompletne. Ogólnie rzecz biorąc, przedsiębiorstwa zainwestowały za dużo pieniędzy w istniejące rejestry użytkowników i powiązane z nimi mechanizmy zabezpieczeń, aby taki typ rozwiązania był praktyczny. Tworzenie innego rejestru użytkowników i powiązanych z nim mechanizmów zabezpieczeń jest rozwiązaniem problemu dla dostawcy aplikacji, ale nie dla użytkowników i administratorów.

Innym rozwiązaniem jest użycie logowania. Dostępnych jest kilka produktów, umożliwiających administratorom zarządzanie plikami zawierającymi wszystkie identyfikatory i hasła użytkowników. Podejście to ma jednak kilka słabych punktów:

- Zajmuje się problemem tylko od strony użytkownika. Wprawdzie umożliwia użytkownikowi zalogowanie się w wielu systemach za pomocą jednego identyfikatora i hasła, ale nadal musi on mieć hasła w innych systemach lub potrzebuje zarządzać tymi hasłami.
- Wprowadza nowy problem, naruszając bezpieczeństwo, gdyż hasła są zapisane w pliku jawnym tekstem lub w sposób łatwy do rozszyfrowania. Hasła nie powinny nigdy być przechowywane w plikach w postaci jawnego tekstu i nie powinny być łatwo dostępne dla nikogo, włącznie z administratorem.
- Nie rozwiązuje to problemu twórców aplikacji z innych firm, którzy udostępniają heterogeniczne, wielowarstwowe aplikacje. Nadal muszą udostępniać własne rejestry użytkowników dla potrzeb swoich aplikacji.

Pomimo tych słabych punktów niektóre przedsiębiorstwa używają tych rozwiązań, gdyż są one trochę pomocne w problemie rejestru wielu użytkowników.

Użycie odwzorowania tożsamości dla przedsiębiorstwa
Architektura EIM opisuje relacje pomiędzy ludźmi lub jednostkami (takimi jak serwery plików czy wydruków) w przedsiębiorstwie i wiele tożsamości reprezentujących je w przedsiębiorstwie. Oprócz tego architektura EIM udostępnia zestaw funkcji API umożliwiający aplikacjom zadawanie pytań o te relacje.

Na przykład nadając komuś identyfikator użytkownika w jednym rejestrze użytkowników, można określić, który identyfikator w innym rejestrze użytkowników reprezentuje tę samą osobę. Jeśli użytkownik został uwierzytelniony jednym identyfikatorem i można odwzorować ten identyfikator na odpowiedni identyfikator w innym rejestrze użytkowników, użytkownik nie musi się uwierzytelniać ponownie. Niezbędna jest jedynie wiedza o tym, który identyfikator oznacza użytkownika w innym rejestrze użytkowników. Dlatego architektura EIM udostępnia uogólnioną funkcję odwzorowania identyfikatorów dla przedsiębiorstwa.

Możliwość odwzorowania identyfikatorów użytkownikach w różnych rejestrach użytkowników ma wiele zalet. Przede wszystkim aplikacje mają elastyczność korzystania z jednego rejestru przy uwierzytelnianiu

przy jednoczesnym wykorzystaniu całkiem innego rejestru w celu autoryzacji. Na przykład administrator może odwzorować identyfikator SAP w celu uzyskania dostępu do zasobów SAP.

Odwzorowanie tożsamości wymaga od administratora wykonania następujących czynności:

1. Utworzenia identyfikatorów EIM reprezentujących ludzi lub jednostki w przedsiębiorstwie.
2. Utworzenia definicji rejestrów EIM, opisujących istniejące rejestry użytkowników w przedsiębiorstwie.
3. Zdefiniowania relacji między identyfikatorami użytkowników w tych rejestrach a utworzonymi identyfikatorami EIM.

Nie trzeba wprowadzać zmian do istniejących rejestrów. Odwzorowania nie są potrzebne dla wszystkich użytkowników z rejestru użytkowników. Architektura EIM umożliwia odwzorowanie jeden do wielu (innymi słowy pojedynczy użytkownik z więcej niż jednym identyfikatorem w pojedynczym rejestrze użytkowników). Architektura EIM umożliwia także odwzorowanie wielu do jednego (innymi słowy wielu użytkowników może współużytkować pojedynczy identyfikator w pojedynczym rejestrze użytkowników, jednak z powodu bezpieczeństwa nie jest to doradzane). Administrator może utworzyć w EIM reprezentację dowolnego rejestru użytkowników dowolnego typu.

Architektura EIM nie wymaga kopiowania istniejących danych do nowego repozytorium i utrzymywania synchronizacji obu kopii. Jedyne nowe dane wprowadzane przez architekturę EIM, to informacje o relacjach. Administratorzy zarządzają tymi danymi w katalogu LDAP, który zapewnia elastyczność zarządzania danymi w jednym miejscu i tworzenie replik gdziekolwiek informacja jest wykorzystywana.

Kerberos

Protokół Kerberos jest usługą uwierzytelniania sieciowego umożliwiającą weryfikację tożsamości nazw użytkowników w sieciach fizycznych, które nie są zabezpieczone. Kerberos zapewnia uwierzytelnianie wzajemne, integrację danych oraz prywatność przy założeniu, że ruch w sieci jest wrażliwy na przechwytywanie, kontrolowanie i zastępowanie.

Nazwa użytkownika Kerberos jest unikalnym identyfikatorem używającym usług uwierzytelniania Kerberos. Protokół Kerberos sprawdza tożsamości bez polegania na uwierzytelnianiu przez system operacyjny hosta, za to bazuje na adresach hostów lub wymaga fizycznego bezpieczeństwa wszystkich hostów w sieci.

Bilety Kerberos uwiarygadniają tożsamość. Są dwa typy biletów: *bilet przydzielania biletu* oraz *bilet usługi*. Bilet przydzielania biletu jest używany w początkowym żądaniu weryfikacji tożsamości. Podczas logowania do hosta potrzebna jest weryfikacja tożsamości, taka jak hasło lub token. Po uzyskaniu biletu przydzielania biletu można go użyć w celu zażądania biletów dla konkretnych usług. Metoda dwóch biletów jest znana jako *zaufana osoba trzecia* Kerberos. Bilet przydzielania biletu uwierzytelnia użytkownika w serwerze Kerberos, a bilet usługi stanowi bezpieczne wprowadzenie do usługi.

Zaufana osoba trzecia lub pośrednik w uwierzytelnianiu Kerberos nosi nazwę *Centrum dystrybucji kluczy* (Key Distribution Center - KDC). KDC wystawia dla klientów wszystkie bilety Kerberos.

Przegląd bezpiecznych komend zdalnych

Poniżej przedstawiono szczegółowe informacje na temat bezpiecznych komend zdalnych.

Uwagi:

1. Począwszy od środowiska Distributed Computing Environment (DCE) wersja 2.2, serwer bezpieczeństwa DCE może zwracać bilety Kerberos, wersja 5.
2. Wszystkie bezpieczne komendy zdalne używają biblioteki Kerberos, wersja 5, udostępnianej przez usługę IBM uwierzytelniania sieciowego (Network Authentication Service - NAS) dostępną na dysku DVD Expansion Pack. Należy także zainstalować zestaw plików `krb5.client.rte`, który także jest dostępny na dysku DVD Expansion Pack.
3. Jeśli system operacyjny AIX jest migrowany z wykorzystaniem nośnika DVD i już zainstalowano Kerberos, skrypty instalacyjne wyświetlają zachętę do zainstalowania zestawu plików `krb5.client.rte` z dysku DVD Expansion Pack.
4. Jeśli system operacyjny AIX jest migrowany za pomocą zasobów NIM i już zainstalowano Kerberos, należy dodać `krb5` do katalogu lpp_source.

Bezpieczne komendy zdalne to **rlogin**, **rcp**, **rsh**, **telnet** i **ftp**. Komendy te są znane jako standardowa metoda uwierzytelniania AIX. Dodatkowe metody to Kerberos.

Jeśli używana jest metoda uwierzytelniania Kerberos wersja 5, klient pobiera bilet Kerberos wersja 5 z serwera bezpieczeństwa DCE lub serwera Kerberos. Bilet jest częścią bieżącego środowiska DCE użytkownika lub lokalnymi referencjami szyfrowanymi dla serwera TCP/IP, z którym chcą się połączyć. Demon na serwerze TCP/IP deszyfruje bilet. To działanie umożliwia identyfikację użytkownika przez serwer TCP/IP. Jeśli środowisko DCE lub lokalna nazwa użytkownika opisana na bilecie może uzyskać dostęp do konta użytkownika systemu operacyjnego, połączenie jest kontynuowane. Bezpieczne komendy zdalne obsługują klientów i serwery Kerberos z Kerberos wersja 5 i środowiska DCE.

Poza uwierzytelnianiem klienta Kerberos wersja 5 przekazuje referencje bieżącego użytkownika do serwera TCP/IP. Jeśli można je przekazywać, klient wysyła je do serwera jako bilet nadania biletu Kerberos. Po stronie serwera TCP/IP, jeśli użytkownik łączy się z serwerem bezpieczeństwa DCE, demon aktualizuje bilet nadania biletu do pełnych referencji DCE, używając komendy **k5dcecreds**.

Komenda **ftp** używa innej metody uwierzytelniania niż pozostałe bezpieczne komendy zdalne. Używa mechanizmu bezpieczeństwa GSSAPI do przekazywania uwierzytelniania pomiędzy komendą **ftp** a demonem **ftpd**. Używając podkomend **clear**, **safe** i **private**, klient ftp obsługuje szyfrowanie danych.

Komenda **ftp** udostępnia klientom i serwerom systemu operacyjnego wielobajtowe przesyłanie dla połączeń szyfrowanych. Standardy definiują tylko przesyłanie jednobajtowe dla połączeń szyfrowanych. Podczas łączenia się z innymi komputerami i używania szyfrowania danych, komenda **ftp** wprowadza ograniczenie przesyłania jednobajtowego.

Konfiguracja systemu
W przypadku wszystkich komend zdalnych mechanizm konfiguracji na poziomie systemu określa, które mechanizmy uwierzytelniania są dozwolone w tym systemie. Konfiguracja steruje połączeniami przychodzącymi i wychodzącymi.

Konfiguracja uwierzytelniania składa się z biblioteki `libauthm.a` oraz komend **lsauthent** i **chauthent**, które udostępniają wiersz komend dla procedur biblioteki **get_auth_methods** i **set_auth_methods**.

Metody uwierzytelniania definiują, która metoda jest używana do uwierzytelniania użytkownika w sieci. System obsługuje następujące metody uwierzytelniania:

- Kerberos, wersja 5, jest najczęściej używaną metodą, ponieważ jest podstawą dla środowiska DCE.
- Kerberos wersja 4 jest używana tylko przez bezpieczne komendy zdalne rlogin, rsh i rcp. Wprowadzono ją do obsługi kompatybilności z wcześniejszymi wersjami tylko w systemach SP. Bilet Kerberos wersja 4 nie jest aktualizowana do referencji DCE.

Jeśli skonfigurowano kilka metod uwierzytelniania, a pierwsza z nich nie zdoła nawiązać połączenia, klient próbuje się uwierzytelnić przy użyciu następnej skonfigurowanej metody uwierzytelniania.

Metody uwierzytelniania można konfigurować w dowolnej kolejności. Jedynym wyjątkiem jest sytuacja, w której standardowy system AIX musi być ostatnią skonfigurowaną metodą uwierzytelniania, ponieważ nie ma opcji rezerwy. Jeśli standardowy system AIX nie jest skonfigurowaną metodą uwierzytelniania, uwierzytelnianie hasła nie jest przeprowadzane i odrzucane są wszystkie próby połączenia używające tej metody.

Można także skonfigurować system bez żadnej metody uwierzytelniania. W tym przypadku system odrzuca wszystkie połączenia przychodzące i wychodzące, używając bezpiecznych komend zdalnych. Ponieważ protokół Kerberos, wersja 4, jest obsługiwany tylko z komendami **rlogin**, **rsh** i **rcp**, również system używający tylko protokołu Kerberos, wersja 4, nie zezwala na połączenia przy użyciu usługi telnet lub protokołu FTP.

Weryfikacja użytkownika w protokole Kerberos w wersji 5
Do sprawdzenia poprawności użytkownika można wykorzystać metodę uwierzytelniania przy użyciu protokołu Kerberos w wersji 5.

Podczas używania metody uwierzytelniania Kerberos wersja 5 klient TCP/IP pobiera bilet bezpieczeństwa zaszyfrowany dla serwera TCP/IP. Po deszyfrowaniu biletu serwer dysponuje bezpieczną metodą identyfikacji użytkownika (poprzez środowisko DCE lub lokalną nazwę użytkownika). Jednak serwer musi

określić, czy to środowisko DCE lub lokalna nazwa użytkownika może uzyskać dostęp do konta lokalnego. Przypisanie środowiska DCE lub lokalnej nazwy użytkownika jako lokalnego konta systemu operacyjnego jest obsługiwane przez współużytkowaną bibliotekę `libvaliduser.a`, która zawiera jedną podprocedurę o nazwie kvalid_user. Jeśli preferowana jest inna metoda przypisania, administrator systemu musi podać alternatywę dla biblioteki `libvaliduser.a`.

Konfiguracja DCE
Aby używać bezpiecznych komend zdalnych, muszą istnieć dwie nazwy użytkowników DCE dla każdego interfejsu sieciowego, z którym mogą być one połączone.

Te dwie nazwy użytkowników DCE, to:

```
host/PełnaNazwaInterfejsu
ftp/PełnaNazwaInterfejsu
```

gdzie *PełnaNazwaInterfejsu* oznacza nazwę interfejsu i nazwę domeny.

Konfiguracja lokalna
Aby można było używać bezpiecznych komend zdalnych, muszą istnieć dwie lokalne nazwy użytkowników dla każdego interfejsu sieciowego, z którym mogą one być połączone.

Te dwie lokalne nazwy użytkowników, to:

```
host/PełnaNazwaInterfejsu@NazwaDziedziny
ftp/PełnaNazwaInterfejsu@NazwaDziedziny
```

gdzie *PełnaNazwaInterfejsu* oznacza nazwę interfejsu i nazwę domeny, a *NazwaDziedziny* oznacza nazwę lokalnej dziedziny Kerberos, wersja 5.

Informacje pokrewne znajdują się w następujących publikacjach:

- Opis podprocedur get_auth_method i set_auth_method zawiera publikacja *Technical Reference: Communications, Volume 2*.
- Komendę chauthent zawiera publikacja *Commands Reference, Volume 1*
- Opis komendy lsauthent zawiera publikacja *Commands Reference, Volume 3*

Uwierzytelnianie w systemie operacyjnym AIX przy użyciu usługi uwierzytelniania sieciowego (NAS) lub usług innych niż systemu AIX
W systemach wcześniejszych niż AIX 6.1 moduł ładowalny KRB5 obsługiwał uwierzytelnianie Kerberos w środowisku usługi uwierzytelniania sieciowego (NAS), a moduł ładowalny KRB5A obsługiwał uwierzytelnianie Kerberos w środowisku systemów innych niż AIX. Od wersji AIX 6.1 moduł ładowalny KRB5 obsługuje uwierzytelnianie Kerberos w obu środowiskach, usługi uwierzytelniania sieciowego (NAS) i systemów innych niż AIX. Atrybut **is_kadmind_compat** w pliku `etc/security/methods.cfg` określa środowisko KRB5 lub KRB5A. Od wersji AIX 7.1 moduł ładujący KRB5A jest niedostępny. Z tego powodu konieczne jest użycie atrybutu **is_kadmind_compat** w pliku `etc/security/methods.cfg` w celu określenia środowiska KRB5 lub KRB5A.

Po skonfigurowaniu klienta Kerberos do uwierzytelniania w usłudze uwierzytelniania sieciowego, moduł ładujący KRB5 wykonuje uwierzytelnianie Kerberos i zarządza nazwami użytkowników Kerberos. Moduł ten umożliwia administratorowi systemu zarządzanie nazwami użytkowników Kerberos za pomocą komend administrowania użytkownikami systemu AIX. Aby skorzystać z zarządzania nazwami użytkowników, serwer Kerberos musi obsługiwać protokół administrowania kadmin. Usługa NAS zapewnia taką obsługę za pomocą demona **kadmind** (serwer Kerberos działający w systemie AIX).

Uwaga: Podczas konfigurowania klienta Kerberos należy określić, że uwierzytelnianie odbywa się z użyciem usługi NAS. W przeciwnym razie klient zostanie skonfigurowany pod kątem uwierzytelniania dla usług innych niż usługi systemu AIX i zarządzanie nazwami użytkowników będzie niedostępne.

Gdy protokół Kerberos jest używany dla systemu innego niż AIX, nazwy użytkowników Kerberos są zapisane w systemie innym niż AIX i nie można nimi zarządzać z systemu AIX za pomocą interfejsu bazy danych Kerberos kadmin. W takiej sytuacji nazwami użytkowników należy zarządzać oddzielnie, używając narzędzi Kerberos do zarządzania tymi nazwami. Narzędzia te mogą być częścią produktu Kerberos lub

mogą być zintegrowane z systemem operacyjnym (przykład: Windows 2000). Pierwotnym celem użycia protokołu Kerberos dla systemów innych niż AIX było udostępnienie uwierzytelniania dla serwerów Active Directory w systemie Windows 2000, gdzie zarządzanie nazwami użytkowników Kerberos jest wykonywane za pomocą narzędzi i interfejsów API Active Directory do zarządzania kontami. Jednak protokołu Kerberos dla systemów innych niż AIX można użyć z innymi zgodnymi KDC, w których interfejs administrowania Kerberos nie jest obsługiwany.

Instalowanie i konfigurowanie systemu pod kątem zintegrowanego logowania Kerberos przy użyciu IBM NAS

Implementacja IBM Kerberos usług Network Authentication Services (NAS) jest dostarczana w pakiecie rozszerzeń.

Aby zainstalować pakiet serwera Kerberos, wersja 5, należy zainstalować zestaw plików `krb5.server.rte`, uruchamiając komendę:

```
installp –aqXYgd . krb5.server
```

Jeśli komputer konfigurowany jako serwer Kerberos będzie używany również jako klient Kerberos, należy zainstalować cały pakiet Kerberos KRB5.

Środowisko DCE także zawiera zestaw programów narzędziowych klienta Kerberos o takich samych nazwach, jak programy narzędziowe Kerberos. Aby uniknąć kolizji w przestrzeni nazw pomiędzy komendami DCE i Kerberos (to znaczy pomiędzy komendami **klist**, **kinit** i **kdestroy**), komendy Kerberos są instalowane w katalogach `/usr/krb5/bin` i `/usr/krb5/sbin`.

Aby uruchamiać komendy Kerberos, należy podawać pełne nazwy ścieżek, chyba że katalogi Kerberos zostaną dodane do definicji PATH w następujący sposób:

```
export PATH=$PATH:/usr/krb5/sbin:/usr/krb5/bin
```

Uwaga: Pakiet SDK Java14 także instaluje komendę **kinit** i może ona poprzedzać inne komendy **kinit** w zmiennej środowiskowej PATH. Jeśli zamiast programu Java14 **kinit** potrzebne są komendy usługi uwierzytelniania sieciowego, należy przenieść program Java14 **kinit** w inne miejsce w definicji zmiennej PATH.

Dokumentacja usług uwierzytelniania sieciowego dostarczana jest w pakiecie `krb5.doc.`*język*`.pdf|html`, gdzie zmienna *język* oznacza obsługiwany język.

System operacyjny AIX zawiera dwa moduły bazy danych dostępne w celu utworzenia złożonego modułu ładowalnego: LDAP i BUILTIN. Moduł LDAP jest używany do uzyskiwania dostępu do informacji zapisanych w rejestrze LDAP (katalog), a moduł BUILTIN jest używany do uzyskiwania informacji zapisanych w rejestrze plików (lokalny system plików). Złożony moduł ładujący, który jest tworzony, ma zwykle nazwę KRB5files lub KRB5LDAP. Nazwy te wskazują, że protokół KRB5 jest używany albo do uwierzytelniania i dla plików lokalnych albo dla LDAP.

Usługa uwierzytelniania sieciowego także obsługuje zapisywanie informacji Kerberos albo w lokalnym systemie plików (wcześniejsza baza danych Kerberos), albo w LDAP. Możliwe są cztery konfiguracje:

- KRB5files z informacjami o serwerze Kerberos zapisanymi we wcześniejszej bazie danych Kerberos,
- KRB5files z informacjami o serwerze Kerberos zapisanymi w bazie danych LDAP Kerberos.
- KRB5LDAP z informacjami o serwerze Kerberos zapisanymi we wcześniejszej bazie danych Kerberos,
- KRB5LDAP z informacjami o serwerze Kerberos zapisanymi w bazie danych LDAP Kerberos.

Gdy mechanizmem zapisywania nazw użytkowników Kerberos lub informacji o użytkownikach i grupach AIX jest LDAP, protokół LDAP należy skonfigurować przed wywołaniem komend konfiguracyjnych Kerberos. Po skonfigurowaniu protokołu LDAP należy użyć komendy **mkkrb5srv**, aby skonfigurować serwery Kerberos.

Konfigurowanie serwera usługi uwierzytelniania sieciowego (NAS) z zapisami we wcześniejszej bazie danych

Użytkownik może skonfigurować KDC usługi uwierzytelniania sieciowego i serwery administracyjne z wcześniejszą bazą danych Kerberos oraz skonfigurować serwery usługi uwierzytelniania sieciowego za pomocą komendy **mkkrb5srv**.

Więcej informacji na temat używania komendy **mkkrb5srv** zawiera opis komendy **mkkrb5srv**.

Uwaga: Nie należy instalować oprogramowania serwera DCE i Kerberos w tym samym systemie fizycznym. Jeśli jest to konieczne, domyślne numery działających portów internetowych należy zmienić dla klientów i serwera DCE lub Kerberos. W tego rodzaju przypadkach taka zmiana może wpłynąć na współpracę z istniejącymi instalacjami DCE i Kerberos w danym środowisku. Informacje na temat współistnienia DCE i Kerberos zawiera dokumentacja Usług uwierzytelniania sieciowego.

Kerberos wersja 5 jest skonfigurowane do odrzucania żądań biletów z serwerów, których opóźnienie zegara KDC jest większe niż określone maksimum. Domyślnie maksymalne opóźnienie zegara wynosi 300 sekund (pięć minut). Kerberos wymaga, aby skonfigurować jakąś formę synchronizacji czasu między serwerami i klientami. Do synchronizacji czasu zaleca się używanie demona **xntpd** lub **timed**. Aby używać demona **timed**:

1. Skonfiguruj serwer KDC jako serwer czasu, uruchamiając demon **timed**:

   ```
   timed -M
   ```

2. Uruchom demon **timed** na każdym kliencie Kerberos:

   ```
   timed -t
   ```

3. Aby skonfigurować serwery KDC Kerberos i kadmin, uruchom komendę **mkkrb5srv**. Na przykład, aby skonfigurować Kerberos dla dziedziny MYREALM, serwera `sundial` i domeny `xyz.com`, uruchom komendę:

   ```
   mkkrb5srv -r MYREALM -s sundial.xyz.com -d xyz.com -a admin/admin
   ```

   Poczekaj kilka minut na uruchomienie komend **kadmind** i **krb5kdc** z pliku `/etc/inittab`.

Usługa uwierzytelniania sieciowego do zapisywania informacji używa miejsca dostępnego w systemie plików **/var**. Informacje te obejmują pliki bazy danych, dzienników i pamięci podręcznej informacji autoryzacyjnych uwierzytelnionych użytkowników. Wielkość tych plików może wzrastać z biegiem czasu. Należy zadbać, aby w systemie plików **/var** znajdowała się wystarczająca ilość wolnego miejsca na pomieszczenie tych informacji, regularnie monitorując ilość wolnego miejsca.

Poniżej przedstawiono typową komendę **mkkrb5srv**:

```
mkkrb5srv –r nazwa_dziedziny –s serwer_KDC –d nazwa_domeny –a nazwa_administratora
```

Wartości zmiennych, które zawiera Tabela 16 na stronie 300, zostały użyte w poniższym przykładzie do zilustrowania konfiguracji serwerów usługi uwierzytelniania sieciowego z wcześniejszą bazą danych.

*Tabela 16. Nazwy zmiennych komendy **mkkrb5srv***

Nazwa zmiennej	**Wartość zmiennej**
Nazwa dziedziny	MYREALM
Serwer KDC	kdcsrv.austin.ibm.com
Nazwa domeny	austin.ibm.com
Nazwa administratora	admin/admin

Jeśli konfiguracja serwera Kerberos już istnieje, można ją usunąć, używając komendy **mkkrb5srv –U** lub komendy **unconfig.krb5**.

Ostrzeżenie: Jeśli trzeba zachować istniejącą konfigurację serwera Kerberos, nie należy wykonywać poniższych kroków.

Poniższa procedura ilustruje sposób konfigurowania serwerów usługi uwierzytelniania sieciowego z wcześniejszą bazą danych.

1. Wprowadź następującą komendę:

   ```
   mkkrb5srv -r MYREALM -s kdcsrv.austin.ibm.com -d austin.ibm.com -a admin/admin
   ```

   Po wprowadzeniu tej komendy użytkownik jest proszony o podanie hasła do głównej bazy danych.

   Ponieważ usługa uwierzytelniania sieciowego nie obsługuje konfiguracji, w których KDC i serwer administracyjny znajdują się na różnych hostach, dla KDC i serwera administracyjnego zostanie użyty host lokalny. Zignoruj następujący komunikat o błędzie, jeśli zostanie wyświetlony: `Opcja -s nie jest obsługiwana`.
2. Po wyświetleniu zachęty wprowadź hasło do głównej bazy danych.
3. Po wyświetleniu zachęty wprowadź hasło użytkownika administracyjnego.

   Po wprowadzeniu hasła użytkownika administracyjnego komenda **mkkrb5srv** uruchomi demony **kadmind** i **krb5kdc**, znajdujące się w ścieżce `/etc/inittab`. Ten proces może potrwać kilka minut.
4. Sprawdź pozycje w pliku `/etc/inittab`, uruchamiając następujące komendy:

   ```
   lsitab krb5kdc
   lsitab kadm
   ```
5. Sprawdź, czy serwery KDC i kadmind zostały uruchomione, wprowadzając następującą komendę:

   ```
   ps -ef | grep -v grep | grep krb5
   ```

Komenda **mkkrb5srv** tworzy główne serwery administracyjne KDC i kadmind dla dziedziny Kerberos (MYREALM). Ponadto tworzy ona pliki konfiguracyjne, inicjuje bazę danych użytkownika, a także uruchamia serwery KDC i kadmind.

Działająca komenda **mkkrb5srv** wykonuje następujące operacje:

1. Tworzy plik `/etc/krb5/krb5.conf`. Wartości dla nazwy dziedziny, serwera administratora Kerberos oraz nazwy domeny są ustawiane zgodnie z wartościami podanymi w wierszu komend. W pliku `/etc/krb5/krb5.conf` ustawiane są również ścieżki dla plików protokołu default_keytab_name, kdc i admin_server.
2. Tworzy plik `/var/krb5/krb5kdc/kdc.conf`. W pliku `/var/krb5/krb5kdc/kdc.conf` ustawiane są wartości zmiennych *kdc_ports*, *kadmin_port*, *max_life*, *max_renewable_life*, *master_key_type* i *supported_enctypes*. Ustawiane są również ścieżki dla zmiennych *database_name*, *admin_keytab*, *acl_file*, *dict_file* i *key_stash_file*.
3. Tworzy plik `/var/krb5/krb5kdc/kadm5.acl`. Konfiguruje kontrolę dostępu dla nazw użytkowników admin, root i host.
4. Tworzy bazę danych i jedną nazwę użytkownika admin. Użytkownik jest proszony o podanie klucza głównego Kerberos oraz o podanie nazwy i ustawienie hasła dla tożsamości użytkownika będącego administratorem. W celu usuwania skutków awarii ważne jest, aby klucz główny oraz tożsamość i hasło użytkownika będącego administratorem były przechowywane w bezpiecznym miejscu.

Więcej informacji na ten temat zawierają sekcje “Przykładowe uruchomienia” na stronie 305 i “Komunikaty o błędach i działania podejmowane w celu odzyskiwania” na stronie 304.

Konfigurowanie serwera Kerberos z zapisami w LDAP
Serwery kadmin i KDC usługi uwierzytelniania sieciowego można skonfigurować pod kątem zintegrowanego logowania Kerberos za pomocą komendy **mkkrb5srv**.

Wartości zmiennych, które zawiera Tabela 17 na stronie 302, zostały użyte w poniższym przykładzie do zilustrowania konfiguracji komponentów serwera usługi uwierzytelniania sieciowego z zapisem w LDAP za pomocą komendy **mkkrb5srv**.

*Tabela 17. Nazwy zmiennych komendy **mkrb5srv***	
Nazwa zmiennej	**Wartość zmiennej**
Realm_Name	MYREALM
KDC_Server	kdcsrv.austin.ibm.com
Domain_Name	austin.ibm.com
Admin_Name	admin/admin
Serwer LDAP	kdcsrv.austin.ibm.com
Nazwa administratora LDAP	cn=root
Hasło administratora LDAP	secret

Poniższa procedura stanowi przykład ilustrujący konfigurowanie komponentów serwera usługi uwierzytelniania sieciowego z zapisem w LDAP za pomocą komendy **mkkrb5srv**.

1. Uruchom komendę:

```
mkkrb5srv -r MYREALM -s kdcsrv.austin.ibm.com -d austin.ibm.com\
-a admin/admin -l kdcsrv.austin.ibm.com -u cn=root -p secret
```

2. Sprawdź, czy serwery KDC i kadmind zostały uruchomione, uruchamiając następującą komendę:

```
ps -ef | grep -v grep | grep krb5
```

Uruchomienie komendy **mkkrb5srv** z LDAP generuje wyniki podobne do uruchomienia tej komendy z wcześniejszą konfiguracją bazy danych. Jednak w przypadku użycia LDAP, bazy danych nie są tworzone w lokalnym systemie plików. Tworzony jest natomiast plik `.kdc_ldap_data` w pliku `/var/krb5/krb5kdc`, który będzie zawierał informacje o LDAP.

Więcej informacji na temat składni zawiera opis komendy **mkkrb5srv**.

Konfigurowanie zintegrowanego logowania Kerberos
Po zakończeniu instalacji protokołu Kerberos należy skonfigurować system pod kątem używania protokołu Kerberos jako głównej metody uwierzytelniania użytkowników.

Aby skonfigurować systemy w celu używania Kerberos jako głównej metody uwierzytelniania użytkowników, należy uruchomić komendę **mkkrb5clnt** z następującymi parametrami:

```
mkkrb5clnt -c KDC -r dziedzina -a admin -s serwer -d domena -A -i baza_danych -K -T
```

Wartości zmiennych, które zawiera Tabela 18 na stronie 302, zostały użyte w poniższym przykładzie do zilustrowania konfiguracji systemu pod kątem zintegrowanego logowania Kerberos z lokalnym systemem plików jako repozytorium użytkownika/grupy systemu AIX.

*Tabela 18. Nazwy zmiennych komendy **mkkrb5clnt***	
Nazwa zmiennej	**Wartość zmiennej**
Nazwa dziedziny	MYREALM
Serwer KDC	kdcsrv.austin.ibm.com
Nazwa domeny	austin.ibm.com
Serwer administracyjny	kdcsrv.austin.ibm.com
Nazwa administratora	admin/admin

*Tabela 18. Nazwy zmiennych komendy **mkkrb5clnt** (kontynuacja)*	
Nazwa zmiennej	**Wartość zmiennej**
Baza danych użytkowników/grup AIX	pliki

Poniższa komenda ilustruje sposób konfiguracji systemu pod kątem zintegrowanego logowania Kerberos z lokalnym systemem plików jako repozytorium użytkowników/grup systemu AIX.

Uruchom komendę:

```
mkkrb5clnt -r MYREALM -c kdcsrv.austin.ibm.com -s kdcsrv.austin.ibm.com\
-a admin/admin -d austin.ibm.com -A -i files -K -T
```

Komenda uruchomiona w poprzednim przykładzie wykonuje następujące czynności:

1. Komenda ta tworzy plik `/etc/krb5/krb5.conf`. Wartości dla nazwy dziedziny, serwera administratora Kerberos oraz nazwy domeny są ustawiane zgodnie z wartościami podanymi w wierszu komend. Aktualizowane są również ścieżki dla plików dziennika `default_keytab_name`, `kdc` i `kadmin`.
2. Opcja **-i** konfiguruje w pełni zintegrowane logowanie. Podana baza danych określa miejsce przechowywania informacji identyfikujących użytkownika systemu AIX. Jest to inna sytuacja niż w przypadku użytkownika Kerberos. Pamięć do przechowywania nazw użytkowników Kerberos konfigurowana jest podczas konfigurowania protokołu Kerberos.
3. Opcja **-K** konfiguruje Kerberos jako domyślną metodę uwierzytelniania. Umożliwia to uwierzytelnianie użytkowników podczas logowania przy użyciu Kerberos.
4. Opcja **-A** dodaje pozycję w bazie danych Kerberos w celu utworzenia użytkownika root i administratora dla Kerberos.
5. Opcja **-T** uzyskuje bilet nadania biletu administratora serwera.

Uwaga: Nie należy używać opcji **-D** w komendzie **mkkrb5clnt** do skonfigurowania środowiska klienta Kerberos do uwierzytelniania w usłudze uwierzytelniania sieciowego IBM (NAS). Jeśli nie zostanie podana opcja **-D** komendy **mkkrb5clnt**, atrybut **is_kadmind_compat** nie zostanie dołączony w pliku `/usr/lib/security/methods.cfg` i środowisko klienta Kerberos zostaje skonfigurowane do uwierzytelniania w usłudze IBM NAS.

Sprawdź konfigurację, weryfikując plik `/etc/krb5/krb5.conf`. Poniżej został przedstawiony przykład pliku `/etc/krb5/krb5.conf` na komputerze klienta:

```
[libdefaults]
     default_realm = MYREALM
     default_keytab_name = FILE:/etc/krb5/krb5.keytab
     default_tkt_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-md5 des-cbc-crc
     default_tgs_enctypes = des3-cbc-sha1 arcfour-hmac aes256-cts des-cbc-md5 des-cbc-crc
[realms]
     MYREALM = {
        kdc = kdcsrv.austin.ibm.com:88
        admin_server = kdcsrv.austin.ibm.com:749
        default_domain = austin.ibm.com
     }
[domain_realm]
    .austin.ibm.com = MYREALM
    kdcsrv.austin.ibm.com = MYREALM
[logging]
     kdc = FILE:/var/krb5/log/krb5kdc.log
     admin_server = FILE:/var/krb5/log/kadmin.log
     default = FILE:/var/krb5/log/krb5lib.log
```

Uwaga: Jeśli do zapisu nazwy użytkownika Kerberos użyto LDAP, to plik `krb5.conf` będzie zawierał następujący wiersz w sekcji `[realms]`:

```
vdb_plugin_lib = /usr/lib/libkrb5ldplug.a
```

Jeśli system zainstalowano w innej domenie DNS niż KDC, wykonaj następujące czynności dodatkowe:

1. Zmodyfikuj plik /etc/krb5/krb5.conf i dodaj nową pozycję po [domain realm].
2. Przypisz inną domenę do dziedziny.

Na przykład, jeśli klient z dziedziny domeny abc.xyz.com ma być dodany do dziedziny MYREALM, należy zmodyfikować plik /etc/krb5/krb5.conf w następujący sposób:

```
[domain realm]
     .austin.ibm.com = MYREALM
     .raleigh.ibm.com = MYREALM
```

Po zakończeniu konfiguracji usługi uwierzytelniania sieciowego proces logowania w systemie operacyjnym pozostaje niezmieniony. Po pomyślnym zalogowaniu użytkownicy będą mieli bilety nadania biletu Kerberos powiązane z ich działającymi procesami. Zmienna środowiskowa $KRB5CCNAME użytkownika wskazuje na ten bilet nadania biletu. Aby sprawdzić, czy logowanie jest pomyślne i czy użytkownik ma bilet nadania biletu, należy użyć komendy **klist**.

Uwaga: Po uruchomieniu komendy **mkkrb5clnt** do pliku methods.cfg dodawana jest następująca sekcja.

```
KRB5:
        program = /usr/lib/security/KRB5
        program_64 = /usr/lib/security/KRB5_64
        options = is_kadmind_compat=yes

KRB5files:
        options = db=BUILTIN,auth=KRB5
```

Więcej informacji na temat:

- komendy **mkkrb5clnt** zawiera opis komendy **mkkrb5clnt**,
- pliku methods.cfg zawiera opis pliku methods.cfg.

Komunikaty o błędach i działania podejmowane w celu odzyskiwania
Błędy, które mogą wystąpić podczas używania komendy **mkkrb5srv**:

- Jeśli pliki krb5.conf, kdc.conf lub kadm5.acl już istnieją, komenda **mkkrb5srv** nie zmienia wartości. Wyświetlany jest komunikat informujący o ich istnieniu. Wszystkie wartości konfiguracji można zmienić, modyfikując pliki krb5.conf, kdc.conf lub kadm5.acl.
- Jeśli jakieś dane będą błędne i nie zostanie utworzona żadna baza danych, należy usunąć pliki konfiguracyjne i ponownie uruchomić komendę.
- W przypadku niespójności pomiędzy bazą danych a wartościami konfiguracyjnymi należy usunąć bazę danych z katalogu /var/krb5/krb5kdc/* i powrócić do komendy.
- Należy sprawdzić, czy demony **kadmind** i **krb5kdc** zostały uruchomione na komputerze. Aby to zrobić, należy użyć komendy **ps**. Jeśli nie zostały one uruchomione, należy przejrzeć plik protokołu.

Błędy, które mogą wystąpić podczas używania komendy **mkkrb5clnt**:

- Nieprawidłowe wartości dla krb5.conf można usunąć, modyfikując plik /etc/krb5/krb5.conf.
- Nieprawidłowe wartości dla opcji **-i** można usunąć, modyfikując plik /usr/lib/security/methods.cfg.

Eliminowanie zależności od demona kadmind podczas uwierzytelniania innego niż KRB5

Moduł ładujący KRB5 powoduje opóźnienie, jeśli demon kadmind jest niedostępny i jeśli używany jest mechanizm uwierzytelniania inny niż KRB5, na przykład pojedyncze logowanie (SSO). Tę zależność można wyeliminować, ustawiając parametr kadmind_timeout w pliku **methods.cfg**.

Dopuszczalne są wartości: kadmind_timeout=<sekundy>, gdzie wartość określająca sekundy musi być większa od 0.

Gdy moduł ładujący KRB5 próbuje nawiązać połączenie z wyłączonym serwerem kadmind, następuje przekroczenie limitu czasu protokołu TCP. Parametr kadmind_timeout zapobiega dalszemu opóźnieniu po początkowym przekroczeniu limitu czasu protokołu TCP. Parametr kadmind_timeout określa okno

czasowe dla próby nawiązania przez moduł ładujący KRB5 następnego połączenia po początkowym przekroczeniu limitu czasu protokołu TCP. Jeśli serwer kadmind działa, obowiązuje zachowanie domyślne.

Domyślnie parametr `kadmind_timeout` jest wyłączony. Aby włączyć parametr `kadmind_timeout`, należy zmodyfikować plik `methods.cfg` w następujący sposób:

```
KRB5:
        program = /usr/lib/security/KRB5
        options = kadmind_timeout=300
KRB5files:
        options = db=BUILTIN,auth=KRB5
```

Tworzone pliki
Komenda **mkkrb5srv** tworzy następujące pliki:

- `/etc/krb5/krb5.conf`
- `/var/krb5/krb5kdc/kadm5.acl`
- `/var/krb5/krb5kdc/kdc.conf`

Komenda **mkkrb5clnt** tworzy następujące pliki:

- `/etc/krb5/krb5.conf`

Opcja **mkkrb5clnt -i** *pliki* dodaje następującą sekcję do pliku `/usr/lib/security/methods.cfg`:

```
KRB5:
        program =
        options =
KRB5files:
        options =
```

Przykładowe uruchomienia
Niniejsza sekcja zawiera informacje o przykładowych uruchomieniach.

Poniżej przedstawiono przykład komendy **mkkrb5srv**:

```
# mkkrb5srv -r MYREALM -s sundial.xyz.com -d xyz.com -a admin/admin
```

Zostaną wyświetlone dane wyjściowe zbliżone do następujących:

```
  Fileset
Level  State      Description
  ----------------------------------------------------------------------------
Path: /usr/lib/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                                 Server

Path: /etc/objrepos
  krb5.server.rte            1.3.0.0  COMMITTED  Network Authentication Service
                                                 Server
```

```
The -s option is not supported.
The administration server will be the local host.
Initializing configuration...
Creating /etc/krb5/krb5.conf...
Creating /var/krb5/krb5kdc/kdc.conf...
Creating database files...
Initializing database '/var/krb5/krb5kdc/principal' for realm 'MYREALM'
master key name 'K/M@MYREALM'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter database Master Password:
Re-enter database Master Password to verify:
WARNING: no policy specified for admin/admin@MYREALM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Enter password for principal "admin/admin@MYREALM":
Re-enter password for principal "admin/admin@MYREALM":
Principal "admin/admin@MYREALM" created.
```

```
Creating keytable...
Creating /var/krb5/krb5kdc/kadm5.acl...
Starting krb5kdc...
krb5kdc was started successfully.
Starting kadmind...
kadmind was started successfully.
The command completed successfully.
Restarting kadmind and krb5kdc
```

Poniżej przedstawiono przykład komendy **mkkrb5clnt**:

```
mkkrb5clnt -r MYREALM -c sundial.xyz.com -s sundial.xyz.com \
           -a admin/admin -d xyz.com -i files -K -T -A
```

Zostaną wyświetlone dane wyjściowe zbliżone do następujących:

```
Initializing configuration...
Creating /etc/krb5/krb5.conf...
The command completed successfully.
Password for admin/admin@MYREALM:
Configuring fully integrated login
Authenticating as principal admin/admin with existing credentials.
WARNING: no policy specified for host/diana.xyz.com@MYREALM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Principal "host/diana.xyz.com@MYREALM" created.

Administration credentials NOT DESTROYED.
Authenticating as principal admin/admin with existing credentials.

Administration credentials NOT DESTROYED.
Authenticating as principal admin/admin with existing credentials.
Principal "kadmin/admin@MYREALM" modified.

Administration credentials NOT DESTROYED.
Configuring Kerberos as the default authentication scheme
Making root a Kerberos administrator
Authenticating as principal admin/admin with existing credentials.
WARNING: no policy specified for root/diana.xyz.com@MYREALM;
  defaulting to no policy. Note that policy may be overridden by
  ACL restrictions.
Enter password for principal "root/diana.xyz.com@MYREALM":
Re-enter password for principal "root/diana.xyz.com@MYREALM":
Principal "root/diana.xyz.com@MYREALM" created.

Administration credentials NOT DESTROYED.
Cleaning administrator credentials and exiting.
```

Eliminowanie zależności od demona kadmind podczas uwierzytelniania
Moduł ładowania KRB5 może nie przeprowadzić uwierzytelniania, jeśli nie będzie dostępny demon **kadmind**. Tę zależność można wyeliminować przez ustawienie parametru *kadmind* w pliku `methods.cfg`.

Możliwe wartości to `kadmind=no` lub `kadmind=false` w przypadku wyłączania wyszukiwań demona **kadmind** i `kadmind=yes` lub `kadmind=true` w przypadku włączania wyszukiwań demona **kadmind** (wartością domyślną jest yes). Gdy ta opcja ma wartość no, podczas uwierzytelniania nie następuje połączenie z demonem **kadmind**. Dlatego użytkownicy mogą się zalogować do systemu bez względu na status demona **kadmind** (podając prawidłowe hasło, gdy system o nie zapyta). Jednak jeśli demon nie jest dostępny (na przykład został wyłączony lub komputer nie jest dostępny), komendy systemu AIX do administrowania użytkownikami, takie jak **mkuser**, **chuser** lub **rmuser**, nie będą działały i nie będzie można administrować zintegrowanymi użytkownikami Kerberos.

Wartością domyślną parametru *kadmind* jest `yes`. Oznacza to, że podczas uwierzytelniania przeprowadzane jest wyszukiwanie demona **kadmind**. W tym przypadku, jeśli demon nie jest dostępny, uwierzytelnianie może potrwać dłużej.

Aby wyłączyć sprawdzanie demona **kadmind** podczas uwierzytelniania, należy zmodyfikować sekcje pliku `methods.cfg`:

```
KRB5:
        program = /usr/lib/security/KRB5
        options = kadmind=no
```

```
KRB5files:
        options = db=BUILTIN,auth=KRB5
```

Gdy demon **kadmind** nie będzie dostępny, użytkownik root nie będzie mógł zmieniać haseł użytkowników. W przypadku, gdy użytkownik zapomni hasła, demon **kadmind** musi być dostępny. Także jeśli użytkownik wprowadzi w wierszu logowania nazwę główną Kerberos, nazwa podstawowa nazwy głównej zostanie obcięta zgodnie z ograniczeniem długości nazwy dla użytkownika systemu AIX. Ta obcięta nazwa będzie używana do odtwarzania informacji identyfikacyjnych użytkownika systemu AIX (na przykład, aby odtworzyć wartość katalogu osobistego).

Jeśli demon **kadmind** nie będzie dostępny (będzie wyłączony lub nieosiągalny), komenda **mkuser** spowoduje wyświetlenie następującego błędu:

```
3004-694 Error adding "krb5user": You do not have permission
(3004-694 błąd podczas dodawania użytkownika "krb5user": Brak uprawnień).
```

Jeśli parametr *kadmind* ma wartość no lub demon **kadmind** jest niedostępny, system nie może sprawdzić istnienia nazwy użytkownika w bazie danych Kerberos, tak więc nie wczyta atrybutów dotyczących Kerberos. Ta sytuacja powoduje powstanie niepełnych lub nieodpowiednich wyników. Na przykład komenda **lsuser** może nie zgłosić żadnych użytkowników dla zapytania ALL.

Ponadto komenda **chuser** będzie zarządzała tylko atrybutami dotyczącymi systemu AIX, ale nie będzie zarządzała atrybutami dotyczącymi protokołu Kerberos. Komenda **rmuser** nie usunie użytkownika Kerberos, a komenda **passwd** nie będzie działała w przypadku użytkowników uwierzytelnianych za pomocą protokołu Kerberos.

Jeśli sieć, w której rezyduje demon **kadmind**, nie jest dostępna, czas odpowiedzi będzie dłuższy. Ustawienie opcji demona kadmind w pliku `methods.cfg` na wartość no wyeliminuje opóźnienia podczas uwierzytelniania, gdy komputer nie jest dostępny.

Gdy demon **kadmind** jest wyłączony, użytkownicy, których hasła utracą ważność, nie mogą się zalogować ani zmienić haseł.

Gdy zostanie wprowadzone ustawienie `kadmind=no`, ale demon **kadmind** jest uruchomiony, można uruchomić następujące komendy: **login**, **su**, **passwd**, **mkuser**, **chuser** i **rmuser**.

Kerberos a usługa uwierzytelniania sieciowego: rozwiązywanie problemów
W tym miejscu podano informacje o rozwiązywaniu problemów dotyczących klientów Kerberos korzystających z serwera Kerberos w systemie operacyjnym AIX.

Moduł LDAP zapisuje informacje o błędach i informacje debugowania w podsystemie syslog.

Usługa uwierzytelniania sieciowego IBM (NAS) używa własnych plików dziennika do rejestrowania żądań skierowanych do centrum KDC i demonów **kadmind**. Pliki te są określone w sekcji `[logging]` pliku `krb5.conf`. Domyślne położenia tych plików to `/var/krb5/log/krb5kdc.log` i `/var/krb5/log/kadmin.log`.

Jeśli problem dotyczy serwera IBM Tivoli Directory Server, należy przejrzeć pliki dziennika wygenerowane przez serwer IBM Tivoli Directory Server. Domyślnie są to pliki `/var/ldap/ibmslapd.log` i `/var/ldap/db2cli.log`.

- ***Jak utworzyć użytkownika systemu AIX uwierzytelnianego przy użyciu protokołu Kerberos?***

  Użytkownik root musi uzyskać referencje Kerberos przyznające wymagane uprawnienia do wykonywania zadań administracyjnych. Zadania administracyjne są wykonywane na następującym serwerze KDC: kdcsrv.austin.ibm.com.

Utwórz konto użytkownika AIX (foo) i nazwę użytkownika Kerberos (foo@MYREALM) w bazie danych Kerberos, wprowadzając następujące komendy:

```
kinit root/kdcsrv.austin.ibm.com
mkuser -R KRB5files SYSTEM=KRB5files registry=KRB5files foo
```

Komendy te ponadto uwierzytelniają użytkownika na potrzeby plików KRB5files.

Jeśli skonfigurowano protokół LDAP, używając komendy **mksecldap**, użytkownika systemu AIX uwierzytelnianego przy użyciu protokołu Kerberos można utworzyć, wprowadzając następującą komendę:

```
mkuser –R KRB5LDAP SYSTEM=KRB5LDAP registry=KRB5LDAP foo
```

- ***Jak usunąć użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby usunąć użytkownika uwierzytelnionego przy użyciu protokołu Kerberos, uruchom następującą komendę:

  ```
  rmuser –R KRB5files foo
  ```

  Jeśli skonfigurowano protokół LDAP, używając komendy **mksecldap**, użytkownika uwierzytelnianego przy użyciu protokołu Kerberos można usunąć, wprowadzając następującą komendę:

  ```
  rmuser –R KRB5LDAP foo
  ```

- ***Jak zmienić hasło użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby zmienić hasło użytkownika uwierzytelnionego przy użyciu protokołu Kerberos, uruchom następującą komendę:

  ```
  passwd –R KRB5files foo
  ```

- ***Czym są rozszerzone atrybuty Kerberos w systemie AIX?***

  Informacjami o nazwach użytkowników Kerberos manipuluje się za pomocą rozszerzonych atrybutów AIX, używając komend AIX **lsuser** i **chuser**. Można wyświetlić tylko te atrybuty, które mają tryb dostępu GET. Atrybutom, które mają tryb dostępu SET, użytkownik uprzywilejowany (w systemie AIX jest to użytkownik root) może przypisywać wartości. Użytkownik uwierzytelniony przy użyciu protokołu Kerberos w systemie AIX może wyświetlać swoje własne atrybuty rozszerzone Kerberos i inne dozwolone atrybuty AIX, takie jak id, pgrp, groups, gecos, home i shell.

  Tabela 19 na stronie 308 zawiera atrybuty rozszerzone Kerberos w systemie AIX i ich tryby dostępu.

Tabela 19. Atrybuty rozszerzone Kerberos w systemie AIX i ich tryby dostępu

Nazwa atrybutu rozszerzonego	Opis	Tryb dostępu
krb5_principal_name	Nazwa użytkownika powiązana z nazwą użytkownika AIX.	GET
krb5_principal	Taki sam, jak dla atrybutu krb5_principal_name.	GET
krb5_realm	Nazwa dziedziny Kerberos, do której należy nazwa użytkownika.	GET
krb5_last_pwd_change	Czas ostatniej zmiany hasła dla danej nazwy użytkownika.	GET
krb5_attributes	Zestaw atrybutów używanych przez centrum KDC.	GET/SET

Tabela 19. Atrybuty rozszerzone Kerberos w systemie AIX i ich tryby dostępu (kontynuacja)

Nazwa atrybutu rozszerzonego	Opis	Tryb dostępu
krb5_mod_name	Nazwa użytkownika, który jako ostatni zmodyfikował tę nazwę użytkownika.	GET
krb5_mod_date	Czas ostatniej modyfikacji nazwy użytkownika.	GET
krb5_kvno	Wersja bieżącego klucza nazwy użytkownika (hasło).	GET/SET
krb5_mkvno	Numer wersji klucza głównego bazy danych. Ten atrybut jest dostępny ze względu na kompatybilność z innymi implementacjami. To pole ma wartość 0.	GET
krb5_max_renewable_life	Maksymalny odnawialny czas życia biletu wystawionego przez tę nazwę użytkownika.	GET/SET
krb5_names	Lista par nazwa:nazwa_hosta. To pole jest przeznaczone do wykorzystania w przyszłości. Tego atrybutu nie należy modyfikować.	GET/SET

Atrybut rozszerzony krb5_attributes reprezentuje zestaw atrybutów nazwy użytkownika Kerberos dostępnych do użycia przez centrum KDC. Do zmodyfikowania tych atrybutów Kerberos użytkownik uprzywilejowany może użyć komendy **chuser**.

```
chuser -R KRB5files krb5_attributes=+requires_preauth krb5user
```

Aby ustawić opcję, dodaj znak plus (+) przed tą opcją. Aby zresetować opcję, dodaj znak minus (-) przed tą opcją. Na przykład:

+*nazwa_atrybutu* ustawia opcję

-*nazwa_atrybutu* resetuje opcję

Uwaga: Podczas tworzenia użytkownika ustawiane są wszystkie atrybuty oprócz następujących: requires_hwauth, needchange, password_changing_service i support_desmd5.

Poniższa lista zawiera atrybuty dla atrybutu rozszerzonego krb5_attributes:

allow_postdated
Jeśli zostanie ustawiony, dla nazwy użytkownika można wystawiać bilety postdatowane.

allow_forwardable
Jeśli zostanie ustawiony, dla nazwy użytkownika można wystawiać bilety przekazywalne.

allow_tgs_req
Jeśli zostanie ustawiony, bilety usług dla nazwy użytkownika są wystawiane za pomocą biletu nadania biletu.

allow_renewable
Jeśli zostanie ustawiony, dla nazwy użytkownika można wystawiać bilety odnawialne.

allow_proxiable
Jeśli zostanie ustawiony, dla nazwy użytkownika można wystawiać bilety pośrednie.

allow_dup_skey
Jeśli zostanie ustawiony, dla nazwy użytkownika włączone jest uwierzytelnianie użytkownik-użytkownik.

allow_tix
Jeśli zostanie ustawiony, dla nazwy użytkownika wystawiane są bilety.

requires_preauth
Jeśli zostanie ustawiony, przed wystawieniem biletu wymagane jest uwierzytelnianie wstępne oprogramowania.

requires_hwauth
Jeśli zostanie ustawiony, przed wystawieniem biletu dla nazwy użytkownika wymagane jest programowe uwierzytelnianie wstępne sprzętu.

needchange
Jeśli zostanie ustawiony, klucz (hasło) dla nazwy użytkownika musi zostać zmieniony przed wystawieniem biletów.

Uwaga: Jeśli ustawiono opcję needchange, podczas kolejnej próby zalogowania się wyświetlana jest zachęta do zmiany hasła. W takiej sytuacji użytkownik zostaje uwierzytelniony (za pomocą protokołu Kerberos), ale nie ma biletu nadania biletu. Aby uzyskać bilet nadania biletu, użytkownik musi wywołać komendę **kinit**. Opcja needchange ma zastosowanie tylko do protokołu Kerberos korzystającego z modułu usługi uwierzytelniania sieciowego.

allow_svr
Jeśli zostanie ustawiony, dla nazwy użytkownika można wystawiać bilety usług.

password_changing_service
Jeśli zostanie ustawiony, nazwa użytkownika staje się specjalną nazwą użytkownika dla usługi zmiany haseł.

support_desmd5
Jeśli zostanie ustawiony, centrum KDC może wystawiać bilety korzystające z algorytmu sumy kontrolnej RSA MD5.

Uwaga: Ustawienie tego atrybutu może spowodować problemy ze współdziałaniem.

- ***Jak wyświetlić rozszerzone atrybuty Kerberos w systemie AIX?***

  Aby wyświetlić rozszerzone atrybuty Kerberos w systemie AIX, uruchom następującą komendę:

  ```
  lsuser –R KRB5files foo
  ```

  Ponadto istnieje możliwość wyświetlenia konkretnych atrybutów rozszerzonych za pomocą opcji –a. Na przykład:

  ```
  lsuser -R KRB5files -f -a krb5_principal krb5_principal_name krb5_realm
  ```

- ***Jak zmodyfikować rozszerzone atrybuty Kerberos w systemie AIX?***

  Tylko użytkownik uprzywilejowany może modyfikować następujące atrybuty rozszerzone z trybem dostępu SET: krb5_kvno, krb5_max_renewable_life, krb5_attributes i krb5_names.

  – Aby zmienić maksymalny odnawialny czas życia na pięć dni dla każdego biletu wystawionego dla foo, wprowadź następującą komendę:

    ```
    chuser -R KRB5files krb5_max_renewable_life=432000 foo
    ```

  – Aby zmienić numer wersji klucza (hasła) nazwy użytkownika powiązanej z foo, wprowadź następującą komendę:

    ```
    chuser -R KRB5files krb5_kvno=4 foo
    ```

– Aby ustawić wszystkie atrybuty nazwy użytkownika Kerberos, które zawiera Tabela 19 na stronie 308, wprowadź komendy:

```
chuser -R KRB5files krb5_attributes=+allow_postdated,+allow_forwardable,\
+allow_tgs_req,+allow_renewble,+allow_proxiable,+allow_dup_skey,+allow_tix,\
+requires_preauth,+requires_hwath,+needchange,+allow_svr,\
+password_changing_service,+support_desmd5 foo
```

```
lsuser -R KRB5files -a krb5_attributes foo
```

– Aby zresetować wszystkie atrybuty nazwy użytkownika Kerberos, które zawiera Tabela 19 na stronie 308, wprowadź komendy:

```
chuser -R KRB5files krb5_attributes=-allow_postdated,-allow_forwardable,\
-allow_tgs_req,-allow_renewable,-allow_proxiable,-allow_dup_skey,\
-allow_tix,-requires_preauth,-requires_hwauth,-needchange,-allow_svr,\
-password_changing_service,-support_desmd5 foo
```

```
lsuser -R KRB5files -a krb5_attributes foo
```

– Aby zmienić krb5_names i dodać parę nazwa użytkownika/nazwa hosta w systemie AIX, wprowadź komendy:

```
lsuser -R KRB5files -a krb5_names foo
```

```
chuser -R KRB5files krb5_names=bar:greenjeans.austin.ibm.com foo
```

```
lsuser -R KRB5files -a krb5_names foo
```

- ***Jak wyświetlić wszystkich użytkowników zdefiniowanych w KRB5files?***

  Aby wyświetlić wszystkich użytkowników uwierzytelnionych przy użyciu protokołu Kerberos, uruchom następującą komendę:

```
lsuser -R KRB5files -a registry ALL
```

- ***Jak przekształcić użytkownika systemu AIX w użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby przekształcić użytkownika AIX w użytkownika uwierzytelnianego przy użyciu protokołu Kerberos, należy użyć komendy **mkseckrb5**. Komenda **mkseckrb5** przekształca użytkowników nieadministracyjnych (użytkownicy o identyfikatorach większych niż 201) w użytkowników uwierzytelnianych za pomocą protokołu Kerberos. Po wywołaniu komendy **mkseckrb5** użytkownik jest proszony o podanie nazwy i hasła użytkownika administracyjnego usługi uwierzytelniania sieciowego. Jeśli nie jest używana opcja randomize, użytkownik jest także proszony o podanie hasła każdego przekształcanego użytkownika.

  Uwaga: Komenda **mkseckrb5** przekształca tylko użytkowników lokalnych. Użytkowników w domenach zdalnych, takich jak LDAP, nie można przekształcać za pomocą tej komendy.

  W poniższym przykładzie *nie jest używana* opcja randomize podczas konwersji użytkownika AIX w użytkownika uwierzytelnianego za pomocą protokołu Kerberos.

  1. Wprowadź następującą komendę:

```
mkseckrb5 foo
```

  2. Przed zalogowaniem użytkownika za pomocą protokołu Kerberos ustaw atrybuty SYSTEM i registry użytkownika w następujący sposób:

```
chuser -R KRB5files SYSTEM=KRB5files registry=KRB5files foo
```

W poniższym przykładzie podczas konwersji użytkownika AIX w użytkownika uwierzytelnianego za pomocą protokołu Kerberos używana jest opcja randomize.

1. Wprowadź następującą komendę:

```
mkseckrb5 -r user1
```

2. Po zakończeniu konwersji ustaw atrybuty SYSTEM i registry użytkownika oraz hasło w następujący sposób:

```
chuser -R KRB5files SYSTEM=KRB5files registry=KRB5files user1
```

```
passwd -R KRB5files user1
```

- ***Jak zmienić hasło użytkownika Kerberos?***

  Hasło użytkownika Kerberos może zmienić użytkownik root, wprowadzając następującą komendę **passwd**:

```
passwd -R KRB5files foo
```

  Po wprowadzeniu komendy **passwd** wyświetlane są następujące komunikaty:

```
Zmieniam hasło dla "foo"
Stare hasło foo:
Nowe hasło foo:
Wprowadź nowe hasło jeszcze raz:
```

  Gdy komenda **passwd** zostanie wprowadzona przez użytkownika root, stare hasło będzie zignorowane. Zachętę do podania starego hasła można wyłączyć, używając opcji rootpwdrequired w pliku `methods.cfg`. Aby wyłączyć zachętę do podania starego hasła, zmodyfikuj plik `/usr/lib/security/methods.cfg` w następujący sposób:

```
KRB5files:
   options = db=BUILTIN,auth=KRB5,rootrequiresopw=false
```

- ***Jak uzyskać bilet nadania biletu po pomyślnym zalogowaniu, gdy atrybut needchange jest ustawiony?***

  Aby uzyskać bilet nadania biletu po pomyślnym zalogowaniu, gdy opcja needchange jest ustawiona, wywołaj komendę **kinit**. Więcej informacji na ten temat zawiera opis atrybutu needhange.

- ***Dlaczego moje hasło nie jest akceptowane przez system operacyjny AIX?***

  Jeśli podawane hasło nie jest akceptowane, wykonaj następujące czynności:

  – Sprawdź, czy serwery KDC i kadmind są uruchomione.
  – Sprawdź, czy hasło spełnia wymagania systemu operacyjnego AIX oraz usługi uwierzytelniania sieciowego.

- ***Jak zmienić reguły dotyczące haseł?***

  Reguły dotyczące haseł w systemie AIX można zmienić, modyfikując atrybuty strategii haseł. Do zmiany strategii haseł w bazie danych Kerberos można użyć narzędzia kadmin serwera uwierzytelniania sieciowego.

- ***Czy użytkownik uwierzytelniany przy użyciu protokołu Kerberos może być uwierzytelniany przy użyciu tylko standardowego uwierzytelniania systemu AIX?***

  Użytkownik uwierzytelniany przy użyciu protokołu Kerberos (foo) może być uwierzytelniany za pomocą uwierzytelniania **crypt()** AIX w następujący sposób:

  1. Ustaw hasło w systemie AIX dla użytkownika foo (`/etc/security/passwd`) za pomocą komendy **passwd**.

2. Wybierz inne hasło do celów testowych. Na przykład:

```
passwd -R files foo
```

3. Zmień atrybut SYSTEM użytkownika w następujący sposób:

```
chuser -R KRB5files SYSTEM=compat foo
```

Zmiana atrybutu SYSTEM powoduje zmianę metody uwierzytelniania z Kerberos na **crypt()**.

Uwaga: Ponieważ użytkownik w tym przykładzie zalogował się za pomocą uwierzytelniania lokalnego, AUTHSTATE ma wartość compat i nie jest wystawiany żaden bilet nadania biletu. Jeśli chcesz użyć uwierzytelniania **crypt()** jako mechanizmu zapasowego, przejdź do kroku “4” na stronie 313.

4. Aby użyć uwierzytelniania **crypt()** jako mechanizmu zapasowego, zmień atrybut SYSTEM w następujący sposób:

```
chuser -R KRB5files SYSTEM="KRB5files or compat" foo
```

- ***Jak zmienić port kadmind klienta?***

  Demon **kadmind** jest używany do zarządzania nazwami użytkowników Kerberos w systemach z uwierzytelnianiem przy pomocy protokołu Kerberos korzystających z serwera NAS. W poniższym przykładzie przedstawiono sposób zmiany portu **kadmind** klienta. W tym przykładzie demon **kadmind** działa na serwerze `kdcsrv.austin.ibm.com` i używa portu 812.

  1. Użyj komendy **config.krb5**, aby skonfigurować klienta:

```
config.krb5 –C –r MYREALM –c kdcsrv.austin.ibm.com –s \
kdcsrv.austin.ibm.com –d austin.ibm.com
```

  2. Zmodyfikuj plik krb5.conf, zmieniając numer portu:

```
admin_server = kdcsrv.austin.ibm.com:812
```

- ***Jak usunąć referencje Kerberos?***

  Podczas każdego logowania użytkownika poprzednie referencje Kerberos są nadpisywane. Jednak gdy użytkownik wyloguje się, nie są one usuwane. Aby usunąć te referencje, wprowadź następującą komendę NAS **kdestroy**:

```
/usr/krb5/bin/kdestroy
```

- ***Jak zmienić czas życia biletu w centrum KDC?***

  Aby zmienić czas życia biletu w centrum KDC, wykonaj następujące czynności:

  1. Zmień atrybut max_life w pliku `kdc.conf`. Na przykład:

```
max_life = 8h 0m 0s
```

  2. Zatrzymaj, a następnie uruchom demony **krb5kdc** i **kadmind**.
  3. Zmień wartość max_life nazw użytkowników krbtgt/MYREALM i kadmin/admin na wartość wprowadzoną w kroku “1” na stronie 313. Na przykład:

```
kadmin.local
kadmin.local: modify_principal -maxlife "8 hours" krbtgt/MYREALM
```

- ***Co dzieje się, gdy demon kadmind jest niedostępny?***

  Jeśli demon kadmind jest niedostępny, uwierzytelnianie może potrwać dłużej lub może się nie powieść. Uwierzytelnianie może się nie powieść, jeśli część sieci, w której znajduje się demon kadmind, jest

niedostępna lub gdy system obsługujący serwer kadmind jest wyłączony. Gdy system jest niedostępny, ustawienie opcji kadmind w pliku `methods.cfg` na wartość no eliminuje opóźnienia podczas uwierzytelniania.

Gdy demon kadmind jest wyłączony, użytkownicy nie mogą logować się, gdy ich hasła utracą ważność. Jeśli demon kadmind nie będzie dostępny (będzie wyłączony lub nieosiągalny) i użytkownik wprowadzi komendę **mkuser**, zostanie wyświetlony następujący błąd:

```
3004-694 Błąd podczas dodawania "krb5user": Brak uprawnień.
```

Ponadto komendy **chuser** i **lsuser** umożliwiają tylko zarządzanie atrybutami dotyczącymi systemu AIX, a nie atrybutami dotyczącymi protokołu Kerberos. Komenda **rmuser** nie usunie użytkownika Kerberos, a komenda **passwd** nie będzie działała w przypadku użytkowników uwierzytelnianych za pomocą protokołu Kerberos.

Gdy demon kadmind będzie niedostępny, użytkownik root nie będzie mógł zmieniać haseł użytkowników. W przypadku, gdy użytkownik zapomni hasła, demon kadmind musi być dostępny. Ponadto, jeśli użytkownik wprowadzi w wierszu logowania nazwę użytkownika Kerberos, nazwa podstawowa nazwy użytkownika zostanie obcięta (zgodnie z ograniczeniem długości nazwy dla użytkownika systemu AIX). Ta obcięta nazwa będzie używana do odtwarzania informacji identyfikacyjnych użytkownika systemu AIX (na przykład, aby odtworzyć wartość katalogu osobistego).

- ***Jak skonfigurować system operacyjny AIX pod kątem zintegrowanego logowania Kerberos z zarządzaniem użytkownikami/grupami AIX przy użyciu LDAP?***

  Jeśli do przechowywania informacji o użytkownikach/grupach AIX planowane jest użycie LDAP, należy użyć komendy **mksecldap**, aby skonfigurować serwer i klienta LDAP przed uruchomieniem komend **mkkrb5srv** i **mkkrb5clnt**. Aby skonfigurować serwery Kerberos, należy użyć komendy **mkkrb5srv**. Aby skonfigurować klienta Kerberos, należy użyć komendy **mkkrb5clnt** z opcją –i LDAP. Na przykład:

  ```
  mkkrb5clnt -r MYREALM -c kdcsrv.austin.ibm.com\
   –s kdcsrv.austin.ibm.com -a admin/admin -d austin.ibm.com -A -i LDAP -K –T
  ```

- ***Jak używać komend zdalnych z obsługą Kerberos po pomyślnym zalogowaniu się?***

  Gdy użytkownik AIX uwierzytelni się w systemie za pomocą protokołu Kerberos, dla komend zdalnych z obsługą Kerberos można użyć biletu nadania biletu.

  W poniższym przykładzie serwer NAS został skonfigurowany na serwerze kdcsrv.austin.ibm.com za pomocą komendy **mkkrb5srv**. Ten system został skonfigurowany również dla logowań z wykorzystaniem protokołu Kerberos za pomocą komendy **mkkrb5clnt**. Drugi system, tx3d.austin.ibm.com, został skonfigurowany jako klient za pomocą komendy **mkkrb5clnt**.

  1. Zapisz klucze dla nazwy użytkownika hosta host/tx3d.austin.ibm.com w pliku `/etc/krb5/krb5.keytab` w systemie tx3d.
  2. Ponieważ do skonfigurowania komputera klienta użyto komendy **mkkrb5clnt**, te klucze zostały wyodrębnione do pliku `/var/krb5/security/keytab/tx3d.austin.ibm.com.keytab`. Dowiąż ten plik do pliku `/etc/krb5/krb5.keytab` w następujący sposób:

     ```
     ln -s /var/krb5/security/keytab/tx3d.austin.ibm.com.keytab /etc/krb5/krb5.keytab
     ```

  3. Jeśli system tx3d.austin.ibm.com został skonfigurowany z serwerem Kerberos innym niż AIX, jawnie utwórz nazwę użytkownika hosta i wyodrębnij klucze. Na przykład:

     ```
     kadmin -p admin/admin

     kadmin: addprinc -randkey host/tx3d.austin.ibm.com
     kadmin: ktadd -k /etc/krb5/krb5.keytab host/tx3d.austin.ibm.com
     kadmin:
     ```

     Ponieważ narzędzie kadmin jest wywoływane z systemu tx3d.austin.ibm.com system, klucze są wyodrębniane do pliku `/etc/krb5/krb5.keytab` w systemie tx3d.austin.ibm.com. Ten krok można także wykonać na komputerze, który obsługuje serwer administracyjny Kerberos (na przykład

kdcsrv). Po wyodrębnieniu kluczy do pliku tabeli kluczy plik ten jest przesyłany i scalany z plikiem `/etc/krb5/krb5.keytab` w systemie tx3d.

4. Aktywuj komendy zdalne pod kątem uwierzytelniania za pomocą protokołu Kerberos, wersja 5, w systemie tx3d.austin.ibm.com:

```
lsauthent
Standard Aix
chauthent -k5 -std
lsauthent
Kerberos 5
Standard Aix
```

5. Aktywuj komendy zdalne pod kątem uwierzytelniania za pomocą protokołu Kerberos wersja 5 w systemie kdcsrv.austin.ibm.com:

```
chauthent -k5 -std
lsauthent
Kerberos 5
Standard Aix
```

6. Utwórz użytkownika uwierzytelnianego za pomocą protokołu Kerberos (foo) na serwerze kdcsrv i ustaw hasło.

```
mkuser -R KRB5files SYSTEM=KRB5files registry=KRB5files foo
passwd -R KRB5files foo
```

7. Utwórz użytkownika foo na serwerze tx3d:

```
mkuser -R files foo
```

8. Połącz się z systemem kdcsrv.austin.ibm.com za pomocą telnetu, używając uwierzytelniania Kerberos.
9. Aby upewnić się, że wystawiono bilet nadania biletu, wprowadź komendę **klist**.

```
/usr/krb5/bin/klist
```

Poniżej podano przykłady komend zdalnych z obsługą Kerberos.

Uwaga: Przed uruchomieniem komend w podanych przykładach usuń pliki `.klogin`, `.rhost` i `hosts.equiv`.

– Wprowadź komendę **date** na zdalnym hoście tx3d.austin.ibm.com wraz z komendą **rsh**:

```
rsh tx3d date
```

– Zaloguj się w zdalnym systemie tx3d.austin.ibm.com za pomocą komendy **rlogin**:

```
hostname
kdcsrv.austin.ibm.com
rlogin tx3d -l foo
*******************************
* Witamy w AIX wersja 6.1! *
*******************************
hostname
tx3d.austin.ibm.com
id
uid=234(foo) gid=1(staff)
```

– Prześlij plik do zdalnego systemu tx3d.austin.ibm.com za pomocą komendy **rcp**:

```
rsh tx3d "ls -l /home/foo"
total 0
echo "Testowanie komend zdalnych z obsługą Kerberos" >> xfile
rcp xfile tx3d:/home/foo
rsh tx3d "ls -l /home/foo"
total 0
-rw-r--r-- 1 foo staff 0 Apr 28 14:30 xfile
rsh tx3d "more /home/foo/xfile"
Testowanie komend zdalnych z obsługą Kerberos
```

– Połącz się z systemem zdalnym tx3d.austin.ibm.com za pomocą telnetu, używając referencji Kerberos:

```
telnet tx3d
Próbuję...
Połączono z tx3d.austin.ibm.com.
Znak kontrolny = '^]'.
[ Kerberos V5 akceptuje Cię jako "foo@MYREALM" ]
```

– Połącz się z systemem tx3d.austin.ibm.com za pomocą telnetu, a następnie wprowadź nazwę hosta i identyfikator po wyświetleniu zachęty:

```
hostname
tx3d.austin.ibm.com
id
uid=234(foo) gid=1(staff)
```

– Przed użyciem komendy **ftp** z obsługą Kerberos należy użyć komendy **kadmin** (z systemu tx3d.austin.ibm.com), aby utworzyć nazwę użytkownika usługi FTP `ftp/tx3d.austin.ibm.com` i wyodrębnić ją do pliku `/etc/krb5/krb5.keytab`:

```
kadmin: addprinc -randkey ftp/tx3d.austin.ibm.com@MYREALM
kadmin: ktadd -k /etc/krb5/krb5.keytab ftp/tx3d.austin.ibm.com@MYREALM
kadmin:
```

Poniżej został przedstawiony przykład użycia FTP dla systemu zdalnego tx3d.austin.ibm.com z użyciem referencji Kerberos.

```
ftp tx3d
Nazwa (tx3d:foo): foo
232 Użytkownik GSSAPI foo@MYREALM został autoryzowany jako foo
230-Ostatnie logowanie: Czw 19 maja 2005 17:58:57 CDT na ftp z kdcsrv.austin.ibm.com
230 Użytkownik foo jest zalogowany.
ftp> ftp> ls -la
```

Konfigurowanie klienta Kerberos dla serwera Kerberos w systemie innym niż AIX
Klienta Kerberos w systemie AIX można skonfigurować dla serwera Kerberos w następujących systemach innych niż AIX: Windows Active Directory, Solaris i HP.

Konfigurowanie protokołu Kerberos pod kątem usługi Kerberos w systemie Windows Server
Istnieje kilka metod konfigurowania protokołu Kerberos dla usługi Kerberos w systemie Windows Server.

W części uwierzytelniającej modułu złożonego ładowania można użyć modułu Kerberos odpowiedzialnego tylko za uwierzytelnianie w KRB5. Podczas konfigurowania użytkownik określa środowisko Kerberos dla modułu ładowania. Moduł ładowania KRB5 aktywuje Kerberos jako alternatywną metodę uwierzytelniania w usłudze Kerberos w systemie Windows 2000 lub Windows 2003 Server. Moduł pseudoładowania AIX BUILTIN zapewnia dostęp do funkcji bibliotecznych bezpieczeństwa. Moduł ładowania BUILTIN można połączyć z modułami ładowania odpowiedzialnymi tylko za uwierzytelnianie, aby zapewnić część bazodanową modułu złożonego ładowania. Ponadto udostępnia on przechowywanie wcześniejszych użytkowników i grup oraz dostęp do systemu plików. Modułu ładowania LDAP można także użyć jako bazodanowej części modułu złożonego ładowania.

Inaczej niż w przypadku innych środowisk Kerberos z serwerem NAS w systemie AIX, to środowisko nie udostępnia funkcji zarządzania nazwami użytkowników Kerberos. W środowisku, w którym nazwy użytkowników Kerberos są zapisane w systemie innym niż AIX i nie można nimi zarządzać z systemu AIX za pomocą interfejsu bazy danych Kerberos **kadmin**, można użyć modułu ładowalnego KRB5. Zarządzanie nazwami użytkowników Kerberos odbywa się oddzielnie przy użyciu narzędzi do zarządzania nazwami użytkowników Kerberos. Narzędzia te mogą być częścią produktu Kerberos opracowanego przez dostawców oprogramowania lub mogą być zintegrowane z systemem operacyjnym, tak jak w przypadku systemu Windows 2000.

Konfigurowanie usługi Kerberos w systemie Windows Server 2000
Usługa Kerberos w systemie Windows Server 2000 i klient usługi NAS współdziałają na poziomie protokołu Kerberos (RFC1510). Ponieważ Windows Server 2000 nie obsługuje interfejsu **kadmin**, należy podać opcję –D w komendzie **mkkrb5clnt** podczas konfigurowania klientów AIX. Do zarządzania nazwami użytkowników w systemie Windows należy użyć narzędzi systemu Windows.

Użyj poniższej procedury, aby skonfigurować klienta AIX dla uwierzytelniania wykorzystującego protokół Kerberos w usłudze Kerberos systemu Windows Server 2000.

1. Skonfiguruj Windows Server 2000. Informacje na temat konfigurowania Microsoft Active Directory Server zawiera dokumentacja firmy Microsoft.
2. Jeśli klient usługi NAS nie jest zainstalowany na kliencie AIX, zainstaluj zestaw plików `krb5.client.rte` znajdujący się na nośniku AIX Expansion Pack.
3. Użyj komendy **mkkrb5clnt** z następującymi informacjami konfiguracyjnymi, aby skonfigurować klienta Kerberos w systemie AIX:

   realm
   Nazwa domeny Windows Active Directory.

   domain
   Nazwa domeny komputera udostępniającego serwer Active Directory.

   KDC
   Nazwa hosta serwera Windows.

   server
   Nazwa hosta serwera Windows.

   Poniżej przedstawiono przykład komendy **mkkrb5clnt**:

   ```
   mkkrb5clnt -r MYREALM -d austin.ibm.com -c w2k.austin.ibm.com -s w2k.austin.ibm.com -D
   ```

   Opcja **-D** w komendzie **mkkrb5clnt** powoduje utworzenie opcji **is_kadmind_compat=no** w pliku `/etc/methods.cfg` i skonfigurowanie środowiska klienta Kerberos do uwierzytelniania w systemach innych niż AIX. Nie należy używać opcji **-D** w komendzie **mkkrb5clnt** do skonfigurowania środowiska klienta Kerberos do uwierzytelniania w usłudze uwierzytelniania sieciowego IBM (NAS).

   Uwaga: Po uruchomieniu komendy **mkkrb5clnt** do pliku `methods.cfg` dodawana jest następująca sekcja.

   ```
   KRB5:
           program = /usr/lib/security/KRB5
           program_64 = /usr/lib/security/KRB5_64
           options = authonly,is_kadmind_compat=no

   KRB5files:
           options = db=BUILTIN,auth=KRB5
   ```

   Więcej informacji na temat:

   - komendy **mkkrb5clnt** i dostępnych opcji zawiera opis komendy **mkkrb5clnt**,
   - pliku `methods.cfg` zawiera opis pliku `methods.cfg`.
4. Ponieważ system Windows obsługuje typy szyfrowania DES-CBC-MD5 i DES-CBC-CRC, zmień informacje w pliku `krb5.conf` na następujące:

   ```
   [libdefaults]
       default_realm = MYREALM
       default_keytab_name = FILE:/etc/krb5/krb5.keytab
       default_tkt_enctypes = des-cbc-md5 des-cbc-crc
       default_tgs_enctypes = des-cbc-md5 des-cbc-crc
   ```

5. Utwórz nazwę użytkownika hosta.

   Ponieważ nazwy kont w systemie Windows nie zawierają wielu części, tak jak nazwy użytkowników usługi NAS, nie można bezpośrednio utworzyć konta za pomocą pełnej nazwy hosta (`host/`

<*pełna_nazwa_hosta*>). Instancja nazwy użytkownika jest natomiast tworzona za pomocą odwzorowania usługa-nazwa_użytkownika-nazwa. W tym przypadku tworzone jest konto odpowiadające nazwie użytkownika hosta i dodawane jest odwzorowanie nazwa_użytkownika-nazwa.

Na serwerze Active Directory użyj narzędzia Active Directory Management, aby utworzyć nowe konto użytkownika odpowiadające klientowi `tx3d.austin.ibm.com` w systemie AIX:

a. Wybierz folder `Użytkownik`.
b. Kliknij prawym przyciskiem myszy, aby wybrać opcję `Nowy`.
c. Wybierz opcję `Użytkownik`.
d. Wpisz `tx3d` w polu `Imię`, a następnie kliknij przycisk `Dalej`.
e. Utwórz hasło, a następnie kliknij przycisk `Dalej`.
f. Kliknij przycisk `Zakończ`, aby utworzyć nazwę użytkownika hosta.

6. Na komputerze z systemem Windows Server 2000 wpisz komendę **Ktpass** w wierszu komend, aby utworzyć plik `tx3d.keytab`, i skonfiguruj konto hosta AIX w następujący sposób:

```
Ktpass -princ host/tx3d.austin.ibm.com@MYREALM -mapuser tx3d -pass password -out tx3d.keytab
```

7. Skopiuj plik `tx3d.keytab` na host AIX.
8. Scal plik `tx3d.keytab` z plikiem `/etc/krb5/krb5.keytab` w systemie AIX w następujący sposób:

```
ktutil
rkt tx3d.keytab
wkt /etc/krb5/krb5.keytab
q
```

9. Utwórz konta domeny Windows, używając narzędzi do zarządzania użytkownikami Active Directory.
10. Aby utworzyć konta AIX odpowiadające kontom w domenie Windows i użyć uwierzytelniania Kerberos, uruchom następującą komendę:

```
mkuser registry=KRB5files SYSTEM=KRB5files foo
```

11. Aby zalogować się w systemie AIX i sprawdzić konfigurację, uruchom komendę **telnet**.

    Poniżej podano przykład zintegrowanej sesji logowania Kerberos korzystającej z KRB5 w Windows Active Directory:

```
telnet tx3d

Próbuję...
Połączono z tx3d.austin.ibm.com.
Znak kontrolny = '^]'.

telnet (tx3d.austin.ibm.com)
login: foo
Hasło foo:
*******************************************************************************
* Witamy w AIX wersja 6.1! *
*******************************************************************************
echo $AUTHSTATE
KRB5files

/usr/krb5/bin/klist
Pamięć podręczna biletu: FILE:/var/krb5/security/creds/krb5cc_foo@AUSTIN.IBM.COM_203
Domyślny podmiot kerberos: foo@AUSTIN.IBM.COM

Poprawne uruchomienie Utrata ważności usługi nazwy użytkownika
04/29/05 14:37:28 04/30/05 00:39:22 krbtgt/AUSTIN.IBM.COM@AUSTIN.IBM.COM
     Odnowione do czasu 04/30/05 14:37:28

04/29/05 14:39:22 04/30/05 00:39:22 host/tx3d.austin.ibm.com@AUSTIN.IBM.COM
```

Konfigurowanie usługi Kerberos w systemie Windows Server 2003
Klienta Kerberos można skonfigurować dla usługi Kerberos w systemie Windows Server 2003.

Aby skonfigurować klienta AIX dla usługi Kerberos w systemie Windows Server 2003, należy wykonać kroki podane w sekcji “Konfigurowanie usługi Kerberos w systemie Windows Server 2000” na stronie 317.

Uwaga: Program narzędziowy klienta **kpasswd** serwera NAS nie może zmienić hasła nazwy użytkownika Kerberos w usłudze Kerberos w systemie Windows Server 2003. Dlatego po pomyślnym zalogowaniu się na komputerze z systemem AIX korzystającym z protokołu Kerberos użytkownik nie może zmienić hasła w systemie Windows Server 2003.

Konfigurowanie protokołu Kerberos pod kątem kontrolerów domen Kerberos Sun Solaris i HP-UX
Klienta Kerberos można skonfigurować dla kontrolerów domen Kerberos w systemach Sun Solaris i HP-UX.

Inaczej niż w przypadku środowisk Kerberos z serwerem NAS w systemie AIX, to środowisko nie udostępnia funkcji zarządzania nazwami użytkowników Kerberos. W środowisku, w którym nazwy użytkowników Kerberos są zapisane w systemie innym niż AIX i nie można nimi zarządzać z operacyjnego AIX za pomocą interfejsu bazy danych Kerberos **kadmin**, można użyć modułu ładowalnego KRB5. Zarządzanie nazwami użytkowników Kerberos odbywa się oddzielnie przy użyciu narzędzi do zarządzania nazwami użytkowników Kerberos. Narzędzia te mogą być częścią produktu Kerberos opracowanego przez dostawców oprogramowania lub mogą być zintegrowane z systemem operacyjnym.

Konfigurowanie systemu Sun Solaris
Klienta Kerberos można skonfigurować dla systemu Sun Solaris.

Mechanizm Sun Enterprise Authentication Mechanism (SEAM) i klient NAS w systemie AIX współdziałają na poziomie protokołu Kerberos (RFC1510). Ponieważ interfejs demona **kadmind** w systemie Solaris nie jest kompatybilny z interfejsem **kadmin** klienta NAS w systemie AIX, należy podać opcję –D w komendzie **mkkrb5clnt** podczas konfigurowania klientów AIX. Aby zarządzać nazwami użytkowników w systemie Solaris, należy użyć narzędzi systemu Solaris. Ponieważ protokół zmiany haseł jest inny na serwerach Kerberos SEAM i na klientach NAS AIX, zmiana hasła dla nazwy użytkownika powoduje niepowodzenie konfiguracji.

W poniższym przykładzie użyto systemu Solaris.

Użyj poniższej procedury, aby skonfigurować klienta AIX dla uwierzytelniania wykorzystującego protokół Kerberos w mechanizmie SEAM.

1. Skonfiguruj mechanizm SEAM, korzystając z dokumentacji firmy Sun.
2. Jeśli klient usługi NAS nie jest zainstalowany na kliencie AIX, zainstaluj zestaw plików `krb5.client.rte` znajdujący się na nośniku AIX Expansion Pack.
3. Aby skonfigurować klienta Kerberos w systemie AIX, użyj komendy **mkkrb5clnt** z następującymi informacjami konfiguracyjnymi:

   realm
   Nazwa dziedziny Kerberos Solaris: AUSTIN.IBM.COM

   domain
   Nazwa domeny komputera udostępniającego serwery: Austin.ibm.com

   KDC
   Nazwa hosta Solaris obsługującego centrum KDC: sunsys.austin.ibm.com

   server
   Nazwa hosta Solaris obsługującego demon **kadmin** (zwykle jest taka sama jak nazwa centrum KDC): sunsys.austin.ibm.com

   Uwaga: Ponieważ interfejsy **kadmin** klienta NAS w systemie AIX i Solaris są inne, nazwa serwera nie jest używana przez klientów NAS i z komendą **mkkrb5clnt** należy użyć opcji -D.

   Poniżej przedstawiono przykład komendy **mkkrb5clnt**:

```
mkkrb5clnt -r AUSTIN.IBM.COM -d austin.ibm.com\
 -c sunsys.austin.ibm.com -s sunsys.austin.ibm.com -D
```

Opcja **-D** w komendzie **mkkrb5clnt** powoduje utworzenie opcji **is_kadmind_compat=no** w pliku `/etc/security/methods.cfg` i skonfigurowanie środowiska klienta Kerberos do uwierzytelniania w systemach innych niż AIX. Nie należy używać opcji **-D** w komendzie **mkkrb5clnt** do skonfigurowania środowiska klienta Kerberos do uwierzytelniania w usłudze uwierzytelniania sieciowego IBM (NAS).

Uwaga: Po uruchomieniu komendy **mkkrb5clnt** do pliku `methods.cfg` dodawana jest następująca sekcja.

```
KRB5:
        program = /usr/lib/security/KRB5
        program_64 = /usr/lib/security/KRB5_64
        options = authonly,is_kadmind_compat=no

KRB5files:
        options = db=BUILTIN,auth=KRB5
```

Więcej informacji na temat:

- komendy **mkkrb5clnt** i dostępnych opcji zawiera opis komendy **mkkrb5clnt**,
- pliku `methods.cfg` zawiera opis pliku `methods.cfg`.

4. Użyj narzędzia **kadmin** systemu Solaris, aby utworzyć nazwę użytkownika hosta `host/tx3d.austin.ibm.com@MYREALM` i zapisać ją w pliku:

```
kadmin: add_principal -randkey host/tx3d.austin.ibm.com
Podmiot kerberos "host/tx3d.austin.ibm.com@AUSTIN.IBM.COM" został utworzony.

kadmin:ktadd -k /tmp/tx3d.keytab host/tx3d.austin.ibm.com
Pozycja podmiotu kerberos host/tx3d.austin.ibm.com o kvno 3,
    typie szyfrowania DES-CBC-CRC została dodana do tablicy kluczy WRFILE:/tmp/tx3d.keytab.

kadmin: quit
```

5. Skopiuj plik `tx3d.keytab` na host AIX.
6. Scal plik `tx3d.keytab` z plikiem `/etc/krb5/krb5.keytab` w systemie AIX w następujący sposób:

```
ktutil
rkt tx3d.keytab
l
slot   KVNO   Principal
wkt /etc/krb5/krb5.keytab
q
```

7. Aby utworzyć nazwę użytkownika Kerberos, użyj narzędzia **kadmin** systemu Solaris.

```
add_principal sunuser
```

8. Aby utworzyć konta AIX odpowiadające nazwie użytkownika Kerberos w systemie Solaris i użyć uwierzytelniania Kerberos, wprowadź następującą komendę:

```
mkuser registry=KRB5files SYSTEM=KRB5files sunuser
```

9. Użyj komendy **telnet**, aby zalogować się w systemie AIX, używając nazwy i hasła użytkownika sunuser, a następnie sprawdź konfigurację.

   Poniżej podano przykład zintegrowanej sesji logowania Kerberos korzystającej z KRB5 w centrum KDC systemu Solaris KDC.

```
telnet tx3d

echo $AUTHSTATE
KRB5files

echo $KRB5CCNAME
FILE:/var/krb5/security/creds/krb5cc_sunuser@AUSTIN.IBM.COM_207

Wyświetl referencje:
/usr/krb5/bin/klist
```

Konfigurowanie systemu HP-UX
Klienta Kerberos można skonfigurować dla systemu HP-UX.

Kroki, które należy wykonać, aby uwierzytelniać użytkowników w systemie HP-UX 11i, są podobne do kroków opisanych w sekcji “Konfigurowanie systemu Sun Solaris” na stronie 319. Centrum KDC systemu HP-UX i klient NAS w systemie AIX współdziałają na poziomie protokołu Kerberos (RFC1510). Protokół zmiany hasła jest także kompatybilny. Ponieważ interfejs demona **kadmind** w systemie HP-UX nie jest kompatybilny z interfejsem **kadmin** klienta NAS w systemie AIX, należy podać opcję –D w komendzie **mkkrb5clnt** podczas konfigurowania klientów AIX.

Użyj poniższej procedury, aby skonfigurować klienta AIX dla uwierzytelniania wykorzystującego protokół Kerberos w systemie HP-UX 11i z protokołem Kerberos w wersji 2.1.

1. Skonfiguruj protokół Kerberos w wersji 2.1 w systemie HP-UX 11i, korzystając z dokumentacji HP.
2. Jeśli klient usługi NAS nie jest zainstalowany na kliencie AIX, zainstaluj zestaw plików `krb5.client.rte` znajdujący się na nośniku AIX Expansion Pack.
3. Użyj komendy **mkkrb5clnt** z następującymi informacjami konfiguracyjnymi, aby skonfigurować klienta Kerberos w systemie AIX:

   realm
   Nazwa dziedziny Kerberos HP: HPSYS.AUSTIN.IBM.COM

   domain
   Nazwa domeny komputera udostępniającego serwery Kerberos HP-UX: austin.ibm.com

   KDC
   Nazwa hosta HP-UX obsługującego centrum KDC: hpsys.austin.ibm.com

   server
   Nazwa hosta serwera HP-UX: hpsys.austin.ibm.com

   Uwaga: Ponieważ interfejsy **kadmin** klienta NAS w systemie AIX i HP-UX są inne, nazwa serwera nie jest używana przez klienty NAS i z komendą **mkkrb5clnt** należy użyć opcji -D.

   Poniżej przedstawiono przykład komendy **mkkrb5clnt**:

   ```
   mkkrb5clnt -r AUSTIN.IBM.COM -d austin.ibm.com\
    -c hpsys.austin.ibm.com -s hpsys.austin.ibm.com -D
   ```

   Opcja **-D** w komendzie **mkkrb5clnt** powoduje utworzenie opcji **is_kadmind_compat=no** w pliku `/etc/security/methods.cfg` i skonfigurowanie środowiska klienta Kerberos do uwierzytelniania w systemach innych niż AIX. Nie należy używać opcji **-D** w komendzie **mkkrb5clnt** do skonfigurowania środowiska klienta Kerberos do uwierzytelniania w usłudze uwierzytelniania sieciowego IBM (NAS).

   Uwaga: Po uruchomieniu komendy **mkkrb5clnt** do pliku `methods.cfg` dodawana jest następująca sekcja.

   ```
   KRB5:
           program = /usr/lib/security/KRB5
           program_64 = /usr/lib/security/KRB5_64
           options = authonly,is_kadmind_compat=no

   KRB5files:
           options = db=BUILTIN,auth=KRB5
   ```

   Więcej informacji na temat:

   - komendy **mkkrb5clnt** i dostępnych opcji zawiera opis komendy **mkkrb5clnt**,
   - pliku `methods.cfg` zawiera opis pliku `methods.cfg`.
4. Zmodyfikuj plik `krb5.conf`, aby typ szyfrowania był zgodny z wartością użytą podczas konfigurowania Kerberos w systemie HP-UX (**krbsetup**). Jeśli używana jest wartość DES-CRC, zmodyfikuj sekcję [libdefaults] w pliku `krb5.conf` w systemie AIX klienta w następujący sposób:

   ```
   default_tkt_enctypes = des-cbc-crc
   ```

```
default_tgs_enctypes = des-cbc-crc
```

5. Użyj narzędzia **kadmin_ui** systemu HP-UX, aby utworzyć nazwę użytkownika hosta `host/tx3d.austin.ibm.com`.
6. Wyodrębnij klucz i zapisz go w pliku. Z menu `Edycja` okna `Informacje o podmiocie Kerberos` wybierz opcję `Wyodrębnij klucz serwisowy`, aby wyodrębnić klucze.
7. Skopiuj plik `tx3d.keytab` na host AIX.
8. Scal plik `tx3d.keytab` z plikiem `/etc/krb5/krb5.keytab` w systemie AIX w następujący sposób:

```
ktutil
rkt tx3d.keytab
l
slot   KVNO   Principal
wkt /etc/krb5/krb5.keytab
q
```

9. Użyj narzędzia **kadmin_ui** systemu HP-UX, aby utworzyć nazwę użytkownika Kerberos hpuser, a następnie kliknij kartę `Edycja/Atrybut`, aby wyczyścić opcję pw_require.
10. Utwórz konto AIX odpowiadające nazwie użytkownika Kerberos w systemie HP-UX w następujący sposób:

```
mkuser registry=KRB5files SYSTEM=KRB5files hpuser
```

11. Użyj komendy **telnet**, aby zalogować się w systemie AIX, używając nazwy i hasła użytkownika hpuser, a następnie sprawdź konfigurację.

    Poniżej podano przykład zintegrowanej sesji logowania Kerberos korzystającej z KRB5 w HP-UX:

```
telnet tx3d

echo $AUTHSTATE
KRB5files

Wyświetl referencje:
/usr/krb5/bin/klist
```

12. Użyj komendy **passwd**, aby zmienić hasło.

    Uwaga: Podczas zmiany hasła wymuszana jest strategia haseł systemu HP-UX. Informacje na temat konfigurowania strategii haseł zawiera dokumentacja HP-UX.

Protokół Kerberos w systemach innych niż AIX: pytania i informacje dotyczące rozwiązywania problemów
W tym miejscu podano odpowiedzi na pytania dotyczące klientów Kerberos korzystających z serwera Kerberos w systemach innych niż AIX.

Uwaga: W poniższych przykładach użyto serwera Microsoft Active Directory Server. Przykłady te mają jednak zastosowanie także do systemów Solaris i HP.

Przystępując do rozwiązywania problemów, najpierw należy upewnić się, że wszystkie serwery i demony są uruchomione.

Protokół Kerberos używany w systemach innych niż AIX używa podsystemu syslog, aby zapisać informacje o błędach i informacje debugowania. Aby dowiedzieć się więcej o rejestrowaniu informacji w dzienniku syslog, zapoznaj się z informacjami dotyczącymi demona **syslogd**.

- ***Jak utworzyć użytkownika systemu AIX?***

  Utwórz konto użytkownika AIX (foo), uruchamiając następującą komendę:

```
mkuser registry=KRB5files SYSTEM=KRB5files foo
```

  Komenda **mkuser** tworzy użytkownika w systemie AIX. Musisz także utworzyć konto dla tego użytkownika w Windows Server Active Directory, które będzie odpowiednikiem tego konta w systemie

AIX. Utworzenie konta użytkownika w Windows Server Active Directory powoduje niejawne utworzenie nazw użytkowników.

- ***Jak usunąć użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby usunąć użytkownika uwierzytelnionego przy użyciu protokołu Kerberos, uruchom następującą komendę:

  ```
  rmuser –R KRB5files foo
  ```

  Komenda **rmuser** usuwa użytkownika z systemu AIX. Tego użytkownika należy także usunąć z Windows Server Active Directory, używając do tego celu narzędzi do zarządzania użytkownikami dostępnych w systemie Windows Server.

- ***Jak zmienić hasło użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby zmienić hasło użytkownika uwierzytelnionego przy użyciu protokołu Kerberos, uruchom następującą komendę:

  ```
  passwd –R KRB5files foo
  ```

  Jeśli KDC obsługuje komendę **kpasswd**, komenda **passwd** zmienia hasło użytkownika Kerberos foo@MYREALM na serwerze Kerberos.

- ***Jak zezwolić użytkownikom na zmianę haseł, które utraciły ważność na kliencie?***

  Aby zezwolić użytkownikom na zmianę haseł, które utraciły ważność na kliencie, dodaj opcję allow_expired_pwd=yes do pliku `methods.cfg`. Gdy dla tej opcji ustawiona jest wartość `yes`, użytkownicy, których hasła utraciły ważność, są proszeni o zmianę tych haseł. Jeśli dla tej opcji ustawiona jest wartość, no lub `not present`, tych użytkowników nie można uwierzytelnić.

  ```
  KRB5:
     program = /usr/lib/security/KRB5
     options = authonly,allow_expired_pwd=yes
  ```

- ***Jak przekształcić użytkownika systemu AIX w użytkownika uwierzytelnianego przy użyciu protokołu Kerberos?***

  Aby przekształcić użytkownika systemu AIX w użytkownika uwierzytelnianego przy użyciu protokołu Kerberos, wykonaj następujące czynności:

  1. Sprawdź, czy ten użytkownik ma konto w Windows Server Active Directory, uruchamiając następującą komendę:

     ```
     chuser registry=KRB5files SYSTEM=KRB5files foo
     ```

  2. Jeśli użytkownik nie ma konta w Active Directory, utwórz je i ustaw atrybuty SYSTEM oraz registry, używając komendy **chuser**. Konto Active Directory nie musi mieć takiej samej nazwy użytkownika, jak nazwa użytkownika AIX. Jeśli nazwa użytkownika w systemie AIX jest inna, użyj atrybutu auth_name, aby ją odwzorować na nazwę w Active Directory.

     ```
     chuser registry=KRB5files SYSTEM=KRB5files auth_name=Christopher chris
     ```

- ***Co zrobić w przypadku zapomnienia hasła?***

  Zapomniane hasło musi zmienić administrator Active Directory. Użytkownik root systemu AIX nie może ustawić hasła dla nazwy użytkownika Kerberos w Active Directory.

- ***Jakie jest znaczenie atrybutów auth_name i auth_domain?***

  Uwaga: Te atrybuty są opcjonalne. Jeśli system AIX obsługuje nazwy użytkowników dłuższe niż 8 znaków, użycie atrybutu auth_name może być zbędne.

  Atrybuty auth_name i auth_domain odwzorowują nazwy użytkowników w systemie AIX na nazwy użytkowników Kerberos w KDC. Na przykład, jeśli użytkownik systemu AIX chris ma atrybuty auth_name=christopher i auth_domain=SOMEREALM, to nazwą użytkownika Kerberos jest christopher@SOMEREALM. Przy użyciu atrybutu auth_domain żądania są wysyłane do dziedziny o

nazwie SOMEREALM zamiast do dziedziny domyślnej. Umożliwia to uwierzytelnienie użytkownika chris w dziedzinie SOMEREALM zamiast w dziedzinie MYREALM. W tym przykładzie należy także zmodyfikować plik `krb5.conf` w taki sposób, aby zawierał nazwę dziedziny SOMEREALM.

- ***Czy użytkownik uwierzytelniany przy użyciu protokołu Kerberos może być uwierzytelniany przy użyciu standardowego uwierzytelniania systemu AIX?***

  Tak, użytkownik uwierzytelniany przy użyciu protokołu Kerberos może być uwierzytelniany przy użyciu standardowego uwierzytelniania systemu AIX. W tym celu:

  1. Ustaw hasło w systemie AIX (`/etc/security/passwd`), używając komendy **passwd**:

     ```
     passwd -R files foo
     ```

  2. Zmień atrybuty registry i SYSTEM użytkownika w następujący sposób:

     ```
     chuser -R KRB5files registry=files SYSTEM=compat foo
     ```

     Ta komenda zmienia uwierzytelnianie z Kerberos na compat (korzystające z procedury crypt). Następnym razem, gdy użytkownik foo będzie próbował się zalogować, zostanie użyte hasło lokalne z pliku `/etc/security/passwd`.

     Uwierzytelniania crypt można także użyć jako mechanizmu zapasowego, zmieniając atrybut SYSTEM, aby zezwolić na uwierzytelnianie lokalne, gdy uwierzytelnianie Kerberos nie powiedzie się:

     ```
     chuser -R KRB5files SYSTEM="KRB5files or compat" foo
     ```

- ***Czy trzeba konfigurować serwer Kerberos w systemie AIX, gdy używana jest usługa Kerberos systemu Windows Server 2000?***

  Nie, nie trzeba konfigurować serwera Kerberos (KDC) na kliencie AIX, ponieważ użytkownicy są uwierzytelniani przy użyciu KDC Active Directory. Jeśli jednak serwer KDC usługi uwierzytelniania sieciowego w systemie AIX ma być używany jako serwer Kerberos do innego celu, trzeba skonfigurować serwer Kerberos w tym systemie.

- ***Co zrobić, jeśli system AIX nie akceptuje hasła?***

  Jeśli system AIX nie akceptuje hasła:

  – Upewnij się, że klient komunikuje się z serwerem Windows 2000 Active Directory Server.
  – Upewnij się, że hasło spełnia wymagania zarówno systemu AIX, jak i oprogramowania Windows Server 2000 Active Directory. Informacje na temat zmiany reguł strategii haseł w systemie AIX zawiera sekcja Zmienianie/wyświetlanie strategi.

  Uwaga: Nie można zmienić hasła dla usługi Kerberos w systemie Windows Server 2003.

- ***Co zrobić, jeśli nie można zalogować się w systemie?***

  Jeśli użytkownik nie może zalogować się w systemie, wykonaj następujące czynności:

  – W systemie Windows sprawdź, czy serwer KDC jest uruchomiony, wykonując następujące czynności:
    1. W Panelu sterowania wybierz ikonę Narzędzia administracyjne.
    2. Wybierz ikonę Usługi.
    3. Sprawdź, czy Kerberos Key Distribution Center ma status Uruchomione.
  – W systemie AIX sprawdź, czy plik `/etc/krb5/krb5.conf` wskazuje właściwe centrum KDC i czy ma poprawne parametry.
  – W systemie AIX sprawdź, czy plik tabeli kluczy klienta zawiera klucz hosta. Na przykład, jeśli domyślnym plikiem tabeli kluczy jest `/etc/krb5/krb5.keytab`, uruchom komendę:

    ```
    ktutil
    rkt /etc/krb5/krb5.keytab
    l
    ```

- Sprawdź, czy dane wyjściowe komendy **kvno** znajdujące się w pliku tabeli kluczy są zgodne z danymi wyjściowymi komendy **Ktpass**.
- Sprawdź, czy jeśli ustawiono atrybuty auth_name i auth_domain, to czy odnoszą się one do poprawnej nazwy użytkownika w centrum KDC Active Directory.
- Sprawdź, czy ustawiono atrybut SYSTEM dla logowania Kerberos.
- Sprawdź, czy hasło nie utraciło ważności.

- ***Jak wyłączyć weryfikację biletu nadania biletu?***

  Weryfikację biletu nadania biletu można wyłączyć, podając opcję w pliku `/usr/lib/security/methods.cfg` w sekcji KRB5:

  ```
  KRB5:
     program = /usr/lib/security/KRB5
     options = tgt_verify=no
  KRB5files:
     options = db=BUILTIN,auth=KRB5
  ```

  Dopuszczalne wartości dla opcji tgt_verify to no lub `false` służące do wyłączenia weryfikacji biletu nadania biletu i wartości `yes` lub `true` służące do włączenia weryfikacji biletu nadania biletu. Domyślnie weryfikacja biletu nadania biletu jest włączona. Ustawienie wartości no dla opcji tgt_verify powoduje wyłączenie weryfikacji biletu nadania biletu i nie trzeba wtedy przekazywać kluczy host-użytkownik. Ta zmiana eliminuje tylko konieczność posiadania pliku tabeli kluczy na potrzeby uwierzytelniania. Inne aplikacje obsługujące Kerberos mogą wymagać pliku tabeli kluczy dla nazw użytkowników hosta i usługi.

- ***Co zrobić, jeśli nie można się zalogować, ponieważ nazwa hosta nie jest tłumaczona, a użycie pełnej nazwy hosta kończy się niepowodzeniem?***

  Weryfikacja biletu nadania biletu wymaga utworzenia nazwy użytkownika `host/<nazwa_hosta>` w centrum KDC. Ta nazwa hosta jest pełną nazwą klienta, na którym wykonywane jest uwierzytelnianie. System klienta żąda biletu usług, używając nazwy użytkownika hosta `host/<nazwa_hosta>`. W niektórych konfiguracjach komputer klienta nie może uzyskać pełnej nazwy hosta i zamiast niej uzyskuje krótką nazwę. W takich sytuacjach występuje niezgodność, weryfikacja biletu nadania biletu kończy się niepowodzeniem i logowanie także kończy się niepowodzeniem. Na przykład, jeśli `/etc/hosts` ma tylko krótką nazwę i plik `/etc/netsvc.conf` określa hosts=local,bind, to tłumaczenie nazw zwraca krótką nazwę.

  Aby usunąć problemy z tłumaczeniem nazw, wykonaj jeden z poniższych kroków:

  - Zmodyfikuj kolejność tłumaczenia nazw w pliku `/etc/netsvc.conf`, aby zwracana była pełna nazwa hosta. Plik `netsvc.conf` określa sekwencyjną kolejność tłumaczenia nazw hostów i aliasów.

    W poniższym przykładzie program tłumaczący używa usługi BIND do przetłumaczenia nazwy hosta. Jeśli usługa BIND nie powiedzie się, program tłumaczący użyje pliku `/etc/hosts`. Jeśli obie metody nie powiodą się, program tłumaczący użyje nis.

    ```
    hosts=bind,local,nis
    ```

    Jeśli pierwszą metodą używaną w kolejności wyszukiwania musi być `local`, zmień krótką nazwę (myhost) w pliku `/etc/hosts` na pełną nazwę hosta (myhost.austin.ibm.com).
  - Jeśli weryfikacja biletu nadania biletu nie jest wymagana, poszukaj instrukcji dotyczących wyłączania weryfikacji biletu nadania biletu w sekcji *Jak wyłączyć weryfikację biletu nadania biletu?*.

- ***Dlaczego procedura passwdexpired zwraca wartość 0, gdy hasło użytkownika Kerberos utraci ważność na serwerze Kerberos z systemem innym niż AIX?***

  Procedura **passwdexpired** zwraca wartość 0, ponieważ nie można bezpośrednio uzyskać informacji o utracie ważności hasła z serwera Kerberos z systemem innym niż AIX z uwagi na niezgodność lub niedostępność interfejsów **kadmin**.

  Flaga **allow_expired_pwd** w pliku **methods.cfg** umożliwia systemowi AIX uzyskanie informacji o utracie ważności hasła z użyciem interfejsu uwierzytelniania Kerberos. Rzeczywisty status informacji o utracie

ważności hasła jest uzyskiwany w momencie logowania lub po wywołaniu procedury **authenticate** i procedury **passwdexpired**.

Moduł protokołu Kerberos
Moduł protokołu Kerberos jest rozszerzeniem jądra używanym przez klienta NFS i kod serwera. Umożliwia on klientowi NFS i kodowi serwera przetwarzanie integralności komunikatów protokołu Kerberos i funkcji prywatności bez wywoływania demona **gss**.

Moduł protokołu Kerberos jest ładowany przez demon **gss**. Używane w nim metody są oparte na usłudze uwierzytelniania NAS (Network Authentication Service), wersja 1.2, która z kolei jest oparta na protokole MIT Kerberos.

Moduł protokołu Kerberos znajduje się w lokalizacji: `/usr/lib/drivers/krb5.ext`.

Informacje pokrewne można znaleźć w opisie demona **gss**.

Informacje pokrewne
Zasoby IBM developerWorks dotyczące usługi uwierzytelniania sieciowego IBM i technologie pokrewne dla systemu AIX

Serwer RADIUS

RADIUS (Remote Authentication Dial-In User Service) jest protokołem dostępu sieciowego IBM zaprojektowanym na potrzeby uwierzytelniania, autoryzowania i rozliczania. Jest protokołem działającym w oparciu o port, definiującym komunikację między serwerami NAS a serwerami uwierzytelniającymi i kont.

Serwer NAS działa jako klient RADIUS. Transakcje między klientem a serwerem RADIUS są uwierzytelniane przez użycie *sekretu współużytkowanego*, który nie jest przesyłany przez sieć. Wszystkie hasła użytkownika wysyłane między klientem a serwerem RADIUS są szyfrowane.

Klient jest odpowiedzialny za przesłanie informacji o użytkowniku do wyznaczonych serwerów RADIUS, a następnie podjęcie działania odpowiedniego do otrzymanej odpowiedzi. Serwery RADIUS są odpowiedzialne za odbieranie żądań połączenia od użytkowników, uwierzytelnianie użytkowników, a następnie zwracanie wszystkich informacji konfiguracyjnych wymaganych przez klienta do zapewnienia usługi dla użytkowników. Po skonfigurowaniu zaawansowanych informacji o serwerze proxy serwer RADIUS może działać jako klient proxy dla pozostałych serwerów RADIUS. Jako protokół transportowy serwer RADIUS wykorzystuje protokół UDP (User Datagram Protocol).

Protokół uwierzytelniania i autoryzacji serwera RADIUS jest oparty na standardzie IETF RFC 2865. Serwer udostępnia także protokół rozliczania zdefiniowany przez standard RFC 2866. Pozostałe obsługiwane standardy to: RFC 2284 (EAP), części standardu RFC 2869, komunikaty o utracie ważności hasła standardu RFC 2882, MD5-Challenge i TLS. Więcej informacji na temat tych RFC można znaleźć, klikając następujące odsyłacze:

IETF RFC 2865
http://www.ietf.org/rfc/rfc2865.txt

RFC 2866
http://www.ietf.org/rfc/rfc2866.txt

RFC 2284
http://www.ietf.org/rfc/rfc2284.txt

RFC 2869
http://www.ietf.org/rfc/rfc2869.txt

RFC 2882
http://www.ietf.org/rfc/rfc2882.txt

Wszystkie te standardy RFC można także odnaleźć w serwisie http://www.ietf.org.

Instalowanie serwera RADIUS
Serwer RADIUS można zainstalować, korzystając albo z komendy **installp**, albo z programu SMIT. Oprogramowanie serwera RADIUS znajduje się na podstawowym nośniku AIX, a obrazy mają nazwy radius.base i bos.msg.<język>.rte.

Jeśli jako baza danych informacji do przechowywania nazw użytkowników i ich haseł ma być wykorzystywany katalog LDAP, należy zainstalować obraz ldap.server. Na każdym serwerze RADIUS musi być zainstalowane oprogramowanie **installp**.

Jeśli planowane jest użycie uwierzytelniania EAP-TLS (na przykład do uwierzytelniania certyfikatów cyfrowych lub sieci bezprzewodowej), należy także zainstalować oprogramowanie OpenSSL 0.9.7 lub nowsze i podać pełną ścieżkę do biblioteki libssl.a w pliku konfiguracyjnym `/etc/radius/radiusd.conf`.

Demony RADIUS można uruchamiać za pomocą komendy **radiusctl**. Po uruchomieniu działa kilka procesów radiusd, po jednym dla następujących zadań:

- autoryzacja
- rozliczanie
- monitorowanie innych demonów

Po restarcie demony są automatycznie uruchamiane na poziomie działania 2, chyba że serwer RADIUS został skonfigurowany dla EAP-TLS.

Aby zmienić tę procedurę, należy zmodyfikować plik `/etc/rc.d/rc2.d/Sradiusd`.

Uwaga: Jeśli serwer RADIUS został skonfigurowany do uwierzytelniania certyfikatów cyfrowych za pomocą EAP-TLS, nie można skonfigurować automatycznego uruchamiania demonów, ponieważ fraza certyfikatu musi być wprowadzona przez administratora, co wymaga ręcznego uruchomienia i restartowania serwera RADIUS za pomocą komendy **radiusctl**.

Zatrzymywanie i restartowanie serwera RADIUS
Zawsze podczas wprowadzania zmian w pliku konfiguracyjnym `/etc/radius/radiusd.conf` serwera RADIUS albo w domyślnych plikach autoryzacji `/etc/radius/authorization/default.policy` lub `/etc/radius/authorization/default.auth` demony **radiusd** należy zatrzymać i zrestartować. Zadanie to można wykonać za pomocą programu SMIT lub w wierszu komend.

Aby uruchomić, zrestartować i zatrzymać serwer RADIUS, należy użyć następujących komend:

```
radiusctl start
radiusctl restart
radiusctl stop
```

Zatrzymywanie i uruchamianie serwera RADIUS jest konieczne, ponieważ demon dla wszystkich domyślnych atrybutów zawartych w powyższych plikach konfiguracyjnych musi zbudować tabelę pamięci. W celu poprawienia wydajności dla każdego użytkownika lokalnego wykorzystywana jest pamięć współużytkowana, a tabela użytkownika lokalnego jest budowana podczas inicjowania demona.

Opcja na żądanie
W razie potrzeby można uruchomić wiele demonów serwerów uwierzytelniających i rozliczających RADIUS.

Każdy serwer nasłuchuje na oddzielnym porcie. Plik `radiusd.conf` dostarczany jest z domyślnym numerem portu 1812 dla opcji uwierzytelniania i 1813 dla opcji rozliczania. Są to numery portów przypisane przez IANA. Jeśli plik `radiusd.conf` jest aktualizowany, te numery portów, mogą być używane razem z innymi portami (wieloma). Należy upewnić się, że numery portów nie są przypisane do istniejących usług. Jeśli w polach **Authentication_Ports** i **Accounting_Ports** pliku `radiusd.conf` zostanie wprowadzonych wiele numerów portów, dla każdego portu uruchamiany będzie demon **radiusd**. Demony będą nasłuchiwać na odpowiednich numerach portów.

Pliki konfiguracyjne serwera RADIUS
Demon serwera RADIUS korzysta z kilku plików konfiguracyjnych. Przykładowe wersje tych plików dostarczane są w pakiecie serwera RADIUS.

Właścicielem wszystkich plików konfiguracyjnych jest użytkownik root oraz grupa `security`. Wszystkie pliki konfiguracyjne, oprócz pliku słownika, można edytować za pomocą programu SMIT. W celu zastosowania wszystkich zmian wprowadzonych w plikach konfiguracyjnych serwer musi być zrestartowany.

Plik radiusd.conf

Plik `radiusd.conf` zawiera parametry konfiguracyjne serwera RADIUS.

Domyślnie serwer RADIUS szuka pliku `radiusd.conf` w katalogu `/etc/radius`. Pozycje pliku konfiguracyjnego muszą być zapisane w formacie zaprezentowanym w przykładowym pliku. Serwer RADIUS akceptuje tylko poprawne słowa kluczowe i wartości, a w przypadku użycia niepoprawnego słowa kluczowego lub wartości korzysta z wartości domyślnej. Po uruchomieniu demonów serwera RADIUS należy sprawdzić, czy w protokole SYSLOG znajdują się wpisy dotyczące błędów parametrów konfiguracyjnych. Nie wszystkie błędy konfiguracji powodują zatrzymanie serwera.

Ten plik powinien być odpowiednio zabezpieczony przed odczytem i zapisem, ponieważ wpływa on na zachowanie serwerów uwierzytelniających i rozliczających. Plik ten może także zawierać poufne dane.

Ważne: Jeśli użytkownik dokonuje edycji pliku `radiusd.conf`, nie może zmieniać kolejności pozycji. Na tej kolejności opierają się panele programu SMIT.

Poniżej przedstawiono przykład pliku `radiusd.conf`:

```
#------------------------------------------------------------------#
#             PLIK KONFIGURACYJNY                                  #
#                                                                  #
#  Domyślnie serwer RADIUS szuka pliku radiusd.conf w              #
#  katalogu /etc/radius.                                          #
#                                                                  #
#  Pozycje pliku konfiguracyjnego muszą być w poniższych           #
#  formatach.  Serwer RADIUS akceptuje tylko poprawne słowa        #
#  kluczowe i wartości, a jeśli nie zostaną podane lub są          #
#  podane błędnie, używa wartości domyślnych.                      #
#                                                                  #
#  Po uruchomieniu demonów radius trzeba sprawdzić dane wyjściowe  #
#  syslog w poszukiwaniu błędów parametrów konfiguracyjnych.       #
# Ponownie, nie wszystkie błędy konfiguracji spowodują             #
#  zatrzymanie serwera.                                            #
#                                                                  #
#  Ten plik powinien być odpowiednio zabezpieczony przed odczytem  #
#  i zapisem, ponieważ wpływa on na zachowanie się serwera         #
#  uwierzytelniającego i rozliczającego i może zawierać poufne     #
#  lub tajne materiały.                                             #
#                                                                  #
#  JEŚLI EDYTUJESZ TEN PLIK, NIE ZMIENIAJ KOLEJNOŚCI POZYCJI W     #
#  PLIKU. OD TEJ KOLEJNOŚCI ZALEŻĄ PANELE PROGRAMU SMIT.           #
#                                                                  #
#                                                                  #
#------------------------------------------------------------------#

#------------------------------------------------------------------#
#                Konfiguracja globalna                             #
#                                                                  #
#   RADIUSdirectory  :  Jest to podstawowy katalog dla demona      #
#                       RADIUS. Demon przeszuka ten katalog        #
#                       w poszukiwaniu plików konfiguracyjnych.    #
#                                                                  #
#   Database_location : Jest to wartość, w której będą             #
#                       przechowywane i odtwarzane dane            #
#                       uwierzytelniające (id użytkowników         #
#                       oraz hasła).                               #
#                       Poprawne wartości: Local, LDAP, UNIX       #
#                       UNIX  - zdefiniowane w systemie AIX        #
#                       Local - lokalna baza AVL używająca raddbm  #
#                       LDAP  - centralna baza danych              #
#                                                                  #
#   Local_Database   :  Wskazuje nazwę pliku lokalnej bazy danych, #
#                       który ma być użyty.                        #
#                       To pole musi być wypełnione, jeśli         #
#                       położenie bazy ma wartość Local.           #
#                                                                  #
#   Debug_Level      :  Ta para ustawia poziom debugowania, na     #
#                       którym będzie działał serwer RADIUS.       #
#                       Poprawne wartości to 0,3 lub 9. Domyślną   #
#                       wartością jest 3. Wynik jest kierowany do  #
#                       lokalizacji podanej w sekcji *.debug       #
#                       pliku /etc/syslog.conf                     #
#                                                                  #
#                       Każdy poziom zwiększa liczbę komunikatów   #
#                       wysyłanych do syslog. Na przykład "9" to   #
#                       nowe komunikaty udostępniane przez "9" i   #
#                       wszystkie generowane przez poziomy 0 i 3.  #
```

```
#                                                                     #
#                       0 : zapewnia minimalne dane dla protokołu     #
#                           syslogd. Wysyła komunikaty o              #
#                           uruchomieniu i zakończeniu każdego        #
#                           procesu RADIUS. Protokołuje także         #
#                           warunki błędów.                           #
#                                                                     #
#                       3 : obejmuje ogólne komunikaty ACCESS         #
#                           ACCEPT, REJECT i DISCARD dla każdego      #
#                           pakietu. Zapewnia ogólną kontrolę         #
#                           śledzenia dla uwierzytelniania.           #
#                                                                     #
#                       9 : maksymalna ilość danych. Specyficzne      #
#                           wartości atrybutów dla przekazywanej      #
#                           przez przetwarzanie transakcji oraz       #
#                           o wiele więcej.                           #
#                          [NIE zalecany przy normalnym działaniu]    #
#                                                                     #
#---------------------------------------------------------------------#
RADIUSdirectory   : /etc/radius
Database_location : UNIX
Local_Database    : dbdata.bin
Debug_Level       : 3
#---------------------------------------------------------------------#
#                 Konfiguracja rozliczania                            #
#                                                                     #
#   Local_Accounting :  Gdy ta flaga jest ustawiona na ON lub TRUE,   #
#                       plik będzie zawierał zapis pakietów           #
#                       ACCOUNTING, START i STOP otrzymanych z        #
#                       serwera Network Access Server(NAS).  #
#                       Domyślnym plikiem protokołu jest:             #
#                           /var/radius/data/accounting               #
#                                                                     #
#  Local_accounting_loc  : /var/radius/data/accounting                #
#                          ścieżka i nazwa lokalnego pliku danych     #
#                          rozliczenia. Używana, tylko jeśli Local_   #
#                          Accounting=ON. Jeśli zmieni się wartość    #
#                          domyślną, administrator musi utworzyć      #
#                          ścieżkę i plik (z odpowiednimi             #
#                          uprawnieniami).                              #
#                                                                     #
#---------------------------------------------------------------------#
Local_Accounting     : ON
Local_Accounting_loc : /var/radius/data/accounting
#---------------------------------------------------------------------#
#     Atrybuty komunikatu odpowiedzi                                  #
#                                                                     #
#     Accept_Reply-Message : Wysyłany, gdy serwer RADIUS odpowiada    #
#                            pakietem Access-Accept                   #
#                                                                     #
#     Reject_Reply-Message : Wysyłany, gdy serwer RADIUS odpowiada    #
#                            pakietem Access-Reject                   #
#                                                                     #
#     Challenge_Reply-Message : Wysyłany, gdy serwer RADIUS           #
#                               odpowiada pakietem                    #
#                               Access-Challenge                      #
#---------------------------------------------------------------------#
Accept_Reply-Message :
Reject_Reply-Message :
Challenge_Reply-Message :
Password_Expired_Reply-Message :
#---------------------------------------------------------------------#
#    Obsługa odnawiania hasła, które utraciło ważność                 #
#                                                                     #
#    Allow_Password_Renewal: YES lub NO                               #
#                            Ustawienie tego atrybutu na YES          #
#                            pozwala użytk. zaktualizować hasło       #
#                            przez protokół RADIUS. Wymaga to         #
#                            obsługi sprzętowej pakietów              #
#                            Access-Password-Request.                 #
#---------------------------------------------------------------------#
Allow_Password_Renewal  : NO
#---------------------------------------------------------------------#
#    Wymaganie hosta uwierzytelniającego w pakiecie Access-Request    #
#                                                                     #
#    Require_Message_Authenticator: YES lub NO                        #
#                                   Ustawienie tego atrybutu na       #
#                                   YES sprawdza host w pakiecie      #
#                                   Access-Request. Jeśli nie jest    #
#                                   podany, pakiet zostanie           #
#                                   odrzucony.                        #
#---------------------------------------------------------------------#
```

```
Require_Message_Authenticator : NO
#-------------------------------------------------------------------#
#          Serwery (uwierzytelniające i rozliczające)               #
#                                                                   #
#   Authentication_Ports : To pole wskazuje, na którym porcie       #
#                          nasłuchuje serwer uwierzytelniający.     #
#                          Jeśli pole jest puste, demon             #
#                          uwierzytelniający nie zostanie           #
#                          uruchomiony.                             #
#                          Pole może zawierać więcej niż jedną      #
#                          wartość. Każda wartość MUSI być          #
#                          oddzielona przecinkiem ','.              #
#                                                                   #
#                          Pole musi zawierać wartość liczbową,     #
#                          taką jak "6666". W przypadku, gdy demon  #
#                          ma nasłuchiwać na porcie "6666".         #
#                                                                   #
#   Accounting_Ports     : Tak samo, jak dla pola                   #
#                          authentication_Ports. Patrz wyżej.       #
#                                                                   #
#[UWAGA] Nie odbywa się żadne sprawdzanie konfliktów portów. Jeśli  #
#        dla danego portu działa serwer, demon spowoduje powstanie  #
#        błędu i nie uruchomi się. Należy sprawdzić dane w          #
#        w protokole syslog, aby sprawdzić, czy wszystkie serwery   #
#        uruchomiły się.                                            #
#                                                                   #
#                                                                   #
# [Przykład]                                                        #
#  Authentication_Ports : 1812,6666 (bez spacji między przecinkami)#
#                                                                   #
#   W powyższym przykładzie serwer zostanie uruchomiony dla         #
#   każdego podanego portu. W przypadku                             #
#                                                                   #
#           6666 : port 6666                                        #
#                                                                   #
#-------------------------------------------------------------------#
Authentication_Ports  : 1812
Accounting_Ports      : 1813
#-------------------------------------------------------------------#
#       Informacje o użytkowniku katalogu LDAP                      #
#                                                                   #
#   Wymagane jeśli RADIUS podłączono do katalogu LDAP wersja 3      #
#   a pole Database_location ma wartość LDAP                        #
#                                                                   #
#   LDAP_User     : Id użytkownika, który ma uprawnienia admin do   #
#                   łączenia ze zdalną bazą (LDAP). Jest to nazwa   #
#                   wyróżniająca administratora LDAP.               #
#                                                                   #
#   LDAP_User_Pwd : Hasło związane z powyższym Id użytkownika,      #
#                   które wymagane jest do uwierzytelnienia w       #
#                   katalogu LDAP.                                  #
#                                                                   #
#-------------------------------------------------------------------#
LDAP_User        : cn=root
LDAP_User_Pwd    :
#-------------------------------------------------------------------#
#       Informacje katalogu LDAP                                    #
#                                                                   #
#   Jeśli pole Database_location ma wartość "LDAP", wtedy           #
#   wypełnione muszą być następujące pola.                          #
#                                                                   #
#   LDAP_Server_name     : To pole określa pełną nazwę hosta,       #
#                          na którym znajduje się serwer LDAP w     #
#                          wersji 3.                                #
#   LDAP_Server_Port     : Numer portu TCP dla serwera LDAP         #
#                          Standardowy port LDAP to 389.            #
#   LDP_Base_DN          : Nazwa wyróżn. do rozpoczęcia wyszuk.     #
#   LDAP_Timeout         : liczba sekund oczekiwania na             #
#                          z odpowiedź serwera LDAP                 #
#   LDAP_Hoplimit        : maksymalna liczba odwołań do             #
#                          wystąpienia w sekwencji                  #
#   LDAP_Sizelimit       : limit wielk. (w pozycjach) dla wyszuk.   #
#   LDAP_Debug_level     : 0=OFF 1=Trace ON                         #
#                                                                   #
#-------------------------------------------------------------------#
LDAP_Server_name          :
LDAP_Server_port          :  389
LDAP_Base_DN              :  cn=aixradius
LDAP_Timeout              :  10
LDAP_Hoplimit             :  0
LDAP_Sizelimit            :  0
LDAP_Debug_level          :  0
```

```
#-------------------------------------------------------------------#
#       Informacje serwera PROXY RADIUS                             #
#                                                                   #
#                                                                   #
#   Proxy_Allow               :  ON lub OFF. Jeśli ma wartość ON,   #
#                                serwer może                        #
#                                przekazywać pakiety do dziedzin,   #
#                                które zna, i skonfigurowane muszą  #
#                                być następujące pola.              #
#   Proxy_Use_Table           :  ON lub OFF. Jeśli ma wartość ON,   #
#                                serwer może                        #
#                                korzystać z tabeli do szybszego    #
#                                przetwarzania powtórzonych żądań.  #
#                                Może być używane bez proxy         #
#                                równego ON, ale wymagane jest,     #
#                                aby miało wartość ON, jeśli        #
#                                Proxy_Use_Table jest równe ON.     #
#   Proxy_Realm_name          :  To pole określa dziedzinę, którą   #
#                                ten serwer obsługuje.              #
#   Proxy_Prefix_delim        :  Lista separatorów do analizowania  #
#                                nazw dziedzin dodawanych jako      #
#                                przyr. do nazw użytk. Ta lista     #
#                                musi być obustronnie wyłączna dla  #
#                                separatorów przedrostków.          #
#   Proxy_Suffix_delim        :  Lista separatorów do analizowania  #
#                                nazw dziedzin dodawanych jako      #
#                                przyr. do nazw użytk. Ta lista     #
#                                musi być obustronnie wyłączna dla  #
#                                separatorów przedrostków.          #
#   Proxy_Remove_Hops         :  YES lub NO. Jeśli YES wtedy proxy  #
#                                usunie nazwę dziedziny, nazwy      #
#                                dziedzin poprzednich przeskoków    #
#                                i nazwę dziedziny następnego       #
#                                serwera, do którego przekazywany   #
#                                jest pakiet.                       #
#                                                                   #
#   Proxy_Retry_count         :  Liczba prób wysyłania pakietu      #
#                                żądania.                           #
#                                                                   #
#   Proxy_Time_Out            :  Liczba sekund do odczekania        #
#                                między próbami.                    #
#                                                                   #
#-------------------------------------------------------------------#
Proxy_Allow               :   OFF
Proxy_Use_Table           :   OFF
Proxy_Realm_name          :
Proxy_Prefix_delim        :   $/
Proxy_Suffix_delim        :   @.
Proxy_Remove_Hops         :   NO
Proxy_Retry_count         :   2
Proxy_Time_Out            :   30
#-------------------------------------------------------------------#
#    Konfiguracja uwierzytelniania lokalnego systemu operacyjnego  #
#                                                                   #
# UNIX_Check_Login_Restrictions : ON lub OFF. Jeśli ON, to podczas  #
#                                  uwierzytelniania lokalnego       #
#                                  systemu operacyjnego następuje   #
#                                  wywołanie loginrestrictions() w  #
#                                  celu sprawdzenia, czy użytkownik #
#                                  nie ma lokalnych                 #
#                                  ograniczeń logowania.   #
#                                                                   #
#-------------------------------------------------------------------#
UNIX_Check_Login_Restrictions : OFF
#-------------------------------------------------------------------#
#    Globalna opcja pul IP                                          #
#                                                                   #
#  Enable_IP_Pool : ON lub OFF. Jeśli ON, to serwer RADIUS będzie   #
#                   przypisywał adres IP z puli adresów,            #
#                   która została dla niego zdefiniowana.                 #
#                                                                   #
#-------------------------------------------------------------------#
Enable_IP_Pool            :   OFF
#-------------------------------------------------------------------#
# Send Accept MA: ON lub OFF. Niektóre serwery NAS nie akceptują,   #
#                 gdy elementy uwierzytelniające komunikaty         #
#                 są w komunikacie ACCEPT. Użyj tej opcji, aby      #
#                 wyłączyć wysłanie elementu uwierzytelniającego    #
#                 komunikaty podczas wysyłania komunikatu ACCEPT.                #
#                                                                   #
# UWAGA: Czasami te same serwery NAS nie akceptują także            #
#        dostosowanych komunikatów ACCEPT.                          #
```

```
#                                                                   #
#-------------------------------------------------------------------#
Send_Accept_MA : ON
#-------------------------------------------------------------------#
#                                                                   #
# Maximum_Threads : Liczba wątków, które utworzą proces do obsługi #
#                   żądań uwierzytelniania.                         #
#                   Jeśli nie zostanie podana żadna wartość,        #
#                   domyślną wartością RADIUS będzie 10.            #
#                                                                   #
#-------------------------------------------------------------------#
Maximum_Threads : 99
#-------------------------------------------------------------------#
#                                                                   #
# EAP_Conversation_Timeout : Liczba sekund do odczekania zanim      #
#                            konwersacja stanie się nieaktualna     #
#                            i zostanie usunięta.                   #
#                                                                   #
# UWAGA: Chroni to przed atakami typu odmowa usługi (DoS) na        #
#        serwerze uwierzytelniającym RADIUS. Jeśli w sieci          #
#        występuje duże opóźnienie, konieczne może być zwiększenie  #
#        wartości tego limitu czasu.                                #
#                                                                   #
#-------------------------------------------------------------------#
EAP_Conversation_Timeout : 30
#-------------------------------------------------------------------#
# Globalne ustawienia konfiguracyjne EAP-TLS (eap-tls):             #
#                                                                   #
# Przykłady:                                                        #
#                                                                   #
# Enable_EAP-TLS : ON lub OFF. Jeśli ma wartość ON, serwer może     #
#                  użyć OpenSSL do uwierzytelnienia użytkowników    #
#                  za pomocą EAP-TLS. Ci użytkownicy muszą mieć     #
#                  mieć typ uwierzytelniania EAP 13                 #
#                  (lub EAP-TLS). To ustawienie można znaleźć w     #
#                  smitty za pomocą: 'smitty rad_conf_users'        #
#                                                                   #
# UWAGA: Atrybuty podane poniżej są ignorowane, jeśli               #
#        powyższy atrybut 'Enable_EAP' nie ma wartości 'ON'.        #
#                                                                   #
# OpenSSL_Library : /opt/freeware/lib/libssl.a(libssl.so.0.9.7)     #
# OpenSSL_Ciphers : ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH               #
# RootCA_Dir          : /etc/radius/tls                             #
# RootCA_File         : /etc/radius/tls/cacert.pem                  #
# Server_Cert_File    : /etc/radius/tls/cert-srv.pem                #
# Server_PrivKey_File : /etc/radius/tls/cert-srv.pem                #
# Server_CRL_File     : /etc/radius/tls/crl.pem                     #
#                                                                   #
# UWAGA: Server_Cert_File i Server_PrivKey_File mogą być tym samym  #
#        plikiem, jeśli plik ten ma następujący format              #
#        (niekoniecznie w takiej kolejności):                       #
#                                                                   #
#       -----BEGIN RSA PRIVATE KEY-----                             #
#       Proc-Type: 4,ENCRYPTED                                      #
#       <dane klucza prywatnego rsa>                                #
#       -----END RSA PRIVATE KEY-----                               #
#       -----BEGIN CERTIFICATE-----                                 #
#       <dane certyfikatu>                                          #
#       -----END CERTIFICATE-----                                   #
#                                                                   #
#-------------------------------------------------------------------#
Enable_EAP-TLS      : ON
OpenSSL_Library     : /opt/freeware/lib/libssl.a(libssl.so.0.9.7)
OpenSSL_Ciphers     : ALL:!ADH:RC4+RSA:+SSLv2:@STRENGTH
RootCA_Dir          : /etc/radius/tls
RootCA_File         : /etc/radius/tls/radiusdcacert.pem
Server_Cert_File    : /etc/radius/tls/cert-srv.pem
Server_PrivKey_File : /etc/radius/tls/cert-srv.pem
Server_CRL_File     :
```

Metodę uwierzytelniania EAP dla każdego użytkownika można ustawić przy użyciu programu SMIT. Aby ustawić metody EAP dla każdego użytkownika, należy wykonać następujące czynności:

```
Serwer Radius
     -> Konfiguruj użytkowników
          -> Lokalna baza danych
             Katalog LDAP
                  -> Dodaj użytkownika
                     Zmień / pokaż charakterystykę użytkownika
                          ->
```

```
                            Identyfikator użytkownika [ ]
                            Typ EAP [0 2 4]
                            MAKS. WIEK hasła
```

W polu Typ EAP dostępne są następujące opcje:

0
Brak

2
MD5 - Challenge

4
TLS

Wybrana metoda EAP jest porównywana z sekwencją metody uwierzytelniania ustawioną w pliku `radiusd.conf`.

Plik /etc/radius/clients

Plik `clients` zawiera listę klientów, które mogą wysyłać żądania do serwera RADIUS.

Zazwyczaj dla każdego klienta, serwera NAS lub AP, należy podać jego adres IP wraz z danymi szyfrującymi współużytkowanymi między serwerem RADIUS a klientem oraz z opcjonalną *nazwę puli* dla pul IP.

Plik składa się z pozycji zapisanych w następującej postaci:

```
<Adres IP klienta>    <Współużytkowane dane szyfrujące> <Nazwa puli>
```

Przykładowa lista pozycji wygląda następująco:

```
10.10.10.1      mojedaneszyfrujące1      piętro6
10.10.10.2      mojedaneszyfrujące2      piętro5
```

Współużytkowane dane szyfrujące to łańcuch znaków skonfigurowany na sprzęcie klienckim oraz na serwerze RADIUS. Maksymalna długość tych danych wynosi 256 bajtów; jest w nich rozróżniana wielkość liter. Współużytkowane dane szyfrujące nie są wysyłane w żadnym z pakietów RADIUS i nigdy nie są przesyłane przez sieć. Administrator systemu musi zapewnić skonfigurowanie dokładnie takich samych danych szyfrujących po obu stronach (klienta i serwera RADIUS). Współużytkowane dane szyfrujące służą do szyfrowania hasła użytkownika; można je także wykorzystać do sprawdzenia integralności komunikatu przy użyciu atrybutu uwierzytelniania komunikatu (Message Authentication).

Współużytkowane dane szyfrujące każdego klienta powinny być unikalne w pliku `/etc/radius/clients` oraz składać się, podobnie jak każde dobre hasło, z kombinacji wielkich i małych liter, cyfr i symboli. W celu zapewnienia bezpieczeństwa dane te powinny zawierać co najmniej 16 znaków. Plik `/etc/radius/clients` można modyfikować za pomocą programu SMIT. Współużytkowane dane szyfrujące należy często zmieniać, aby zapobiec atakom z użyciem słownika.

Nazwa puli jest nazwą puli, z której przydzielane są globalne adresy IP podczas translacji dynamicznej. Administrator systemu tworzy *nazwę puli* podczas konfigurowania serwera RADIUS. Korzystając z panelu programu SMIT, można dodać *nazwę_puli* za pomocą opcji menu **Konfiguruj reguły proxy** > **IP Pool (Pula IP)** > **Utwórz pulę IP**. Informacja ta jest używana podczas określania puli IP po stronie serwera.

Plik /etc/radius/dictionary

Plik `dictionary` zawiera opisy atrybutów, które są definiowane przez protokół RADIUS i obsługiwane przez serwer RADIUS w systemie AIX.

Są one używane przez demon RADIUS podczas sprawdzania poprawności i tworzenia danych pakietu. W tym pliku powinny być dodane także atrybuty specyficzne dla dostawcy. Plik dictionary można edytować za pomocą dowolnego edytora. Program SMIT nie ma odpowiedniego interfejsu.

Poniżej zaprezentowano część przykładowego pliku dictionary:

```
##########################################################################
#                                                                        #
#   Ten plik zawiera tłumaczenia słownikowe do analizy żądań             #
#   i generowania odpowiedzi.  Wszystkie transakcje są komponowane       #
```

```
#   z par atrybut/wartość. Wartość każdego atrybutu określona jest     #
#   jako jeden z 4 typów danych. Poprawnymi typami danych są:          #
#                                                                      #
#   string - oktety 0-253                                              #
#   ipaddr - 4 oktety w kolejności bajtów sieciowych                   #
#   integer - 32-bitowa wartość w układzie big endian                  #
#             (starszy bajt pierwszy)                                  #
#   date - 32-bit wartość w układzie big endian - sekundy od           #
#                                  00:00:00 GMT,  1 styczeń 1970       #
#                                                                      #
#   Wyszczególnione wartości przechowywane są w pliku użytkownika z    #
#   tłumaczeniem słownikowym wartości do łatwiejszego administrowania. #
#                                                                      #
#   Przykład:                                                          #
#                                                                      #
#   ATTRIBUTE         VALUE                                            #
#   ---------------   -----                                            #
#   Framed-Protocol = PPP                                              #
#   7               = 1     (integer encoding)                         #
#                                                                      #
########################################################################
ATTRIBUTE       User-Name                       1       string
ATTRIBUTE       User-Password                   2       string
ATTRIBUTE       CHAP-Password                   3       string
ATTRIBUTE       NAS-IP-Address                  4       ipaddr
ATTRIBUTE       NAS-Port                        5       integer
ATTRIBUTE       Service-Type                    6       integer
ATTRIBUTE       Framed-Protocol                 7       integer
ATTRIBUTE       Framed-IP-Address               8       ipaddr
ATTRIBUTE       Framed-IP-Netmask               9       ipaddr
ATTRIBUTE       Framed-Routing                  10      integer
ATTRIBUTE       Filter-Id                       11      string
.
.
.
```

Uwaga: Każdy atrybut zdefiniowany w pliku `default.policy` lub pliku `default.auth` (bądź określonym pliku `identyfikator_użytkownika.policy` lub `identyfikator_użytkownika.auth`) musi być poprawnym atrybutem protokołu RADIUS, tak jak zdefiniowano to w lokalnym pliku konfiguracyjnym słownika AIX. Jeśli atrybut nie zostanie znaleziony w słowniku, demon **radiusd** nie załaduje go i zaprotokołowany zostanie komunikat o błędzie.

Uwaga: Jeśli słownik, plik `default.policy` i plik `default.auth` dla systemu zostaną zmodyfikowane, trzeba zrestartować demony RADIUS za pomocą komend **stopsrc** i **startsrc** lub za pomocą programu SMIT.

Plik /etc/radius/proxy

Plik `/etc/radius/proxy` jest plikiem konfiguracyjnym, który obsługuje opcję proxy. Ten plik odwzorowuje znane dziedziny, do których serwer proxy może przekazywać pakiety.

Plik `/etc/radius/proxy` korzysta z adresu IP serwera, który obsługuje pakiety dla danej dziedziny oraz sekret współużytkowany między dwoma serwerami.

Plik ten zawiera następujące pola, których zawartość można modyfikować przy użyciu programu SMIT:

- **Nazwa dziedziny**
- **Adres IP następnego przeskoku**
- **Współużytkowane dane szyfrujące**

Poniżej przedstawiono przykład pliku `/etc/radius/proxy`:

Uwaga:

Współużytkowane dane szyfrujące powinny mieć długość 16 znaków. Takie same współużytkowane dane szyfrujące muszą być skonfigurowane na serwerze RADIUS następnego przeskoku.

```
# @(#)91 1.3  src/rad/usr/sbin/config_files/proxy, radconfig, radius530 1/23/04 13:11:14
################################################################################
#                                                                              #
#       Ten plik zawiera listę dziedzin proxy, które są autoryzowane           #
#       do wysyłania/odbierania żądań/odpowiedzi proxy z/do tego               #
#       serwera RADIUS oraz ich sekret współużyt. używany do szyfr.            #
#                                                                              #
```

```
#       Pierwsze pole to nazwa dziedziny zdalnego serwera             #
#       RADIUS.                                                       #
#                                                                     #
#       Drugie pole to poprawny adres IP dla zdalnego serwera         #
#       RADIUS.                                                       #
#                                                                     #
#       Trzecia kolumna to sekret współużytkowany związany z tą       #
#       dziedziną.                                                    #
#                                                                     #
#UWAGA: Ten plik zawiera ważne informacje o bezpieczeństwie i dlatego #
#             należy podjąć środki ostrożności, aby zabezpieczyć      #
#             dostęp do niego.                                        #
#                                                                     #
#######################################################################
# REALM NAME               REALM IP               SHARED SECRET
#---------------       ------------------     ----------------------
#  mojaDziedzina           10.10.10.10           współużdaneszyfr
```

Uwierzytelnianie
Tradycyjne uwierzytelnianie korzysta z nazwy oraz stałego hasła i zazwyczaj ma miejsce, gdy użytkownik po raz pierwszy loguje się na komputerze lub żąda usługi. Serwer RADIUS używa bazy danych uwierzytelniania, w której przechowywane są identyfikatory użytkowników, hasła oraz pozostałe informacje.

W celu uwierzytelniania użytkowników serwer może korzystać z lokalnej bazy danych, haseł UNIX lub katalogu LDAP. Lokalizacja bazy danych podawana jest podczas procesu konfiguracji w pliku serwera `/etc/radius/radiusd.conf` lub podczas jego aktualizacji za pośrednictwem programu SMIT. Więcej informacji na temat plików konfiguracyjnych serwera RADIUS zawiera sekcja “Pliki konfiguracyjne serwera RADIUS” na stronie 327.

Bazy danych użytkowników
Oprogramowanie serwera RADIUS może przechowywać informacje o użytkownikach w różnych bazach danych.

Do przechowywania informacji o użytkownikach można wykorzystać lokalną bazę danych systemu UNIX lub bazę danych LDAP.

UNIX
Opcja uwierzytelniania UNIX umożliwia serwerowi RADIUS użycie w celu uwierzytelniania użytkowników metody uwierzytelniania systemu lokalnego.

Aby użyć uwierzytelniania lokalnego systemu UNIX, należy w pliku `radiusd.conf` zmodyfikować pole **database_location** lub wybrać wartość `UNIX` w polu `Położenie bazy danych` programu SMIT. Ta metoda w celu uwierzytelnienia identyfikatora użytkownika i hasła wywołuje funkcję API `authenticate()` systemu UNIX. Hasła zapisywane są w tym samym pliku danych, który wykorzystywany jest przez system UNIX. Jest to plik `/etc/passwords`. Identyfikatory użytkowników i hasła tworzone są za pomocą komendy **mkuser** lub za pośrednictwem programu SMIT.

Aby korzystać z bazy danych UNIX, należy wybrać opcję `UNIX` w polu **Położenie bazy danych**, tak jak przedstawiono poniżej:

```
       Konfiguruj serwer

Katalog RADIUS                                  /etc/radius
*Położenie bazy danych                           [UNIX]
Nazwa pliku lokalnej bazy danych AVL             [dbdata.bin]
Rozliczanie lokalne                  [WŁ]

Poziom śledzenia błędów              [3]
.
.
.
```

Lokalna
Jeśli pole **database_location** pliku `radiusd.conf` lub pozycja Położenie bazy danych programu SMIT zawiera słowo `Local` (Lokalna), wtedy serwer RADIUS, będzie umieszczał wszystkie identyfikatory użytkowników i hasła w pliku `/etc/radius/dbdata.bin`.

Lokalna baza danych użytkowników jest plikiem tekstowym, który zawiera informacje o identyfikatorach użytkowników oraz ich hasła. Hasła zapisane są w formacie mieszanym. Mieszanie jest techniką szybkiego adresowania służącą do bezpośredniego dostępu do danych w obszarze pamięci. Aby dodawać, usuwać lub modyfikować hasła, należy uruchomić komendę **raddbm** lub skorzystać z programu SMIT. Podczas uruchamiania demon **radiusd** odczytuje plik `radiusd.conf` i ładuje do pamięci identyfikatory użytkowników oraz hasła.

Uwaga: Maksymalna długość identyfikatora użytkownika wynosi 253 znaki, a maksymalna długość hasła 128 znaków.

Aby korzystać z lokalnej bazy danych użytkowników, w polu `Database Location`, należy wybrać opcję `Local` (Lokalna), tak jak przedstawiono poniżej:

```
       Konfiguruj serwer

Katalog RADIUS                                  /etc/radius
*Położenie bazy danych                [Local]
Nazwa pliku lokalnej bazy danych AVL             [dbdata.bin]
Rozliczanie lokalne                   [WŁ]

Poziom śledzenia błędów               [3]
.
.
.
```

LDAP
Serwer RADIUS może korzystać z LDAP w wersji 3 do przechowywania danych na temat zdalnych użytkowników.

W celu uzyskania zdalnego dostępu do danych o użytkownikach serwer RADIUS będzie korzystał z funkcji API protokołu LDAP w wersji 3. Dostęp za pośrednictwem LDAP w wersji 3 ma miejsce, jeśli pole **database_location** w pliku `/etc/radiusd.conf` ma wartość LDAP oraz skonfigurowana została nazwa serwera, identyfikator administratora LDAP oraz hasło administratora LDAP.

System AIX korzysta z bibliotek klienta LDAP w wersji 3, które są obsługiwane i znajdują się w pakiecie IBM Tivoli Directory Server. LDAP jest skalowalnym protokołem, a jego główną zaletą jest to, że dane o użytkownikach oraz wewnątrz-procesowe mogą być przechowywane w centralnym miejscu, co ułatwia administrowanie serwerem RADIUS. Do przeglądania dowolnych danych serwera RADIUS można używać programu narzędziowego wiersza komend **ldapsearch**.

Zanim protokół LDAP zostanie użyty z serwerem RADIUS, musi zostać skonfigurowany.

Serwer RADIUS udostępnia pliki `ldif` LDAP dodające do katalogu schemat serwera RADIUS, w tym klasy i atrybuty obiektów, ale konfigurację protokołu LDAP musi przeprowadzić użytkownik.

Do korzystania z obiektów LDAP serwera RADIUS tworzony jest osobny przyrostek. Ten przyrostek jest kontenerem o nazwie cn=aixradius i zawiera dwie klasy obiektów, tak jak opisano to w sekcji “Konfiguracja serwera LDAP RADIUS” na stronie 337. Użytkownik stosuje plik `ldif` dostarczany z serwerem RADIUS, który tworzy przyrostek oraz schemat serwera RADIUS.

Jeśli jako baza danych uwierzytelniania wykorzystywany jest katalog LDAP, dostępne są następujące opcje:

1. Przeglądanie i dostęp do bazy danych użytkowników może odbywać się ze wszystkich serwerów RADIUS.
2. Lista aktywnych użytkowników.
3. Opcja umożliwiająca określenie maksymalnej liczby logowań identyfikatora użytkownika.
4. Typ EAP, który może zostać skonfigurowany dla użytkownika.

5. Datę ważności hasła.

Aby korzystać z bazy danych LDAP, w polu **Położenie bazy danych** należy wybrać opcję LDAP, tak jak przedstawiono poniżej:

```
       Konfiguruj serwer

Katalog RADIUS                                  /etc/radius
*Położenie bazy danych                [LDAP]
Nazwa pliku lokalnej bazy danych AVL                [dbdata.bin]
Rozliczanie lokalne                   [WŁ]

Poziom śledzenia błędów               [3]
.
.
.
```

Informacje pokrewne

IBM Directory Server

Konfiguracja serwera LDAP RADIUS

Po skonfigurowaniu opcji uwierzytelniania użytkowników LDAP należy zaktualizować schemat serwera LDAP. Administrator systemu LDAP musi, przed zdefiniowaniem użytkowników LDAP RADIUS, dodać zdefiniowane atrybuty i klasy obiektów RADIUS systemu AIX oraz obiekty klas.

Do serwera LDAP trzeba dodać przyrostek. Przyrostek dla serwera RADIUS to `cn=aixradius`. Przyrostek jest nazwą wyróżniającą, która identyfikuje pierwszą pozycję w hierarchii katalogów.

Po dodaniu przyrostka katalog LDAP ma pusty kontener. *Kontener* jest pustą pozycją, która może zostać użyta do partycjonowania przestrzeni nazw. Kontener jest podobny do katalogu systemu plików, w którym mogą znajdować się pozycje katalogu. Następnie, za pomocą programu SMIT, do katalogu LDAP można dodać informacje o profilu użytkownika. Za pomocą programu SMIT na serwerze RADIUS można skonfigurować identyfikator i hasło administratora serwera LDAP, które przechowywane są w pliku `/etc/radius/radiusd.conf`.

Aby zorganizować informacje przechowywane w pozycjach katalogu LDAP, w schemacie definiuje się klasy obiektów. Klasa obiektu składa się z zestawu wymaganych i opcjonalnych atrybutów. Atrybuty mają postać par `typ=wartość`, w których typ jest definiowany przez unikalny identyfikator obiektu (OID) a wartość ma zdefiniowaną składnię. Każda pozycja w katalogu LDAP jest instancją obiektu.

Uwaga: Sama klasa obiektu nie definiuje drzewa informacji katalogu ani przestrzeni nazw. Ma to miejsce tylko podczas tworzenia pozycji, gdy specyficzne instancje klas obiektu otrzymują unikalne nazwy wyróżniające. Na przykład, gdy klasa obiektu kontenera otrzymuje unikalną nazwę wyróżniającą, może zostać powiązana z dwoma innymi pozycjami, które są instancjami jednostki organizacyjnej klasy obiektu. Wynikiem tego jest struktura drzewiasta lub przestrzeń nazw.

Klasy obiektu są specyficzne dla serwera RADIUS i pobierane są z pliku `ldif`. Niektóre atrybuty są istniejącymi atrybutami schematu LDAP, a niektóre są specyficzne dla serwera RADIUS. Nowe klasy obiektów RADIUS są strukturalne i abstrakcyjne.

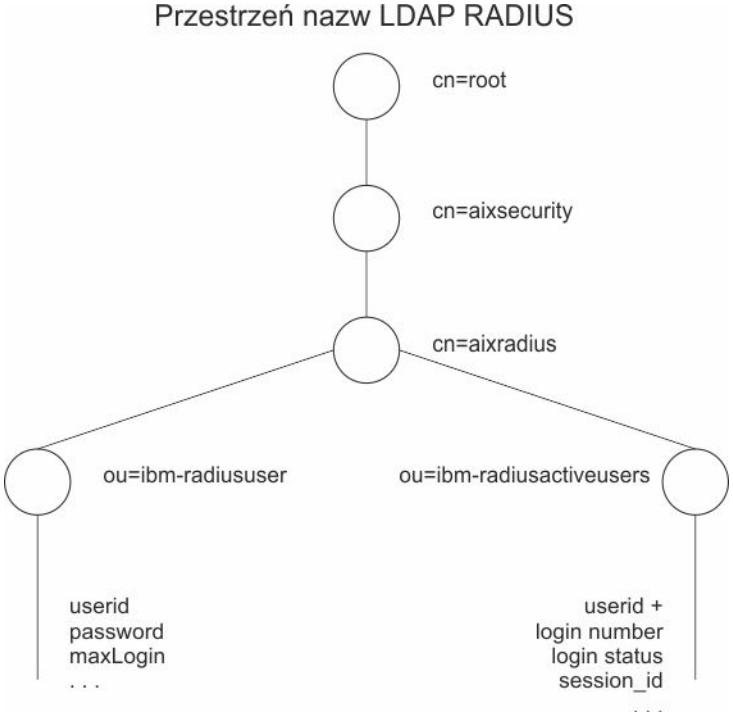
W celu zapewnienia bezpieczeństwa, połączenia z serwerem LDAP wywołują funkcję API SASL `ldap_bind_s`, która zawiera nazwę wyróżniającą, algorytm CRAM-MD5 jako metodę uwierzytelniania oraz hasło administratora serwera LDAP. Powoduje to przesłanie przez sieć streszczenia komunikatu, a nie samego hasła. Algorytm CRAM-MD5 jest mechanizmem bezpieczeństwa, dla którego po żadnej ze stron (klienta lub serwera) nie jest wymagana żadna specjalna konfiguracja.

Uwaga: Wszystkie atrybuty w klasach obiektów są pojedynczymi wartościami.

Przestrzeń nazw LDAP RADIUS

Na szczycie hierarchii przestrzeni nazw LDAP serwera RADIUS znajduje się kontener `cn=aixradius`. Poniżej kontenera `cn=aixradius` występują dwie jednostki organizacyjne (organizational unit - OU). Jednostki organizacyjne są kontenerami ułatwiającymi tworzenie unikalnych pozycji.

Przedstawiony poniżej rysunek pokazuje schemat LDAP RADIUS w postaci graficznej. Na tym rysunku kontenery oraz jednostki organizacyjne przedstawione są w postaci kółek połączonych liniami lub gałęziami. Kontener `aixradius`, znajdujący się w środku, rozgałęzia się na dwie jednostki organizacyjne: `ibm-radiususer` i `ibm-radiusactiveusers`. Poniżej kontenera `ibm-radiususer` występują w sposób niejawny kontenery: `userid`, `password` i `maxLogin`. Poniżej kontenera `ibmradiusactiveusers` występują w sposób niejawny kontenery: `userid +`, `login number`, `login status` i `session_id`. Powyżej kontenera `aixradius` znajduje się kontener `aixsecurity`, a dalej kontener `root`, będący na szczycie hierarchii.



Rysunek 16. Przestrzeń nazw LDAP RADIUS

Pliki schematu przestrzeni nazw LDAP
Pliki schematu LDAP definiują klasy obiektów i specyficzne dla serwera RADIUS atrybuty na potrzeby przestrzeni nazw LDAP.

W katalogu `/etc/radius/ldap` znajdują się następujące pliki schematu LDAP:

`IBM.V3.radiusbase.schema.ldif`

Ten plik definiuje klasę obiektów najwyższego poziomu dla serwera RADIUS (`cn=aixradius`). Plik ten tworzy także następujące gałęzie pod klasą obiektów `cn=aixradius`:

```
ou=ibm-radiususer
ou=ibm-radiusactiveusers
```

Wymagane informacje można dodać, korzystając z następującej komendy:

```
ldapadd -D ldap_admin_id -w password -i /etc/radius/ldap/IBM.V3.radiusbase.schema.ldif
```

Komendę tę można wykonać w systemie serwera LDAP lub zdalnie, korzystając z opcji **-h** (nazwa systemu hosta).

`IBM.V3.radius.schema.ldif`

Ten plik definiuje specyficzne dla serwera RADIUS atrybuty i klasy obiektów.

Nowe atrybuty RADIUS oraz klasy obiektów można dodać, wpisując następującą komendę:

```
ldapmodify -D ldap_admin_id -w password -i /etc/radius/ldap/IBM.V3.radius.schema.ldif
```

Za pomocą programu SMIT, jako lokalizację bazy danych należy podać LDAP, a także wprowadzić nazwę serwera LDAP oraz hasło administratora. Po wykonaniu tych czynności można za pomocą programu SMIT dodać do katalogu użytkowników LDAP RADIUS.

Klasa obiektu profilu użytkownika
Zanim serwer RADIUS będzie mógł uwierzytelnić użytkownika w systemie, muszą zostać wprowadzone profile użytkowników LDAP. Profile składają się z identyfikatora użytkownika oraz hasła.

Obiekt profilu użytkownika udostępnia dane dotyczące poszczególnych użytkowników, którzy mają dostęp od sieci, oraz zawiera informacje uwierzytelniające. Po wywołaniu przez demon funkcji API LDAP następuje synchroniczny dostęp do klasy obiektu **ibm-radiusUserInstance**. Unikalnym polem, które jest początkiem nazwy wyróżniającej, jest identyfikator użytkownika. Pole **MaxLoginCount** ogranicza liczbę logowań użytkownika LDAP.

Klasa obiektu listy aktywnego logowania
Lista aktywnego logowania LDAP reprezentuje dane, które zawierają informacje dotyczące aktualnie zalogowanych użytkowników.

Dla każdego użytkownika istnieje wiele rekordów, począwszy od rekordu początkowego `login_number = 1`, aż do `MaxLoginCount`. Identyfikator sesji pobierany jest z komunikatu RADIUS `start_accounting`. Częściowo kompletne rekordy tworzone są podczas tworzenia obiektu `ibm-radiusUserInstance`. Oznacza to, że przed otrzymaniem pakietów rozliczających RADIUS większość pól jest pusta. Po otrzymaniu komunikatu RADIUS `start_accounting` obiekt `ibm-radiusactiveusers` jest aktualizowany, tak aby wskazywał, że w danej chwili zalogowany jest użytkownik, a do odpowiedniego numeru logowania zapisywane są unikalne informacje o sesji. Po otrzymaniu komunikatu `stop_accounting` informacje listy aktywnego logowania są usuwane. Rekord aktywnego logowania jest aktualizowany w celu odzwierciedlenia faktu, że użytkownik wylogował się. Numer sesji w rozpoczynającym i kończącym komunikacie rozliczeniowym jest takim samym unikalnym numerem. W wywołaniach funkcji API LDAP następuje synchroniczny dostęp do klasy obiektu.

Protokół PAP (Password Authentication Protocol)
Protokół PAP zapewnia bezpieczeństwo poprzez kodowanie hasła użytkownika za pomocą algorytmu mieszającego MD5 o wartości, którą może skonstruować zarówno klient jak i serwer.

Działa to w następujący sposób:

1. W pakietach, które mają hasło użytkownika, pole Authentication (Uwierzytelnianie) zawiera 16-oktetową liczbę losową zwaną Request Authenticator (Element uwierzytelniający żądania).
2. Ta liczba oraz sekret współużytkowany klienta wstawiane są do algorytmu MD5. Wynikiem jest liczba 16-oktetowa.
3. Hasło użytkownika jest dopełniane pustymi znakami do długości 16 oktetów.
4. Dla liczby z kroku 2 i uzupełnionego hasła wykonywana jest operacja logiczna XOR (Exclusive-OR). W ten sposób powstają dane wysyłane w pakiecie jako atrybut *user_password*.
5. Serwer RADIUS oblicza taką samą liczbę, jak w kroku 2.
6. Dla tej liczby oraz danych pakietu z kroku 4 wykonywana jest operacja XOR, w wyniku której uzyskiwane jest hasło.

Protokół CHAP (Challenge Handshake Authentication Protocol)
Serwer RADIUS w celu zabezpieczenia hasła obsługuje także protokół **CHAP** PPP.

Podczas korzystania z protokołu CHAP, hasło użytkownika nie jest wysyłane przez sieć. Zamiast tego wysyłana jest liczba algorytmu mieszającego MD5, a serwer RADIUS odtwarza ją na podstawie informacji użytkownika, w tym przechowywanego hasła, a następnie porównuje ją z wartością przysłaną przez klienta.

Protokół EAP (Extensible Authentication Protocol)
Protokół EAP jest protokołem zaprojektowanym do obsługi wielu metod uwierzytelniania.

Protokół EAP określa strukturę komunikacji uwierzytelniającej między klientem a serwerem uwierzytelniającym bez definiowania treści danych uwierzytelniających. Ta treść jest definiowana przez określoną metodę EAP, która używana jest do uwierzytelniania. Najczęściej używane metody EAP to:

- MD5-challenge,
- hasło jednorazowe,
- ogólna karta tokenu,
- protokół TLS (Transport layer security).

Serwer RADIUS wykorzystuje zalety protokołu EAP przez określenie atrybutów RADIUS, które są używane do przesyłania danych EAP między serwerem RADIUS a jego klientami. Te dane EAP mogą być przesłane przez serwer RADIUS bezpośrednio do serwerów zaplecza, które implementują różne metody uwierzytelniania EAP.

Serwer RADIUS systemu AIX obsługuje jedynie metody EAP-TLS i MD5-challenge (wezwania MD5) protokołu EAP.

Metodę EAP używaną do uwierzytelniania użytkownika można skonfigurować na poziomie użytkownika, ustawiając wartości dla pozycji użytkownika w lokalnej bazie danych lub w katalogu LDAP.

Domyślnie protokół EAP jest wyłączony dla wszystkich użytkowników.

Autoryzacja
Serwer RADIUS przyznaje użytkownikom atrybuty autoryzacji, które zostały zdefiniowane w plikach strategii `default.auth` i `default.policy`.

Atrybuty autoryzacji są poprawnymi atrybutami protokołu RADIUS, które określono w standardzie RFC i zdefiniowano w pliku `/etc/radius/dictionary`. Autoryzacja jest opcjonalna i zależy od tego, w jaki sposób skonfigurowany jest sprzęt NAS lub punkt dostępu. Jeśli atrybuty autoryzacji są wymagane, trzeba je skonfigurować. Autoryzacja ma miejsce tylko po pomyślnym uwierzytelnieniu.

Strategie to konfigurowalne pary atrybut-wartość dla użytkownika, które mogą sterować dostępem użytkownika do sieci. Strategie można skonfigurować globalnie dla serwera RADIUS lub tylko dla danego użytkownika.

Dostarczane są dwa pliki konfiguracyjne autoryzacji: `/etc/radius/authorization/default.auth` i `default.policy`. Plik `default.policy` używany jest do porównywania przychodzących pakietów access request (żądanie dostępu). Ten plik zawiera pary atrybut-wartość, które początkowo są puste i muszą być skonfigurowane dla wymaganych ustawień. Po uwierzytelnieniu od wybranej strategii zależy, czy do klienta zostanie zwrócony pakiet access accept (dostęp przyznany), czy access reject (odmowa dostępu).

Każdy użytkownik może także mieć plik *identyfikator_użytkownika*`.policy`. Jeśli użytkownik ma unikalny plik strategii utworzony dla określonego identyfikatora użytkownika, wtedy najpierw sprawdzane są atrybuty z tego pliku. Jeśli pary atrybut-wartość z pliku *identyfikator_użytkownika*`.policy` nie są w pełni zgodne, wtedy sprawdzany jest plik `default.policy`. Jeśli pary atrybutu z pakietu access request (żądanie dostępu) nie są zgodne z żadnym plikiem, wtedy wysyłany jest pakiet access reject (odmowa dostępu). Jeśli zgodność z jednym z plików zostaje potwierdzona, do klienta wysyłany jest pakiet access accept (dostęp przyznany). Taki sposób faktycznie ustanawia dwa poziomy strategii.

Plik `default.auth` używany jest jako lista par atrybut-wartość w celu zwracania do klienta po sprawdzeniu strategii. Plik `default.auth` także zawiera pary atrybut-wartość, które początkowo są puste i muszą być skonfigurowane dla wymaganych ustawień. Aby skonfigurować wymagane ustawienia atrybutu autoryzacji, należy dokonać edycji pliku `default.auth` lub użyć programu SMIT. Każdy atrybut, który ma wartość, będzie automatycznie zwracany do serwera NAS w pakiecie access accept (dostęp przyznany).

Można także zdefiniować zwracane atrybuty autoryzacji specyficzne dla użytkownika, tworząc plik w oparciu o unikalną nazwę użytkownika z rozszerzeniem .auth, taki jak ***identyfikator_użytkownika***`.auth`.

Ten niestandardowy plik musi znajdować się w katalogu `/etc/radius/authorization`. W programie SMIT dostępny jest panel, który umożliwia tworzenie i edytowanie każdego pliku użytkownika.

Wszystkie atrybuty autoryzacji użytkownika są zwracane w pakiecie access-accept (dostęp przyznany) razem z wszystkimi domyślnymi atrybutami autoryzacji znalezionymi w pliku `default.auth` lub pliku `global.auth`.

Jeśli wartości z pliku `default.auth` i pliku *identyfikator_użytkownika*`.auth` są wspólne, wtedy wartości użytkownika nadpisują wartości domyślne. Uwzględnia to niektóre globalne atrybuty autoryzacji (usług lub zasobów) dla wszystkich użytkowników oraz bardziej szczegółowy poziom autoryzacji.

Uwaga: Do połączenia atrybutów autoryzacji z atrybutami autoryzacji specyficznymi dla użytkownika należy użyć pliku `global.auth` zamiast pliku `default.auth`, chyba że potrzebna jest inna kombinacja.

Począwszy od systemu AIX w wersji 6.1 z poziomem poprawek 6100-02, RADIUS obsługuje plik autoryzacji `global.auth`. Ten plik zastępuje i rozszerza oryginalne zastosowanie kombinacji atrybutów autoryzacji specyficznych dla użytkownika (takich jak zdefiniowane w plikach `user_id.auth`) z zestawem globalnych atrybutów autoryzacji.

Plik `user_id.auth`, w przeciwieństwie do pliku `default.auth`, nie jest nadpisywany przez podobne atrybuty znalezione w plikach autoryzacji specyficznych dla użytkownika, ale zamiast tego jest łączony z nimi, co zapewnia większą elastyczność w obsłudze autoryzacji dla użytkowników.

Jeśli atrybuty występują zarówno w pliku `default.auth`, jak i w pliku `user_id.auth`, wtedy wartości użytkownika przesłaniają wartości domyślne. To przesłonięcie wartości domyślnych umożliwia uwzględnienie niektórych domyślnych atrybutów autoryzacji (usług lub zasobów) dla wszystkich użytkowników oraz zapewnia bardziej szczegółowy poziom autoryzacji poszczególnych użytkowników.

Ta sama zasada ma zastosowanie dla atrybutów w pliku `global.auth`, przy czym nie są one nadpisywane przez atrybuty `user_id.auth`. W tym przypadku atrybuty w tych dwóch plikach są łączone. Jest to przydatne podczas określania atrybutów specyficznych dla dostawcy (vendor-specific attributes - VSA).

Proces autoryzacji odbywa się w następujący sposób:

1. Podczas uruchamiania demona do pamięci wczytywane są domyślna strategia i listy autoryzacji z plików `/etc/radius/authorization/default.policy`, `default.auth` i `default.auth`.
2. Uwierzytelnianie identyfikatora użytkownika i hasła.
3. Pakiet przychodzący sprawdzany jest pod kątem par atrybut-wartość.
   a. Odbywa się sprawdzanie niestandardowego pliku ***identyfikator_użytkownika*`.auth`**.
   b. Jeśli nie znaleziono zgodności, sprawdzany jest plik `default.policy`.
   c. Jeśli zgodność nie zostanie potwierdzona, wysyłany jest pakiet access reject (odmowa dostępu).
4. Stosowane są dostępne atrybuty uwierzytelniania użytkownika.
   a. Odczytywany jest plik `/etc/radius/authorization/`***user_id***`.auth` oraz plik `default.auth` i obie pozycje są porównywane.
   b. Używana jest pozycja z pliku użytkownika, która przysłania pozycję domyślną.
   c. Następuje połączenie wynikowych atrybutów z atrybutami znalezionymi w pliku `global.auth`.
5. Następuje zwrot atrybutów autoryzacji w pakiecie access accept (dostęp przyznany).

Rozliczanie
Serwer rozliczający RADIUS jest odpowiedzialny za odbieranie żądań rozliczenia od klienta i zwracanie do klienta odpowiedzi wskazujących, że pomyślnie odebrał żądanie i zapisał dane rozliczeniowe.

Rozliczanie lokalne można włączyć w pliku `radiusd.conf`.

Jeśli klient został skonfigurowany do korzystania z serwera rozliczającego RADIUS, podczas uruchamiania usługi będzie generował pakiet ACCOUNTING_START opisujący rodzaj dostarczanej usługi oraz użytkownika, do którego ma być ona dostarczana. Klient wysyła pakiet do serwera rozliczającego RADIUS, a ten zwraca potwierdzenie, że pakiet został odebrany. Podczas kończenia dostarczania usługi klient generuje pakiet ACCOUNTING_STOP opisujący rodzaj usługi oraz opcjonalne statystyki, takie jak czas,

który upłynął, oktety wejściowe i wyjściowe lub numery pakietu wejściowego i wyjściowego. Gdy serwer rozliczający RADIUS otrzymuje pakiet ACCOUNTING_STOP, zwraca do klienta rozliczającego potwierdzenie, że pakiet został odebrany.

Pakiet ACCOUNTING_REQUEST, czy to START, czy STOP, wprowadzany jest do serwera rozliczającego RADIUS za pośrednictwem sieci. Zaleca się, aby klient próbował wysyłać pakiet ACCOUNTING_REQUEST do momentu otrzymania potwierdzenia. Klient może także przekazywać żądania do alternatywnego serwera lub serwerów w momencie, gdy serwer podstawowy jest wyłączony lub nieosiągalny za pośrednictwem konfiguracji proxy. Więcej informacji na temat usług proxy zawiera sekcja “Usługi Proxy” na stronie 343.

Dane rozliczeniowe zapisywane są w standardowym formacie RADIUS w postaci par *atrybut=wartość* w lokalnym pliku `/etc/var/radius/data/accounting`. Zapisywane dane są danymi rozliczenia pochodzącymi z pakietu, ze znacznikiem czasowym. Jeśli serwer rozliczający RADIUS nie może pomyślnie zapisać pakietu rozliczenia, nie wyśle do klienta potwierdzenia `Accounting_Response`, a w pliku `syslog` zaprotokołowane zostaną informacje o błędzie.

Plik /var/radius/data/accounting

W pliku `/var/radius/data/accounting` przechwytywane są dane wysyłane przez klienta w pakietach ACCOUNTING START i ACCOUNTING STOP.

Po pierwszym zainstalowaniu plik `/var/radius/data/accounting` jest pusty. Dane zapisywane są w pliku w oparciu o wysyłane przez klienta pakiety ACCOUNTING START i ACCOUNTING STOP.

Poniżej pokazano przykład typu danych, które serwer RADIUS systemu AIX zapisuje w pliku `/var/radius/data/accounting`. Informacje mogą różnić się w zależności od konfiguracji systemu.

Uwaga:

- Należy się upewnić, że system plików `/var` jest wystarczająco duży, aby obsłużyć wszystkie dane rozliczenia.
- Do analizowania danych w tym pliku można użyć skryptów Perl innych firm. Przykłady skryptów generujących raporty na podstawie danych rozliczeniowych można znaleźć w serwisie WWW http://www.pgregg.com/projects/radiusreport.
- Pakiety rozliczenia mogą być także przesyłane z wykorzystaniem serwerów proxy.

```
Thu May 27 14:43:19 2004
    NAS-IP-Address = 10.10.10.1
    NAS-Port = 1
    NAS-Port-Type = Async
    User-Name = "rod"
    Acct-Status-Type = Start
    Acct-Authentic = RADIUS
    Service-Type = Framed-User
    Acct-Session-Id = "0000000C"
    Framed-Protocol = PPP
    Acct-Delay-Time = 0
    Timestamp = 1085686999

Thu May 27 14:45:19 2004
    NAS-IP-Address = 10.10.10.1
    NAS-Port = 1    <-- rod był fizycznie podłączony do portu #1 sprzętu
    NAS-Port-Type = Async
    User-Name = "rod"
    Acct-Status-Type = Stop
    Acct-Authentic = RADIUS
    Service-Type = Framed-User
    Acct-Session-Id = "0000000C"   <-- należy zauważyć, że identyfikator sesji jest taki sam,
                                   <-- tak więc start i zatrzymanie są zgodne
    Framed-Protocol = PPP
    Framed-IP-Address = 10.10.10.2   <-- adres IP użytkownika rod
    Acct-Terminate-Cause = User-Request  <-- użytkownik anulował sesję
    Acct-Input-Octets = 4016
    Acct-Output-Octets = 142
    Acct-Input-Packets = 35
    Acct-Output-Packets = 7
    Acct-Session-Time = 120  <-- sekundy
    Acct-Delay-Time = 0
```

```
    Timestamp = 1085687119  <--- należy zauważyć, że użytkownik "rod" był zalogowany
                         <--- tylko przez 120 sekund (2 minuty)
```

Usługi Proxy
Usługi proxy umożliwiają serwerowi RADIUS przekazywanie żądań z serwera NAS do innego serwera RADIUS, a następnie zwracanie komunikatów odpowiedzi do serwera NAS. Usługi proxy oparte są o nazwy dziedziny.

Serwer RADIUS może działać jednocześnie jako serwer proxy oraz serwer zaplecza. Ten mechanizm można zastosować zarówno dla pakietów rozliczania, jak i pakietów uwierzytelniania. Domyślnie usługa proxy jest wyłączona w pliku `radiusd.conf`.

Dziedziny
Dziedziny są identyfikatorami, które są umieszczane przed lub po wartościach podanych w atrybucie User-Name (Nazwa użytkownika) i których serwer RADIUS może użyć do identyfikowania serwera w celu rozpoczęcia procesu uwierzytelniania i rozliczania.

Poniższy przykład ilustruje użycie dziedzin z serwerem RADIUS:

Użytkownik *Jan* jest pracownikiem firmy *XYZ* z Sacramento. Dziedziną dla tego obszaru jest *SAC*. Jednak *Jan* aktualnie przebywa w Nowym Jorku na delegacji. Dziedziną dla Nowego Jorku jest *NYC*. Gdy *Jan* łączy się z dziedziną *NYC*, przekazywana jest nazwa użytkownika *SAC/Jan*. Informuje to serwer RADIUS dziedziny *NYC*, że ten pakiet należy przekazać do serwera, który przeprowadza uwierzytelnianie i rozliczanie użytkowników dziedziny *SAC*.

Atrybut user-name dziedziny
Pakiety uwierzytelniające i rozliczeniowe są kierowane przez dziedzinę w oparciu o atrybut **User-Name** (nazwa użytkownika). Atrybut ten określa porządek dziedzin, przez które przechodzi pakiet kierowany do serwera końcowego, przeprowadzającego uwierzytelnianie lub rozliczanie.

Pakiety są kierowane w oparciu o łańcuch dziedzin określony dla atrybutu **User-Name**. Rzeczywiste dziedziny wstawiane do atrybutu **User-Name**, który ostatecznie określa ścieżkę pakietu, zależą od decyzji administratora określającego układ serwerów RADIUS. Nazwy dziedzin można umieścić przed atrybutem **User-Name**, a także za nim. Najpopularniejszymi znakami do określania różnych dziedzin są ukośnik (/) do oddzielania przedrostków z przodu atrybutu **User-Name** i znak ampersand (&) do oddzielania przyrostków za atrybutem User-Name. Znaki oddzielające konfiguruje się w pliku `radiusd.conf` . Atrybut **User-Name** jest analizowany od lewej do prawej strony.

Przykład atrybutu **User-Name** (Nazwa użytkownika) wykorzystujący tylko metodę przedrostków wygląda następująco:

```
 USA/TEXAS/AUSTIN/jan
```

Przykład atrybutu **User-Name** (Nazwa użytkownika) wykorzystujący tylko metodę przyrostków wygląda następująco:

```
jan@USA@TEXAS@AUSTIN
```

Możliwe jest wykorzystywanie obu metod. Należy pamiętać, że po określeniu dziedzin pakiet będzie kierowany w kolejności analizowania od lewej do prawej, a wszystkie dziedziny będące przedrostkami zostaną przetworzone przed dziedzinami będącymi przyrostkami. Użytkownik musi zostać uwierzytelniony, a dane rozliczenia zapisane w pojedynczym węźle.

Przedstawiony poniżej przykład, korzystający z obu metod, daje taki sam wynik, jak poprzednie przykłady:

```
USA/jan@TEXAS@AUSTIN
```

Konfigurowanie usług proxy
Informacje konfiguracyjne serwera proxy RADIUS znajdują się w pliku `proxy` w katalogu `/etc/radius`.

Początkowy plik `proxy` zawiera pozycje przykładowe. W pliku proxy znajdują się trzy pola: **Realm Name** (Nazwa dziedziny), **Next Hop IP address** (Następny adres IP przeskoku) i **Shared Secret** (Sekret współużytkowany).

Aby skonfigurować reguły proxy, wybierz jedną z następujących opcji:

```
      Konfiguruj reguły proxy

Wyświetl wszystkie reguły
Dodaj proxy
Zmień / pokaż charakterystykę proxy
Usuń proxy
```

Opcja **Wyświetl wszystkie reguły** powoduje odczytanie pliku `/etc/radius/proxy` i wyświetlenie trzech pól w formacie kolumnowym. Poniżej przedstawiono nagłówki kolumn:

```
realm_name   next_hop_address  shared_secret
```

Opcja **Dodaj proxy** powoduje wyświetlenie poniższego ekranu. Z panelu odczytywane są informacje, które jako dane dodawane są na końcu pliku `/etc/radius/proxy`.

W każdym przeskoku w łańcuchu proxy używane są dane szyfrujące współużytkowane między dwoma serwerami RADIUS. Współużytkowane dane szyfrujące znajdują się w pliku `/etc/radius/proxy_file`. Dane te powinny być unikalne dla każdego przeskoku proxy w łańcuchu.

Więcej informacji na temat tworzenia współużytkowanych danych szyfrujących zawiera sekcja “Plik /etc/radius/clients” na stronie 333.

Aby dodać proxy, wybierz wartości następujących pól:

```
            Dodaj proxy
*Nazwa dziedziny                          []  (maks. 64 znaki)
*Adres IP następnego przeskoku (postać dziesiętna z kropkami)[xx.xx.xx.xx]
*Współużytkowane dane szyfrujące          []  (minimum 6, maksimum 256 znaków)
```

Wybranie opcji **Change/Show** (Pokaż/zmień) wyświetla listę nazw dziedzin. Lista wyświetlana jest na wywoływanym ekranie, na którym należy wybrać nazwę dziedziny.

Opcja **Remove a Proxy** (Usuń proxy) powoduje wyświetlenie nazw dziedzin. Lista wyświetlana jest na wywoływanym ekranie, na którym należy wybrać nazwę dziedziny. Po wybraniu nazwy, przed usunięciem dziedziny, wyświetlany jest ekran potwierdzający.

Poniżej przedstawiona została przykładowa sekcja informacyjna konfiguracji serwera proxy pliku `radiusd.conf`:

```
#--------------------------------------------------------------------#
#       Informacje serwera PROXY RADIUS                              #
#                                                                    #
#                                                                    #
#   Proxy_Allow               :  ON lub OFF. Jeśli ma wartość ON,  #
#                                serwer może                         #
#                                przekazywać pakiety do dziedzin,  #
#                                które zna, i skonfigurowane muszą #
#                                być następujące pola.             #
#   Proxy_Use_Table           :  ON lub OFF. Jeśli ma wartość ON,  #
#                                serwer może                         #
#                                korzystać z tabeli do szybszego   #
#                                przetwarzania powtórzonych żądań. #
#                                Może być używane bez proxy        #
#                                równego ON, ale wymagane jest,    #
#                                aby miało wartość ON, jeśli       #
#                                Proxy_Use_Table jest równe ON.    #
#   Proxy_Realm_name          :  To pole określa dziedzinę, którą  #
#                                ten serwer obsługuje.             #
#   Proxy_Prefix_delim        :  Lista separatorów do analizowania #
#                                nazw dziedzin dodawanych jako     #
#                                przyr. do nazw użytk. Ta lista    #
#                                musi być obustronnie wyłączna dla #
```

```
#                                  separatorów przedrostków.          #
#   Proxy_Suffix_delim         :  Lista separatorów do analizowania #
#                                 nazw dziedzin dodawanych jako      #
#                                 przyr. do nazw użytk. Ta lista     #
#                                 musi być obustronnie wyłączna dla #
#                                 separatorów przedrostków.          #
#   Proxy_Remove_Hops          :  YES lub NO. Jeśli YES wtedy proxy #
#                                 usunie nazwę dziedziny, nazwy      #
#                                 dziedzin poprzednich przeskoków    #
#                                 i nazwę dziedziny następnego       #
#                                 serwera, do którego przekazywany   #
#                                 jest pakiet.                       #
#                                                                    #
#   Proxy_Retry_count          :  Liczba prób wysyłania pakietu      #
#                                 żądania.                           #
#                                                                    #
#   Proxy_Time_Out             :  Liczba sekund do odczekania        #
#                                 między próbami.                    #
#                                                                    #
#--------------------------------------------------------------------#
Proxy_Allow               :   OFF
Proxy_Use_Table           :   OFF
Proxy_Realm_name          :
Proxy_Prefix_delim        :   $/
Proxy_Suffix_delim        :   @.
Proxy_Remove_Hops         :   NO
Proxy_Retry_count         :   2
Proxy_Time_Out            :   3
```

Konfigurowanie serwera RADIUS

Demon serwera RADIUS korzysta z kilku plików konfiguracyjnych. Informacje o konfiguracji serwera przechowywane są w pliku `/etc/radius/radiusd.conf`. Dostarczany plik konfiguracyjny serwera zawiera wartości domyślne.

Uwaga: Poniżej przedstawiono przykładowy panel programu SMIT do konfigurowania serwera RADIUS:

```
       Konfiguruj serwer

Katalog RADIUS                                  /etc/radius
*Położenie bazy danych                           [UNIX]
Nazwa pliku lokalnej bazy danych AVL             [dbdata.bin]
Rozliczanie lokalne                  [WŁ]
Local Accounting Directory                       []

Poziom śledzenia błędów              [3]
Komunikat odpowiedzi akceptującej                []
Komunikat odpowiedzi odrzucającej                []
Komunikat odpowiedzi wyzwania                    []
Komunikat odpowiedzi o wygaśnięciu hasła         []
Obsługa odnawiania wygasłego hasła               [NIE]
Wymagaj hosta uwierzytelniającego komunikaty     [NIE]

*Numer portu uwierzytelniania                    [1812]
*Numer portu rozliczania                         [1813]

Nazwa serwera LDAP                               []
Numer portu serwera LDAP                         []
Nazwa wyróżniająca administratora serwera LDAP   []
Hasło administratora serwera LDAP                []
Bazowa nazwa wyróżniająca LDAP                   [cn=aixradius]
Limit wielkości LDAP                             [0]
Limit liczby przeskoków LDAP                     [0]
Limit czasu oczekiwania LDAP                     [10]
Poziom śledzenia błędów LDAP                     [ 0]

Proxy dozwolony                                  [WYŁ]
Tabela użycia proxy                              [WYŁ]
Nazwa dziedziny proxy                            []
Ograniczniki przedrostków proxy                  [$/]
Ograniczniki przyrostków proxy                   [@.]
                  UWAGA: przedrostek i przyrostek wzajemnie się wykluczają
Proxy usuwa nazwy dziedzin                       [NIE]
Liczba ponownych prób proxy                      [2]
Limit czasu proxy                                [30]
UNIX Check Login Restrictions                    [WYŁ]
Enable IP Pool                                   [WŁ]
Authentication Method Sequence     [TLS, MD5]
OpenSSL Configuration File         []
```

Narzędzia protokołujące

Do protokołowania aktywności oraz informacji o błędach serwer RADIUS korzysta z narzędzia SYSLOG.

Dostępne są trzy poziomy protokołowania informacji:

0
Protokołowane są tylko problemy i błędy oraz uruchomienia demonów.

3
Protokołowany jest zapis kontrolny komunikatów `access_accept`, `access_reject*`, `discard` i `error`.

Uwaga: Komunikaty `discard` protokołowane są w momencie, gdy przychodzący pakiet jest niepoprawny, a pakiet odpowiedzi nie został wygenerowany.

9
Obejmuje protokołowanie informacji z poziomu 0 i 3 oraz dużo więcej. Protokołowanie na poziomie 9 należy uruchamiać tylko w celu debugowania.

Domyślnym poziomem protokołowania jest poziom 3. Protokołowanie na poziomie 3 używane jest do poprawienia poziomu kontroli serwera RADIUS. W zależności od poziomu protokołowania na serwerze, można skorzystać z zapisanych informacji o aktywności przechowywanych w protokole, aby sprawdzić podejrzane wzorce aktywności. Jeśli zostaną naruszone zasady bezpieczeństwa, dane wyjściowe SYSLOG mogą zostać użyte do określenia, w jaki sposób i kiedy wystąpiło naruszenie oraz jaki był prawdopodobnie zakres uzyskanego dostępu. Te informacje są przydatne przy projektowaniu lepszych zabezpieczeń w celu zapobiegania występowaniu podobnych problemów w przyszłości.

Informacje pokrewne

IBM Directory Server

Konfigurowanie serwera RADIUS do użycia demona syslogd
Aby można było używać narzędzia SYSLOG do wyświetlania informacji o aktywności i błędach, należy włączyć demon syslogd.

Aby włączyć demon syslogd:

1. Zmodyfikuj plik `/etc/syslog.conf`, dodając następującą pozycję:`local4.debug var/adm/ipsec.log`.

   Użyj narzędzia *local4*, aby zapisywać zdarzenia dotyczące ruchu danych i bezpieczeństwa IP. Stosowane są standardowe poziomy priorytetu systemu operacyjnego. Poziom priorytetu powinien być ustawiony na *debug*, dopóki ruch danych przez tunele bezpieczeństwa IP i filtry nie będzie stabilny i poprawny.

   Uwaga: Protokołowanie zdarzeń filtrowania może spowodować znaczącą aktywność hosta bezpieczeństwa IP i zająć dużą ilość pamięci.
2. Zapisz plik `/etc/syslog.conf`.
3. Przejdź do katalogu określonego dla pliku protokołu i utwórz pusty plik o tej samej nazwie. W sytuacji przedstawionej powyżej można przejść do katalogu `/var/adm` i wykonać następującą komendę **touch**:

   ```
   touch ipsec.log
   ```
4. Wykonaj komendę **refresh** dla podsystemu `syslogd`:

   ```
   refresh -s syslogd
   ```

Konfigurowanie ustawień wyjściowych narzędzia SYSLOG
Parametr Debug_Level, znajdujący się w pliku `radiusd.conf`, może przyjmować wartości: 0, 3 lub 9 zależnie od ilości informacji diagnostycznych, które mają być zawarte w danych wyjściowych narzędzia SYSLOG.

Wartość domyślna wynosi 3. Sekcji debugowania pliku `radiusd.conf` wygląda w sposób podobny do poniższego:

```
#.
#.
#.
#   Debug_Level      :  Ta para ustawia poziom debugowania, na     #
#                       którym będzie działał serwer RADIUS.       #
#                       Poprawne wartości to 0,3 lub 9. Domyślną   #
#                       wartością jest 3. Wynik jest kierowany do  #
#                       lokalizacji podanej w sekcji *.debug       #
#                       pliku /etc/syslog.conf                     #
#                                                                  #
#                       Każdy poziom zwiększa liczbę komunikatów   #
#                       wysyłanych do syslog. Na przykład "9" to   #
#                       nowe komunikaty udostępniane przez "9" i   #
#                       wszystkie generowane przez poziomy 0 i 3.  #
#                                                                  #
#                       0 : zapewnia minimalne dane dla protokołu  #
#                           syslogd. Wysyła komunikaty o           #
#                           uruchomieniu i zakończeniu każdego     #
#                           procesu RADIUS. Protokołuje także      #
#                           warunki błędów.                        #
#                                                                  #
#                       3 : obejmuje ogólne komunikaty ACCESS      #
#                           ACCEPT, REJECT i DISCARD dla każdego   #
#                           pakietu. Zapewnia ogólną kontrolę      #
#                           śledzenia dla uwierzytelniania.        #
#                                                                  #
#                       9 : maksymalna ilość danych. Specyficzne   #
#                           wartości atrybutów dla przekazywanej   #
#                           przez przetwarzanie transakcji oraz    #
#                           o wiele więcej.                        #
#                          [NIE zalecany przy normalnym działaniu] #
#                                                                  #
#------------------------------------------------------------------#
```

Poniższe przykłady ilustrują przykładowe dane wyjściowe dla różnych poziomów debugowania.

Pakiet rozliczający na poziomie debugowania 3

```
Aug 18 10:23:57 server1 syslog: [0]:Monitor process [389288] has started
Aug 18 10:23:57 server1 radiusd[389288]: [0]:Local database (AVL) built.
Aug 18 10:23:57 server1 radiusd[389288]: [0]:Authentication process started : Pid= 549082 Port = 1812
Aug 18 10:23:57 server1 radiusd[389288]: [0]:Accounting process started : Pid= 643188 Port = 1813
Aug 18 10:23:57 server1 radiusd[643188]: [0]:Socket created [15]
Aug 18 10:23:57 server1 radiusd[643188]: [0]:Bound Accounting socket [15]
Aug 18 10:23:57 server1 radiusd[549082]: [0]:Socket created [15]
Aug 18 10:23:57 server1 radiusd[549082]: [0]:Bound Authentication socket [15]
Aug 18 10:24:07 server1 radiusd[643188]: [1]:*** Start Process_Packet() ***
Aug 18 10:24:07 server1 radiusd[643188]: [1]:Code 4, ID = 96, Port = 41639 Host = 10.10.10.10
Aug 18 10:24:07 server1 radiusd[643188]: [1]:ACCOUNTING-START - sending Accounting Ack to User [ user_id1 ]
Aug 18 10:24:07 server1 radiusd[643188]: [1]:Sending Accounting Ack of id 96 to 10.10.10.10 (client1.ibm.com)
Aug 18 10:24:07 server1 radiusd[643188]: [1]:send_acct_reply() Outgoing Packet:
Aug 18 10:24:07 server1 radiusd[643188]: [1]: Code = 5, Id = 96, Length = 20
Aug 18 10:24:07 server1 radiusd[643188]: [1]:*** Leave Process_Packet() ***
Aug 18 10:24:13 server1 radiusd[643188]: [2]:*** Start Process_Packet() ***
Aug 18 10:24:13 server1 radiusd[643188]: [2]:Code 4, ID = 97, Port = 41639 Host = 10.10.10.10
Aug 18 10:24:13 server1 radiusd[643188]: [2]:ACCOUNTING-STOP - sending Accounting Ack to User [ user_id1 ]
Aug 18 10:24:14 server1 radiusd[643188]: [2]:Sending Accounting Ack of id 97 to 10.10.10.10 (client1.ibm.com)
Aug 18 10:24:14 server1 radiusd[643188]: [2]:send_acct_reply() Outgoing Packet:
Aug 18 10:24:14 server1 radiusd[643188]: [2]: Code = 5, Id = 97, Length = 20
Aug 18 10:24:14 server1 radiusd[643188]: [2]:*** Leave Process_Packet() **
```

Pakiety rozliczające na poziomie 9

```
Aug 18 10:21:18 server1 syslog: [0]:Monitor process [643170] has started
Aug 18 10:21:18 server1 radiusd[643170]: [0]:Local database (AVL) built.
Aug 18 10:21:18 server1 radiusd[643170]: [0]:Authentication process started : Pid= 389284 Port = 1812
Aug 18 10:21:18 server1 radiusd[643170]: [0]:Accounting process started : Pid= 549078 Port = 1813
Aug 18 10:22:03 server1 radiusd[643170]: [0]:PID = [389284] dead
Aug 18 10:22:03 server1 radiusd[643170]: [0]:PID = [549078] dead
Aug 18 10:22:03 server1 radiusd[643170]: [0]:All child processes stopped. radiusd parent stopping
Aug 18 10:22:09 server1 syslog: [0]:Monitor process [1081472] has started
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Local database (AVL) built.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Inside client_init()
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Number of client entries read: 1
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Inside read_authorize_policy routine for file:
  /etc/radius/authorization/default.policy.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Inside read_authorize_file routine for file:
  /etc/radius/authorization/default.policy.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:read_authorize_file() routine complete.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Inside read_authorize_file routine for file:
  /etc/radius/authorization/default.auth.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:read_authorize_file() routine complete.
Aug 18 10:22:09 server1 radiusd[549080]: [0]:connect_to_LDAP_server:Database Location (where the data
  resides)=LDAP.
Aug 18 10:22:09 server1 radiusd[549080]: [0]:connect_to_LDAP_server:LDAP Server name= server1.austin.ibm.com.
Aug 18 10:22:09 server1 radiusd[549080]: [0]:connect_to_LDAP_server:LDAP Server port= 389.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Authentication process started : Pid= 549080 Port = 1812
Aug 18 10:22:09 server1 radiusd[389286]: [0]:connect_to_LDAP_server:Database Location (where the data
 resides)=LDAP.
Aug 18 10:22:09 server1 radiusd[389286]: [0]:connect_to_LDAP_server:LDAP Server name= server1.austin.ibm.com.
Aug 18 10:22:09 server1 radiusd[389286]: [0]:connect_to_LDAP_server:LDAP Server port= 389.
Aug 18 10:22:09 server1 radiusd[1081472]: [0]:Accounting process started : Pid= 389286 Port = 1813
Aug 18 10:22:10 server1 radiusd[549080]: [0]:Socket created [15]
Aug 18 10:22:10 server1 radiusd[549080]: [0]:Bound Authentication socket [15]
Aug 18 10:22:10 server1 radiusd[389286]: [0]:Socket created [15]
Aug 18 10:22:10 server1 radiusd[389286]: [0]:Bound Accounting socket [15]
Aug 18 10:22:15 server1 radiusd[389286]: [1]:*** Start Process_Packet() ***
Aug 18 10:22:15 server1 radiusd[389286]: [1]:Incoming Packet:
Aug 18 10:22:15 server1 radiusd[389286]: [1]:  Code = 4, Id = 94, Length = 80
Aug 18 10:22:15 server1 radiusd[389286]: [1]:  Authenticator = 0xC5DBDDFE6EFFFDBD6AE64CA35947DD0F
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =  40, Length =   6, Value = 0x00000001
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =   1, Length =   8, Value = 0x67656E747931
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =   4, Length =   6, Value = 0x00000000
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =   8, Length =   6, Value = 0x0A0A0A01
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =  44, Length =   8, Value = 0x303030303062
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =  30, Length =  10, Value = 0x3132332D34353638
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =  31, Length =  10, Value = 0x3435362D31323335
Aug 18 10:22:15 server1 radiusd[389286]: [1]:    Type =  85, Length =   6, Value = 0x00000259
Aug 18 10:22:15 server1 radiusd[389286]: [1]:Starting parse_packet()
Aug 18 10:22:15 server1 radiusd[389286]: [1]:Code 4, ID = 94, Port = 41639 Host = 10.10.10.10
Aug 18 10:22:15 server1 radiusd[389286]: [1]:Acct-Status-Type = Sta
```

Pakiet uwierzytelniający na poziomie 0

```
Aug 18 10:06:11 server1 syslog: [0]:Monitor process [1081460] has started
Aug 18 10:06:11 server1 radiusd[1081460]: [0]:Local database (AVL) built.
Aug 18 10:06:11 server1 radiusd[1081460]: [0]:Authentication process started : Pid= 549076 Port = 1812
Aug 18 10:06:11 server1 radiusd[1081460]: [0]:Accounting process started : Pid= 389282 Port = 18
```

Pakiet uwierzytelniający na poziomie 3

```
Aug 18 10:01:32 server2 radiusd[389276]: [3]:*** Start Process_Packet() ***
Aug 18 10:01:32 server2 radiusd[389276]: [3]:Code 1, ID = 72, Port = 41638 Host = 10.10.10.10
Aug 18 10:01:32 server2 radiusd[389276]: [3]:authenticate_password_PAP: Passwords do not match, user is
rejected
Aug 18 10:01:32 server2 radiusd[389276]: [3]:Authentication failed for user [user_id1] using IP [10.10.10.10]
Aug 18 10:01:32 server2 radiusd[389276]: [3]:ACCESS-REJECT - sending reject for id 72 to 10.10.10.10
  (client1.ibm.com)
Aug 18 10:01:32 server2 radiusd[389276]: [3]:send_reject() Outgoing Packet:
Aug 18 10:01:32 server2 radiusd[389276]: [3]: Code = 3, Id = 72, Length = 30
Aug 18 10:01:32 server2 radiusd[389276]: [3]:*** Leave Process_Packet() ***
Aug 18 10:01:53 server2 radiusd[389276]: [4]:*** Start Process_Packet() ***
Aug 18 10:01:53 server2 radiusd[389276]: [4]:Code 1, ID = 74, Port = 41638 Host = 10.10.10.10
Aug 18 10:01:53 server2 radiusd[389276]: [4]:authenticate_password_PAP: Passwords Match, user is authenticated
Aug 18 10:01:53 server2 radiusd[389276]: [4]:Authentication successful for user [user_id1] using IP
[10.10.10.10]
Aug 18 10:01:53 server2 radiusd[389276]: [4]:Authorization successful for user [user_id1] using IP
[10.10.10.10]
Aug 18 10:01:53 server2 radiusd[389276]: [4]:ACCESS-ACCEPT - sending accept for id 74 to 10.10.10.10
  (client1.ibm.com)
Aug 18 10:01:53 server2 radiusd[389276]: [4]:send_accept() Outgoing Packet:
Aug 18 10:01:53 server2 radiusd[389276]: [4]: Code = 2, Id = 74, Length = 31
Aug 18 10:01:53 server2 radiusd[389276]: [4]:*** Leave Process_Packet() **
```

Pakiet uwierzytelniający na poziomie 9

```
Aug 18 10:03:56 server1 radiusd[389278]: [1]:*** Start Process_Packet() ***
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Incoming Packet:
Aug 18 10:03:56 server1 radiusd[389278]: [1]:  Code = 1, Id = 77, Length = 58
Aug 18 10:03:56 server1 radiusd[389278]: [1]:  Authenticator = 0xE6CB0F9C22BB4E799854E734104FB2D5
Aug 18 10:03:56 server1 radiusd[389278]: [1]:    Type =   1, Length =   8, Value = 0x67656E747931
Aug 18 10:03:56 server1 radiusd[389278]: [1]:    Type =   4, Length =   6, Value = 0x00000000
Aug 18 10:03:56 server1 radiusd[389278]: [1]:    Type =   2, Length =  18, Value = 0x**********
**********************
Aug 18 10:03:56 server1 radiusd[389278]: [1]:    Type =   7, Length =   6, Value = 0x00000001
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Starting parse_packet()
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Code 1, ID = 77, Port = 41638 Host = 10.10.10.10
Aug 18 10:03:56 server1 radiusd[389278]: [1]:User-Name = "user_id1"
Aug 18 10:03:56 server1 radiusd[389278]: [1]:NAS-IP-Address = 10.10.10.10
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Framed-Protocol = PPP
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Leaving parse_packet()
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Verifying Message-Authenticator
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Message-Authenticator successfully verified
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside proxy_request_needed() function
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Proxy is not turned on
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Username = [user_id1]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Client IP = [10.10.10.10]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside parse_for_login( user_id1 )
Aug 18 10:03:56 server1 radiusd[389278]: [1]:User_id remaining after prefix removal = [user_id1]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:User_id remaining after suffix removal = [user_id1]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside rad_authenticate() function
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Authentication request received for [client1.austin.ibm.com]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Calling get_ldap_user() to get LDAP user data
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_user:LDAP user id: user_id1.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_user:LDAP max_login_cnt:2.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_user:LDAP EAP_type: 4.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_user:LDAP passwordexpiredweeks: 9.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_active_sessions:number of free entries= 2.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:get_ldap_active_session:dn retrieved=
radiusuniqueidentifier=user_id11,ou=radiusActiveUsers,cn=aixradius.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside get_client_secret routine for ip:10.10.10.10
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Found NAS-IP = [10.10.10.10]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Found shared secret.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:authenticate_password_PAP: Passwords Match, user is authenticated
Aug 18 10:03:56 server1 radiusd[389278]: [1]:is_ldap_pw:password for user has NOT expired
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Authentication successful for user [user_id1] using IP
[10.10.10.10]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside rad_authorize() routine.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside read_authorize_policy routine for file:
  /etc/radius/authorization/user_id1.policy.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside read_authorize_file routine for file:
  /etc/radius/authorization/user_id1.policy.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Did not open /etc/radius/authorization/user_id1.policy file.
  File may not be found.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Error reading policy file: /etc/radius/authorization/
user_id1.policy.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:rad_authorize:default policy list and userpolicy list were empty.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:In create_def_copy() routine.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Successfully made a copy of the master authorization list.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside read_authorize_file routine for file:
  /etc/radius/authorization/user_id1.auth.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Did not open /etc/radius/authorization/user_id1.auth file.
  File may not be found.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:rad_authorize:copy authorization list and user list were empty.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Authorization successful for user [user_id1] using IP
[10.10.10.10]
```

```
Aug 18 10:03:56 server1 radiusd[389278]: [1]:ACCESS-ACCEPT - sending accept for id 77 to 10.10.10.10
  (client1.austin.ibm.com)
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside proxy_response_needed() function
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Proxy is not turned on
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Inside get_client_secret routine for ip:10.10.10.10
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Found NAS-IP = [10.10.10.10]
Aug 18 10:03:56 server1 radiusd[389278]: [1]:Found shared secret.
Aug 18 10:03:56 server1 radiusd[389278]: [1]:send_accept() Outgoing Packet:
Aug 18 10:03:56 server1 radiusd[389278]: [1]:  Code = 2, Id = 77, Length = 31
Aug 18 10:03:56 server1 radiusd[389278]: [1]:send_accept() Outgoing Packet:
Aug 18 10:03:56 server1 radiusd[389278]: [1]:  Code = 2, Id = 77, Length = 31
Aug 18 10:03:56 server1 radiusd[389278]: [1]:  Authenticator = 0xCCB2B645BBEE86F5E4FC5BE24E904B2A
Aug 18 10:03:56 server1 radiusd[389278]: [1]:    Type =  18, Length =  11, Value = 0x476F6F646E65737321
Aug 18 10:03:56 server1 radiusd[389278]: [1]:*** Leave Process_Packet() ***
Aug 18 10:04:18 server1 radiusd[389278]: [2]:*** Start Process_Packet() ***
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Incoming Packet:
Aug 18 10:04:18 server1 radiusd[389278]: [2]:  Code = 1, Id = 79, Length = 58
Aug 18 10:04:18 server1 radiusd[389278]: [2]:  Authenticator = 0x774298A2B6DD90D7C33B3C10C4787D41
Aug 18 10:04:18 server1 radiusd[389278]: [2]:    Type =   1, Length =   8, Value = 0x67656E747931
Aug 18 10:04:18 server1 radiusd[389278]: [2]:    Type =   4, Length =   6, Value = 0x00000000
Aug 18 10:04:18 server1 radiusd[389278]: [2]:    Type =   2, Length =  18, Value = 0x*******
************************
Aug 18 10:04:18 server1 radiusd[389278]: [2]:    Type =   7, Length =   6, Value = 0x00000001
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Starting parse_packet()
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Code 1, ID = 79, Port = 41638 Host = 10.10.10.10
Aug 18 10:04:18 server1 radiusd[389278]: [2]:User-Name = "user_id1"
Aug 18 10:04:18 server1 radiusd[389278]: [2]:NAS-IP-Address = 10.10.10.10
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Framed-Protocol = PPP
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Leaving parse_packet()
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Verifying Message-Authenticator
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Message-Authenticator successfully verified
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside proxy_request_needed() function
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Proxy is not turned on
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Username = [user_id1]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Client IP = [10.10.10.10]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside parse_for_login( user_id1 )
Aug 18 10:04:18 server1 radiusd[389278]: [2]:User_id remaining after prefix removal = [user_id1]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:User_id remaining after suffix removal = [user_id1]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside rad_authenticate() function
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Authentication request received for [client1.austin.ibm.com]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Calling get_ldap_user() to get LDAP user data
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_user:LDAP user id: user_id1.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_user:LDAP max_login_cnt:2.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_user:LDAP EAP_type: 4.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_user:LDAP passwordexpiredweeks: 9.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_active_sessions:number of free entries= 2.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:get_ldap_active_session:dn retrieved=
  radiusuniqueidentifier=user_id11, ou=radiusActiveUsers, cn=aixradius.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside get_client_secret routine for ip:10.10.10.10
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Found NAS-IP = [10.10.10.10]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Found shared secret.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:authenticate_password_PAP: Passwords do not match, user is
rejected
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Authentication failed for user [user_id1] using IP [10.10.10.10]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:ACCESS-REJECT - sending reject for id 79 to 10.10.10.10
 (client1.austin.ibm.com)
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside proxy_response_needed() function
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Proxy is not turned on
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Inside get_client_secret routine for ip:10.10.10.10
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Found NAS-IP = [10.10.10.10]
Aug 18 10:04:18 server1 radiusd[389278]: [2]:Found shared secret.
Aug 18 10:04:18 server1 radiusd[389278]: [2]:send_reject() Outgoing Packet:
Aug 18 10:04:18 server1 radiusd[389278]: [2]:  Code = 3, Id = 79, Length = 30
Aug 18 10:04:18 server1 radiusd[389278]: [2]:send_reject() Outgoing Packet:
Aug 18 10:04:18 server1 radiusd[389278]: [2]:  Code = 3, Id = 79, Length = 30
Aug 18 10:04:18 server1 radiusd[389278]: [2]:  Authenticator = 0x05D4865C6EBEFC1A9300D2DC66F3DBE9
Aug 18 10:04:18 server1 radiusd[389278]: [2]:    Type =  18, Length =  10, Value = 0x4261646E65737321
Aug 18 10:04:18 server1 radiusd[389278]: [2]:*** Leave Process_Packet() **
```

Utrata ważności hasła

Opcja utraty ważności hasła umożliwia powiadomienie klienta RADIUS o utracie ważności hasła użytkownika oraz zaktualizowanie hasła użytkownika przy użyciu protokołu RADIUS.

Utrata ważności hasła pociąga za sobą obsługę czterech typów pakietów oraz nowego atrybutu. Nowe typy pakietów znajdują się w słowniku systemu AIX, a opcja utraty ważności hasła musi być włączona.

Nie w każdej instalacji serwera RADIUS pożądana jest opcja umożliwiająca aktualizowanie hasła, które utraciło ważność, za pośrednictwem serwera RADIUS. Pozycja w pliku `radiusd.conf` daje możliwość włączenia lub wyłączenia obsługi zmiany hasła za pośrednictwem serwera RADIUS. Domyślnie taka opcja jest wyłączona. Istnieje możliwość dodania komunikatu odpowiedzi użytkownika `Password_Expired_Reply_Message`, który zwracany jest w pakiecie password-expired. Atrybuty hasła, zarówno stare jak i nowe, muszą być szyfrowane i deszyfrowane za pomocą metody PAP.

Atrybuty specyficzne dla dostawcy
Atrybuty specyficzne dla dostawcy definiowane są przez dostawców serwerów zdalnego dostępu, zazwyczaj dostawców sprzętu, w celu dostosowania działania serwera RADIUS do swoich serwerów.

Atrybuty specyficzne dla dostawcy są konieczne, jeśli użytkownicy mają mieć uprawnienia do więcej niż jednego rodzaju dostępu. Atrybuty specyficzne dla dostawcy mogą być używane w połączeniu z atrybutami zdefiniowanymi dla serwera RADIUS.

Atrybuty specyficzne dla dostawcy są opcjonalne, ale jeśli sprzęt serwera NAS, w celu prawidłowego działania, wymaga skonfigurowania dodatkowych atrybutów, należy je dodać do pliku słownika.

Atrybuty specyficzne dla dostawcy mogą być użyte także do przyszłej autoryzacji. W celu dokonania autoryzacji, atrybutów specyficznych dla dostawcy można użyć razem z atrybutami `User-Name` (Nazwa użytkownika) i `Password` (Hasło). Po stronie serwera plik strategii autoryzacji użytkownika zawiera listę atrybutów, które mają być sprawdzone w pakiecie Access-Request (Żądanie dostępu) dla danego użytkownika. Jeśli pakiet nie zawiera atrybutów z listy pliku users, wtedy do serwera NAS odsyłany jest pakiet access_reject (odmowa dostępu). Atrybuty specyficzne dla dostawcy mogą być także użyte jako lista par atrybut=wartość w pliku ***identyfikator_użytkownika*****.**`policy`.

Poniżej przedstawiono przykładową sekcję atrybutów specyficznych dla dostawcy z pliku słownika:

```
###############################################################################
#                                                                             #
#   Ta sekcja zawiera przykłady tłumaczeń słownikowych dla analizy     #
#   atrybutów specyficznych dla dostawcy. Poniższy przykład dotyczy    #
#   "Cisco". Przed zdefiniowaniem pary atrybut/wartość dla             #
#   dostawcy, wymagana jest definicja "VENDOR" (dostawcy).             #
#                                                                             #
#   Przykład:                                                                 #
#                                                                             #
#   VENDOR          Cisco           9                                         #
#                                                                             #
#   VENDOR:  Określa to, że atrybuty po tej pozycji dotyczą dostawcy   #
#            Cisco.                                                           #
#   Cisco :  Oznacza nazwę dostawcy                                           #
#   9     :  Id dostawcy zdefiniowany w RFC "Assigned Numbers"         #
#                                                                             #
###############################################################################

#VENDOR          Cisco           9

#ATTRIBUTE       Cisco-AVPair              1       string
#ATTRIBUTE       Cisco-NAS-Port            2       string
#ATTRIBUTE       Cisco-Disconnect-Cause    195     integer
#
#----------------Cisco-Disconnect-Cause--------------------------------#
#
#VALUE           Cisco-Disconnect-Cause    Unknown                 2
#VALUE           Cisco-Disconnect-Cause    CLID-Authentication-Failure 4
#VALUE           Cisco-Disconnect-Cause    No-Carrier              10
#VALUE           Cisco-Disconnect-Cause    Lost-Carrier            11
#VALUE           Cisco-Disconnect-Cause    No-Detected-Result-Codes    12
#VALUE           Cisco-Disconnect-Cause    User-Ends-Session       20
#VALUE           Cisco-Disconnect-Cause    Idle-Timeout            21
#VALUE           Cisco-Disconnect-Cause    Exit-Telnet-Session     22
#VALUE           Cisco-Disconnect-Cause    No-Remote-IP-Addr       23
```

Obsługa komunikatu odpowiedzi serwera RADIUS
Komunikat odpowiedzi jest tekstem tworzonym i konfigurowanym w pliku `radiusd.conf`.

Przeznaczony jest dla serwera NAS lub AP i jest to łańcuch zwracany użytkownikowi. Może to być komunikat dotyczący powodzenia, niepowodzenia lub zakwestionowania. Są to możliwe do odczytu pola tekstowe, których zawartość jest zależna od implementacji i jest ustawiana na serwerze podczas konfigurowania. Wartością domyślną dla tych atrybutów jest brak tekstu. Użytkownik może skonfigurować wszystkie atrybuty, jeden, dwa lub trzy atrybuty lub nie konfigurować żadnego.

Serwer RADIUS obsługuje następujące atrybuty komunikatu odpowiedzi:

- Accept Reply-Message (Komunikat odpowiedzi zaakceptowania),
- Reject Reply-Message (Komunikat odpowiedzi odrzucenia),

- CHAP Reply-Message (Komunikat odpowiedzi protokołu CHAP),
- Password Expired Reply-Message (Komunikat odpowiedzi utraty ważności hasła).

Te atrybuty są dodawane do pliku konfiguracyjnego `radiusd.conf` i odczytywane w globalnej strukturze konfiguracji podczas startu demona. Te wartości można ustawić za pomocą paneli RADIUS programu SMIT jako część opcji `Configure Server` (Konfiguruj serwer). Maksymalna liczba znaków dla każdego łańcucha wynosi 256 bajtów.

Funkcja implementowana jest w następujący sposób:

1. Podczas uruchamiania demona **radiusd** odczytywany jest plik `radiusd.conf` oraz ustawiane są atrybuty Reply-Message (Komunikatu odpowiedzi).
2. Po otrzymaniu pakietu access request (żądanie dostępu) użytkownik jest uwierzytelniany.
3. Jeśli odpowiedzią uwierzytelniania jest access accept (dostęp przyznany), wtedy sprawdzany jest tekst atrybutu Accept Reply-Message (Komunikat odpowiedzi zaakceptowania). Jeśli tekst jest dostępny, łańcuch zwracany jest w pakiecie access accept (dostęp przyznany).
4. Jeśli uwierzytelnianie zostanie odrzucone, wtedy sprawdzany jest tekst atrybutu Reject Reply-Message (Komunikat odpowiedzi odrzucenia), który zwracany jest z pakietem access reject (dostęp odrzucony).
5. Jeśli uwierzytelnianie zostanie zakwestionowane, wtedy sprawdzany jest atrybut CHAP Reply-Message (Komunikat odpowiedzi protokołu CHAP) i, jeśli istnieje, wysyłany jako część pakietu Access-Challenge (Dostęp zakwestionowany).

Konfigurowanie puli IP serwera RADIUS
Przy użyciu serwera RADIUS można adres IP przypisywać dynamicznie z puli adresów IP.

Przydzielanie adresu IP jest częścią procesu autoryzacji wykonywaną po uwierzytelnieniu. Administrator systemu musi przypisać unikalny adres IP każdemu użytkownikowi. Na serwerze RADIUS dostępne są trzy opcje dynamicznego udostępniania adresu IP użytkownikowi.

- Atrybut Framed Pool
- Korzystanie z atrybutu specyficznego dla dostawcy
- Przydzielanie adresu IP z puli przez serwer RADIUS

Atrybut Framed Pool

Nazwa puli dla puli IP musi być zdefiniowana na serwerze NAS (Network Access Server). Serwer NAS musi być zgodny ze standardem RFC2869, aby serwer RADIUS mógł wysyłać atrybut **Framed-Pool** w pakiecie Access-Accept (akceptacja dostępu) (atrybut typu 88). Administrator systemu musi skonfigurować serwer NAS i zaktualizować atrybuty autoryzacji dla użytkownika, włączając atrybut **Framed-Pool** albo do pliku globalnego `default.auth`, albo do pliku `użytkownik.auth` na serwerze RADIUS. Plik słownika na serwerze RADIUS zawiera ten atrybut:

```
ATTRIBUTE    Framed-Pool    88       string
```

Jeśli serwer NAS nie może używać wielu pul adresów, zignoruje ten atrybut. Pula adresów na serwerze NAS zawiera listę adresów IP. Serwer NAS dynamicznie wskazuje jeden z adresów IP zdefiniowanych w określonej puli i przypisuje go do użytkownika.

Atrybuty specyficzne dla dostawcy

Niektórzy niezależni producenci oprogramowania nie mogą używać atrybutu **Framed-Pool**, ale mają możliwość zdefiniowania pul adresów IP. Serwer RADIUS może wykorzystać te pule adresów przy użyciu modelu atrybutu specyficznego dla dostawcy (Vendor-Specific Attribute - VSA). Na przykład serwer NAS Cisco udostępnia atrybut zwany Cisco-AVPair. Plik słownika na serwerze RADIUS zawiera ten atrybut:

```
VENDOR     Cisco           9
ATTRIBUTE  Cisco-AVPair    1       string
```

Kiedy serwer wysyła pakiet Access-Request (żądanie dostępu), włącza ten atrybut w postaci kodu `Cisco-AVPair="ip:addr-pool=`*`nazwapuli`*`"`, gdzie *nazwa puli* jest nazwą puli adresów zdefiniowaną na serwerze NAS. Po uwierzytelnieniu i autoryzowaniu żądania, serwer RADIUS zwraca atrybut w pakiecie Access-Accept (akceptacja dostępu). Wówczas serwer NAS może przydzielić użytkownikowi adres IP, korzystając ze zdefiniowanej puli. Administrator systemu musi skonfigurować serwer NAS i zaktualizować atrybuty autoryzacji dla użytkownika, włączając atrybut VSA albo do pliku globalnego `default.auth`, albo do pliku `użytkownik.auth` na serwerze RADIUS.

Przydzielanie adresu IP z puli przez serwer RADIUS

Serwer RADIUS można skonfigurować, tak aby generował adres IP z puli adresów IP. Adres IP jest zwracany w atrybucie Framed-IP-Address (Adres IP z ramką) pakietu Access-Accept (akceptacja dostępu).

Administrator systemu może zdefiniować pulę adresów IP przy użyciu interfejsu programu SMIT. Adresy są przechowywane w pliku `/etc/radius/ippool_def`. *Nazwy pul* definiuje się w pliku `etc/radius/clients`. Administrator systemu musi także skonfigurować numer portu serwera NAS. Demon serwera RADIUS wykorzystuje informacje z plików `etc/radius/clients` i `/etc/radius/ippool_def` do tworzenia plików danych. Po uruchomieniu demona administrator nie może zmieniać ani dodawać *nazw pul* i zakresów adresów IP, dopóki serwery RADIUS nie zostaną zatrzymane. Demon serwera RADIUS po uruchomieniu odczytuje plik konfiguracyjny (`/etc/radius/radius.conf`) i jeśli przydzielanie adresów IP jest włączone (`Enable_IP_Pooling=YES`), włącza globalną opcję przydzielania adresów IP (`IP_pool_flag`). Następnie demon sprawdza, czy istnieje plik `nazwapuli.data`. Jeśli tak, to go odczytuje i umieszcza odczytane informacje w pamięci współużytkowanej. Następnie aktualizuje plik i pamięć współużytkowaną na podstawie żądań przychodzących od klientów. Jeśli plik nie istnieje, demon tworzy nowy plik, korzystając z informacji w plikach `etc/radius/clients` i `/etc/radius/ippool_def`. Maksymalna wielkość pliku `nazwa puli.data` wynosi 256 MB (ograniczenie wielkości segmentu AIX). Jeśli plik `nazwa puli.data` jest większy niż 256 MB, serwer RADIUS protokołuje komunikat o błędzie i kończy pracę.

Demon pobiera szczegóły puli IP z pliku `/etc/radius/ippool_def` i obsługuje tabelę adresów IP dla każdej nazwy puli w pamięci współużytkowanej. Tabela ma pozycje dla atrybutów NAS-IP-address (Adres IP serwera NAS), NAS-port (Port serwera NAS) i opcji IN USE (W UŻYCIU). Demon obsługuje tabelę mieszającą z kluczem NAS-IP NAS-port. Kiedy przychodzą żądania od wielu użytkowników, są kolejkowane przez protokół UDP, a demon pobiera z żądania dane NAS-IP i NAS-port. Korzystając z tych informacji, sprawdza, czy dla tego serwera NAS została zdefiniowana *nazwa puli*; w tym celu przegląda informacje odczytane z pliku `etc/radius/clients`.

Demon próbuje uzyskać z puli nieużywany adres. Jeśli nieużywany adres jest dostępny, zostanie on oznaczony jako używany przez opcje NAS-IP (Adres IP serwera NAS) i NAS-port (Port serwera NAS) i zwrócony do serwera RADIUS. Adres IP zostanie umieszczony przez demon w atrybucie **Framed-IP-Address** i zwrócony do serwera NAS w pakiecie akceptacji. Plik `nazwa puli.data` także zostanie zaktualizowany w celu zsynchronizowania z informacjami w pamięci współużytkowanej.

Jeśli pula nie istnieje lub istnieje, ale nie zawiera już nieużywanych adresów, do serwera RADIUS zwracany jest błąd. W pliku protokołu zapisywany jest błąd `Could not allocate IP address` (Nie można przydzielić adresu IP) i serwer RADIUS wysyła do serwera NAS pakiet Access-Reject (odrzucenie dostępu).

Kody błędów są następujące:

- NOT_POOLED – nie ma puli zdefiniowanej dla `nas_ip`.
- POOL_EXHAUSTED – istnieje pula zdefiniowana dla `nas_ip`, ale wszystkie adresy z tej puli są aktualnie w użyciu.

Kiedy żądanie uwierzytelnienia przychodzi z kombinacji serwera NAS i numeru portu NAS, która ma już przydzielony adres IP, demon zwraca poprzedni przydział do puli, zaznaczając opcję IN USE (W UŻYCIU) jako wyłączoną i zerując w tabeli pozycje NAS-IP-address (Adres IP serwera NAS) i NAS-port (Port serwera NAS). Następnie przydziela nowy adres IP z puli.

Adres IP jest zwracany do puli także wówczas, gdy serwer RADIUS otrzymuje od serwera NAS pakiet Accounting-Stop (koniec rozliczania). Pakiet Accounting-Stop musi zawierać pozycje NAS-IP-address i NAS-port. Demon uzyskuje dostęp do pliku `ippool_mem` w następujących przypadkach:

- Przychodzi żądanie pobrania nowego adresu IP. Demon ustawia opcję IN USE na wartość True.
- Otrzymano pakiet Accounting-Stop. Demon zwalnia adres IP, ustawiając opcję In Use (W użyciu) na wartość False.

Za każdym razem wywołania systemowe pamięci współużytkowanej zapewniają zsynchronizowanie danych w pamięci współużytkowanej i w pliku `nazwa puli.data`. Administrator systemu może włączyć lub wyłączyć opcję przydzielania adresów IP, ustawiając wartość parametru *Enable_IP_Pooling* na ON lub OFF w pliku konfiguracyjnym serwera RADIUS (`radiusd.conf`). Jest to przydatne w przypadkach, gdy administrator systemu ma przypisany adres IP albo w globalnym pliku `default.auth`, albo w pliku `użytkownik.auth`. Aby korzystać z tego przypisanego adresu IP, administrator systemu musi ustawić parametr `Enable_IP_Pool = NO`.

Przykład pliku `/etc/radius/ippool_def` utworzonego w programie SMIT:

Pool Name (Nazwa puli)	**Start Range (Początek zakresu)**	**End Range (Koniec zakresu)**
Piętro 5	192.165.1.1	192.165.1.125
Piętro 6	192.165.1.200	192.165.1.253

Przykład pliku `/etc/radiusclients` utworzonego w programie SMIT:

NAS-IP (Adres IP serwera NAS)	**Shared Secret (Współużytkowane dane szyfrujące)**	**Pool Name (Nazwa puli)**
1.2.3.4	Dane szyfrujące 1	Piętro 5
1.2.3.5	Dane szyfrujące 2	Piętro 6
1.2.3.6	Dane szyfrujące 3	Piętro 5
1.2.3.7	Dane szyfrujące 4	

W powyższym przykładzie dla adresu IP serwera NAS 1.2.3.7 nazwa puli jest pusta. W takim przypadku dla tego serwera NAS nie będzie wykonywane przydzielanie adresu IP z puli (nawet jeśli globalna opcja `IP_pool_flag = True`). Kiedy nadchodzi pakiet Access-Request (żądanie dostępu), serwer RADIUS wykonuje uwierzytelnianie i autoryzację. Jeśli wynik będzie pomyślny, serwer wyśle w pakiecie Access-Accept (akceptacja dostępu) statyczny adres IP zdefiniowany w żądaniu lub pochodzący z pliku globalnego `default.auth` lub pliku `użytkownik.auth`. W takim przypadku nie jest wymagany atrybut NAS-Port (Port serwera NAS).

Jeśli opcja przydzielania adresu IP z puli jest ustawiona na `True`, a administrator systemu zdefiniuje także statyczny adres IP w pliku globalnym `default.auth` lub w pliku `użytkownik.auth`, lub w pakiecie Access-Request (żądanie dostępu), serwer RADIUS zastąpi ten adres IP adresem IP przydzielonym z puli zdefiniowanej dla tego serwera NAS. Jeśli wszystkie adresy IP z tej puli są w użyciu, serwer zaprotokołuje błąd (pula jest pełna) i wyśle pakiet Access-Reject (odrzucenie dostępu). Serwer zignoruje statyczny adres IP określony w plikach `auth`.

Jeśli opcja przydzielania adresu IP z puli jest ustawiona na `True` i dla serwera NAS zdefiniowana jest poprawna nazwa puli, to kiedy z adresu IP tego serwera NAS przyjdzie pakiet Access-Request bez określonego atrybutu NAS-Port (Port serwera NAS), serwer wysyła pakiet Access-Reject (odrzucenie dostępu).

Poniżej przedstawiono przykład pliku `Piętro 5.data` utworzonego przez demon:

IP Address (Adres IP)	NAS-IP (Adres IP serwera NAS)	NAS-Port (Port serwera NAS)	In Use (W użyciu)
192.165.1.1	1.2.3.4	2	1
192.165.1.2	1.2.3.4	3	0
.....	.....	....	....
192.165.1.124	1.2.3.6	1	1
192.165.1.125	1.2.3.6	6	1

Poniżej przedstawiono przykład pliku `Piętro 6.data` utworzonego przez demon:

IP Address (Adres IP)	NAS-IP (Adres IP serwera NAS)	NAS-Port (Port serwera NAS)	In Use (W użyciu)
192.165.200	1.2.3.4	1	1
192.165.201	1.2.3.4	4	1
.....	.....	....	....
192.165.1.252	1.2.3.4	5	0
192.165.1.253	1.2.3.4	6	1

Kiedy konieczne jest zwolnienie wszystkich adresów IP przydzielonych do określonego serwera NAS (na przykład, gdy serwer zostanie zatrzymany), potrzebne może być zwolnienie wszystkich adresów IP ze wszystkich pul, w celu zainicjowania pliku *nazwa puli*`.data`. Administrator systemu może to zrobić za pomocą programu SMIT, korzystając z następujących opcji menu:

- Wyzeruj pulę IP dla klienta
- Wyzeruj całą pulę IP

Panele programu SMIT dotyczące puli IP

Po wybraniu opcji **Dodaj klienta** z menu Konfiguracja klienta można wprowadzić opcjonalny parametr **Nazwa puli**. Nazwa może składać się maksymalnie z 64 znaków. Jeśli pole **Nazwa puli** jest puste, przydzielanie adresów IP z puli nie będzie wykonywane i serwer RADIUS będzie przypisywał adres IP zdefiniowany przez administratora systemu za pomocą atrybutu autoryzacji **Framed-IP-Address**.

Po wybraniu opcji **IP Pool** (Pula IP) wyświetlane są następujące opcje:

- List all IP Pools (Wyświetl wszystkie pule IP),
- Create an IP Pool (Utwórz pulę IP),
- Change/Show Characteristics of an IP Pool (Zmień/pokaż charakterystykę puli IP),
- Delete an IP Pool (Usuń pulę IP),
- Wyzeruj pulę IP dla klienta
- Wyzeruj całą pulę IP

List all IP Pools (Wyświetl wszystkie pule IP): ta opcja służy do wyświetlenia wartości pól **Pool Name** (Nazwa puli), **Start Range IP address** (Początek zakresu adresów IP) i **Stop Range IP address** (Koniec zakresu adresów IP).

Create an IP Pool (Utwórz pulę IP): Ta opcja służy do dodania nazwy puli oraz początku i końca zakresu. Dane te są dodawane na końcu pliku `ippool_def`. Aby zapewnić, że nazwy pul się nie duplikują i że zakresy adresów IP są rozłączne, wykonywane są odpowiednie sprawdzenia. Czynność tę można wykonać tylko wtedy, gdy demony serwera RADIUS nie są uruchomione.

Change/Show Characteristics of an IP Pool (Zmień/pokaż charakterystykę puli IP): Ta opcja powoduje wyświetlenie listy nazw pul w panelu wywoływanym. Na tym panelu trzeba wybrać konkretną nazwę puli.

Po jej wybraniu zostanie wyświetlony panel dotyczący tej nazwy puli. Po naciśnięciu klawisza Enter dane dotyczące tej puli są aktualizowane w pliku `ippool_def`. Czynność tę można wykonać tylko wtedy, gdy demony serwera RADIUS nie są uruchomione.

Delete an IP Pool (Usuń pulę IP): Wybranie tej opcji powoduje wyświetlenie listy nazw pul do wyboru. Po wybraniu nazwy puli wyświetlany jest panel wywoływany `Are You Sure` (Czy na pewno), na którym należy potwierdzić zamiar usunięcia puli. Wywoływany jest skrypt **`rmippool`**, który usuwa nazwę puli z pliku `ippool_def`. Czynność tę można wykonać tylko wtedy, gdy demony serwera RADIUS nie są uruchomione.

Clear IP Pool for a Client (Wyzeruj pulę IP dla klienta): Ta opcja ustawia pozycję `IN-USE` (W UŻYCIU) na wartość `0` dla adresów IP należących do serwera NAS, co oznacza, że wszystkie adresy IP dla tego serwera NAS są teraz dostępne. Czynność tę można wykonać tylko wtedy, gdy demony serwera RADIUS nie są uruchomione.

Clear Entire IP Pool (Wyzeruj całą pulę IP): Po wybraniu tej opcji wyświetlany jest panel wywoływany `Are You Sure` (Czy na pewno), na którym należy dokonać potwierdzenia przed wyzerowaniem całego pliku `ippool_mem`. Czynność tę można wykonać tylko wtedy, gdy demony serwera RADIUS nie są uruchomione.

Panele RADIUS programu SMIT
Podczas konfigurowania serwera RADIUS za pomocą programu SMIT wypełnienie pól oznaczonych gwiazdką (*) jest wymagane.

Krótka ścieżka programu SMIT wygląda następująco:

```
smitty radius
```

Menu główne serwera RADIUS wygląda następująco:

```
       Serwer RADIUS

Konfiguruj serwer
Konfiguruj klientów
Konfiguruj użytkowników
Konfiguruj reguły proxy
Zaawansowana konfiguracja serwera
Uruchom demony serwera RADIUS
Zatrzymaj demony serwera RADIUS
```

Poniżej przedstawiono przykładowy panel programu SMIT do konfigurowania serwera RADIUS:

```
Konfiguruj serwer
  Katalog RADIUS                                    /etc/radius
* Położenie bazy danych                             [Lokalna]          +
  Nazwa pliku lokalnej bazy danych AVL              [dbdata.bin]
  Poziom śledzenia błędów                           [9]                +#
  Rozliczanie lokalne                               [ON]               +
  Katalog rozliczania lokalnego                [/var/radius/data/accou>
  Komunikat odpowiedzi akceptującej                 []
  Komunikat odpowiedzi odrzucającej                 []
  Komunikat odpowiedzi wzywania                     []
  Komunikat odpowiedzi o wygaśnięciu hasła          []
  Obsługa odnawiania wygasłego hasła               [NIE]              +
  Wymagaj hosta uwierzytelniającego komunikaty      [NIE]               +
*Numer portu uwierzytelniania                        [1812]
*Numer portu rozliczania                             [1813]
  Nazwa serwera LDAP                                []
  Numer portu serwera LDAP                          [389]               #
  Nazwa wyróżniająca administratora serwera LDAP    [cn=root]
  Hasło administratora serwera LDAP                 []
  Bazowa nazwa wyróżniająca LDAP                    [cn=aixradius]
  Limit wielkości LDAP                              [0]                 #
  Limit liczby przeskoków LDAP                      [0]                 #
  Limit czasu oczekiwania LDAP                      [10]                #
  Poziom śledzenia błędów LDAP                      [0]                +#
  Proxy dozwolony                                   [WYŁ]              +
  Tabela użycia proxy                               [WYŁ]              +
  Nazwa dziedziny proxy                             []
  Ograniczniki przedrostków proxy                   [$/]
  Ograniczniki przyrostków proxy                    [@.]
  Proxy usuwa nazwy dziedzin                        [NIE]              +
  Liczba ponownych prób proxy                       [2]                 #
  Limit czasu proxy                                 [30]                #
  Sprawdzanie ograniczeń logowania UNIX             [WYŁ]              +
  Utwórz pulę IP                                    [WYŁ]              +
  Wyślij element uwierzytelniający dla ACCEPT       [WŁ]               +
  Maksymalna liczba wątków serwera RADIUS           [15]                #
  Limit czasu konwersacji EAP (sekundy)             [30]                #
  Włącz EAP-TLS                                     [WŁ]                +
  Wymagane opcje dla EAP-TLS
       Ścieżka do biblioteki OpenSSL                [/opt/freeware/lib/libs>
       Lista szyfrów OpenSSL                        [ALL:!ADH:RC4+RSA:+SSLv>
       Katalog głównego ośrodka CA (pełna ścieżka) [/etc/radius/tls]
       Certyfikat głównego ośrodka CA (pełna ścieżka)[/etc/radius/tls/radius>
       Certyfikat serwera RADIUS (pełna ścieżka)   [/etc/radius/tls/cert-s>
       Klucz prywatny serwera RADIUS (pełna ścieżka) [/etc/radius/tls/cert-s>
       CRL serwera RADIUS (pełna ścieżka)           []
```

Szczegółowe informacje pomocy programu SMIT dla wszystkich pól i opcji menu są dostępne po naciśnięciu klawisza F1.

Generator liczb losowych
Liczby losowe są wymagane podczas generowania pola Authenticator (Host uwierzytelniający) pakietu RADIUS.

Ważne jest udostępnianie najlepszego z możliwych generatorów, ponieważ włamywacz może próbować oszukać serwer RADIUS w odpowiadaniu na przewidywane żądania, a następnie użyć odpowiedzi w celu podszycia się pod ten serwer RADIUS dla przyszłych żądań dostępu. Serwer RADIUS systemu AIX, do generowania liczb pseudolosowych korzysta z rozszerzenia jądra `/dev/urandom` . To rozszerzenie jądra zbiera próbki entropii ze źródeł sprzętowych poprzez sterownik pseudourządzenia. W celu zapewnienia prawidłowej losowości urządzenie to przeszło testy NIST.

Obsługa globalizacji
Komenda **raddbm** serwera RADIUS oraz panele SMIT za pośrednictwem standardowych wywołań funkcji API globalizacji systemu AIX zapewniają obsługę globalizacji.

Informacje pokrewne

Komendy: **installp**,**mkuser** i **raddbm**

Zapobieganie włamaniom w systemie AIX

Opcja zapobiegania włamaniom w systemie AIX wykrywa nieodpowiednie, nieautoryzowane lub inne dane, które mogą być szkodliwe dla systemu.

Przedstawiona poniżej sekcja opisuje różne sposoby wykrywania włamań udostępniane przez system AIX.

Informacje pokrewne

Komendy: **chfilt**, **ckfilt**, **expfilt**, **genfilt**, **impfilt**, **lsfilt**, **mkfilt**, **mvfilt**, **rmfilt**.

Wykrywanie włamań

Wykrywanie włamań jest działaniem polegającym na monitorowaniu i analizowaniu zdarzeń systemowych, w celu przechwycenia i odrzucenia prób dostępu do systemu przez nieuprawnionych użytkowników. W systemie AIX takie wykrywanie dostępu przez nieuprawnionych użytkowników lub prób takiego dostępu przeprowadzane jest przez obserwowanie pewnych działań, a następnie stosowanie reguł filtrowania wobec tych działań.

Uwaga: Aby włączyć wykrywanie włamań w systemie hosta, należy zainstalować zestaw plików `bos.net.ipsec`. Technologie wykrywania zbudowane są w oparciu o istniejące opcje protokołu IPsec systemu AIX.

Dopasowywanie wzorca reguł filtrowania

Dopasowywanie wzorca polega na używaniu reguły filtrowania IPsec w celu filtrowania pakietów sieciowych. Wzorzec filtrowania może być łańcuchem tekstowym, łańcuchem szesnastkowym lub plikiem zawierającym więcej niż jeden wzorzec. Po wykryciu w treści pakietu sieciowego ustanowionej reguły wzorca filtrowania wykonane zostanie zdefiniowane wcześniej działanie reguły filtrowania.

Dopasowywanie wzorca reguł filtrowania ma zastosowanie tylko do przychodzących pakietów sieciowych. Aby dodać regułę do tabeli reguł filtrowania, należy użyć komendy **genfilt**. Reguły filtrowania generowane przez tę komendę nazywane są ręcznymi regułami filtrowania. Aby aktywować lub dezaktywować reguły filtrowania, należy użyć komendy **mkfilt** . Komenda **mkfilt** może zostać także użyta do sterowania funkcjami protokołowania filtrowania.

Plik wzorca może zawierać listę wzorców tekstowych lub szesnastkowych (jeden w wierszu). Dopasowywanie wzorca reguł filtrowania może być używane do zabezpieczenia przed wirusami, przepełnieniem buforu oraz innymi atakami sieciowymi.

Dopasowywanie wzorca reguł filtrowania może mieć negatywny wpływ na wydajność systemu, jeśli jest stosowane zbyt szeroko wraz z dużą liczbą wzorców. Najlepiej, aby zasięg ich stosowania był jak najwęższy. Na przykład, jeśli dla komendy `sendmail` jest stosowany znany wzorzec wirusa, w regule filtrowania dla tej komendy jako port docelowy SMTP należy podać 25. Zapewni to, że dopasowywanie wzorca nie będzie miało wpływu na pozostały ruch.

Komenda **genfilt** wykrywa i rozpoznaje formaty wzorca używane w niektórych wersjach dostępnych w serwisie ClamAV.

Informacje pokrewne

Komenda genfilt
Komenda mkfilt
Serwis WWW ClamAV

Typy wzorców

Istnieją trzy podstawowe typy wzorców: tekstowy, szesnastkowy i plik. Dopasowywanie wzorca reguł filtrowania ma zastosowanie tylko do pakietów przychodzących.

Wzorzec tekstowy

Tekstowy wzorzec filtrowania jest łańcuchem ASCII, który wygląda podobnie do następującego:

```
GET /../../../../../../../../
```

Wzorzec szesnastkowy

Wzorzec szesnastkowy wygląda podobnie do następującego:

```
0x33c0b805e0cd16b807e0cd1650558becc7460200f05d0733ffb8c800b9fffff3abb00150
e670e47132c0e67158fec03c8075f033c033c9b002fa99cd26fb4183f90575f5c3
```

Uwaga: Wzorzec szesnastkowy jest odróżniany od tekstowego za pomocą początkowych znaków 0x.

Pliki zawierające wzorce tekstowe

Plik może zawierać listę wzorców tekstowych lub szesnastkowych (jeden w wierszu). Przykładowe pliki wzorców można znaleźć pod adresem http://www.clamav.net .

Reguły filtrowania umożliwiające unikanie portu i hosta

Konfigurując regułę filtrowania umożliwiającą unikanie, można odmówić dostępu do lokalnego komputera zdalnemu hostowi lub parze zdalny host i port.

Reguła filtrowania umożliwiająca unikanie dynamicznie tworzy regułę wynikową, która odmawia zdalnemu hostowi lub parze zdalny host i port dostępu do lokalnego komputera, gdy spełnione zostaną określone kryteria reguły.

Ponieważ ataki powszechnie poprzedzane są skanowaniem portów, reguły filtrowania umożliwiające unikanie portu są szczególnie przydatne przy zabezpieczaniu przed włamaniem przez wykrywanie tego typu zachowania.

Na przykład, jeśli host lokalny nie korzysta z portu 37 serwera, który jest serwerem czasu, wtedy zdalny host nie powinien uzyskiwać dostępu do portu 37, chyba że przeprowadza skanowanie portów. Dla portu 37 należy umieścić regułę filtrowania umożliwiającą unikanie portu tak, że jeśli zdalny host spróbuje uzyskać dostęp do tego portu, reguła filtrowania umożliwiająca unikanie utworzy regułę wynikową, która zablokuje danemu hostowi dalszy dostęp na czas określony w polu **Czas utraty ważności** reguły unikania.

Jeśli pole **Czas utraty ważności** reguły unikania ma wartość 0, wtedy dynamicznie tworzona wynikowa reguła unikania nie traci ważności.

Uwaga:

1. Czas utraty ważności podany w regule filtrowania umożliwiającej unikanie portu ma zastosowanie tylko dla dynamicznie tworzonej reguły wynikowej.
2. Dynamicznie tworzone reguły wynikowe można przeglądać jedynie za pomocą komendy **lsfilt -a**.

Reguły filtrowania umożliwiające unikanie hosta

Gdy spełnione zostaną kryteria reguły filtrowania umożliwiające unikanie hosta, dynamicznie tworzona reguła wynikowa będzie blokowała lub unikała całego ruchu w sieci ze zdalnego hosta przez określony czas.

Reguły filtrowania umożliwiające unikanie portu

Gdy spełnione zostaną kryteria reguły filtrowania umożliwiające unikanie portu, dynamicznie tworzona reguła wynikowa będzie przez określony czas blokowała lub unikała ruchu w sieci pochodzącego z danego portu zdalnego hosta.

Stanowe reguły filtrowania

Filtry stanowe sprawdzają takie informacje, jak adresy źródłowy i docelowy, numery portów oraz status. Następnie stosując dla flag nagłówka reguły filtrowania IF, ELSE lub ENDIF, systemy stanowe mogą podejmować decyzje filtrowania w kontekście całej sesji, a nie tylko dotyczące pojedynczego pakietu i jego informacji nagłówkowych.

Inspekcja stanowa sprawdza przychodzące i wychodzące pakiety komunikacyjne. Gdy stanowe reguły filtrowania aktywowane są za pomocą komendy **mkfilt -u**, reguły znajdujące się w bloku ELSE zawsze sprawdzane są do momentu spełnienia reguły IF. Po spełnieniu reguły lub warunku IF, reguły w bloku IF używane są do ponownego aktywowania reguł filtrowania za pomocą komendy **mkfilt -u**.

Komenda **ckfilt** sprawdza składnię stanowych reguł filtrowania i wyświetla je na ekranie z dodatkowymi objaśnieniami, jak poniżej:

```
%ckfilt -v4
Beginning of IPv4 filter rules.
Rule 2
IF Rule 3
    IF Rule 4
        Rule 5
    ELSE Rule 6
        Rule 7
    ENDIF Rule 8
ELSE Rule 9
    Rule 10
ENDIF Rule 11
Rule 0
```

Reguły czasowe
Reguły czasowe określają czas, w sekundach, przez który reguła filtrowania jest stosowana po rozpoczęciu jej obowiązywania za pomocą komendy **mkfilt -v [4|6] -u**.

Czas utraty ważności określany jest za pomocą komendy **genfilt -e**. Więcej informacji na ten temat zawierają sekcje dotyczące komend **mkfilt** i **genfilt**.

Uwaga: Reguły czasowe nie mają wpływu na reguły IF, ELSE lub ENDIF. Jeśli w regule unikania hosta lub portu określono czas utraty ważności, czas ten ma zastosowanie tylko dla reguły wynikowej, która jest inicjowana przez regułę unikania. Dla reguł unikania nie istnieje czas utraty ważności.

Uzyskiwanie dostępu do reguł filtrowania z poziomu programu SMIT
Istnieje możliwość konfigurowania reguł z poziomu programu SMIT.

Aby z poziomu programu SMIT skonfigurować reguły filtrowania, należy wykonać następujące czynności:

1. W wierszu komend wpisz:`smitty ipsec4`
2. Wybierz opcję **Zaawansowana konfiguracja IPsec**.
3. Wybierz opcję **Konfiguruj reguły filtru IPsec**.
4. Wybierz opcję **Dodaj regułę filtru IPsec**.

```
                        Dodaj regułę filtru IPsec

Wpisz lub wybierz wartości w polach wprowadzania danych.
Naciśnij Enter PO wprowadzeniu wszystkich zmian.

[POCZĄTEK]                                          [Pola wprowadzania]
* Akcja reguły                                      [dozwolone]             +
* Adres IP źródłowy                                 []
* Maska IP źródłowa                                 []
  Adres IP docelowy                                 []
  Maska IP docelowa                                 []
* Zastosować do pakietów z opcją source routing?
  (POZWÓL/tylko wejściowy)                          [tak]                   +
* Protokół                                          [wszystkie]             +
* Port źródłowy / typ operacji ICMP                 [dowolna]               +
* Numer portu źródłowego / typ ICMP                 [0]                     #
* Port docelowy / kod operacji ICMP                 [dowolny]               +
* Numer portu docelowego / typ ICMP                 [0]                     #
* Routing                                           [oba]                   +
* Kierunek                                          [oba]                   +
* Sterowanie raportowaniem                          [nie]                   +
* Sterowanie fragmentacją                           [0]                     +
* Interfejs                                         []                      +
  Czas utraty ważności (sek)                        []                      #
  Typ wzorca                                        [brak]                  +
  Wzorzec / Plik wzorca                             []
  Opis                                              []


Gdzie "Typ wzorca" może mieć wartość:
  x   brak                                                                  x#
  x   wzorzec                                                               x
  x   plik                                                                  x
  x   Wzorce antywirusów
```

Możliwe wartości pola działanie to: `permit, deny, shun_host, shun_port, if, else, endif`.

Jeśli podany zostanie plik wzorca, musi on być możliwy do odczytu podczas aktywowania reguł filtrowania za pomocą komendy **mkfilt -a**. Reguły filtrowania przechowywane są w bazie danych /etc/security/ipsec_filter.

Program AIX Security Expert

Program Program AIX Security Expert umożliwia określanie wszystkich ustawień dotyczących bezpieczeństwa (TCP, NET, IPSEC, systemu i kontroli) w jednym miejscu.

Program Program AIX Security Expert jest narzędziem umożliwiającym wzmocnienie zabezpieczenia systemu. Należy do zestawu plików **bos.aixpert**. Program Program AIX Security Expert udostępnia kilka prostych opcji menu ustawień poziomu bezpieczeństwa: High Level Security (Wysoki poziom bezpieczeństwa), Medium Level Security (Średni poziom bezpieczeństwa), Low Level Security (Niski poziom bezpieczeństwa) oraz AIX Standard Settings (Ustawienia standardowe systemu AIX), integrujących ponad 300 ustawień konfiguracji zabezpieczeń, a jednocześnie zapewnia zaawansowanym administratorom kontrolę nad każdym elementem zabezpieczeń. Przy użyciu programu Program AIX Security Expert można zaimplementować odpowiedni poziom bezpieczeństwa bez konieczności zapoznawania się z dużą liczbą dokumentów na temat jego wzmacniania i bez konieczności samodzielnego implementowania poszczególnych elementów zabezpieczeń.

Program Program AIX Security Expert umożliwia rejestrację obrazu stanu konfiguracji zabezpieczeń. Ten obraz stanu można wykorzystać w celu ustawienia takiej samej konfiguracji zabezpieczeń w innych systemach. Pozwala to skrócić czas konfigurowania oraz zapewnia właściwą konfigurację zabezpieczeń wszystkich systemów znajdujących się w przedsiębiorstwie.

Program Program AIX Security Expert można uruchomić z programu SMIT lub za pomocą komendy **aixpert**.

Ustawienia programu Program AIX Security Expert

Dostępne są następujące zgrubne ustawienia poziomu bezpieczeństwa:

Wysoki poziom bezpieczeństwa
Ustawienia zapewniające wysoki poziom bezpieczeństwa.

Średni poziom bezpieczeństwa
Ustawienia zapewniające średni poziom bezpieczeństwa.

Niski poziom bezpieczeństwa
Ustawienia zapewniające niski poziom bezpieczeństwa.

Zaawansowane ustawienia zabezpieczeń
Niestandardowe zabezpieczenia określone przez użytkownika.

Ustawienia standardowe systemu AIX
Oryginalne systemowe ustawienia zabezpieczeń.

Cofnij ustawienia zabezpieczeń
Niektóre ustawienia konfiguracyjne programu Program AIX Security Expert można wycofać.

Sprawdź poziom bezpieczeństwa
Udostępnia szczegółowy raport na temat bieżących ustawień zabezpieczeń.

Wzmacnianie zabezpieczeń przy pomocy programu AIX Security Expert

Proces wzmacniania zabezpieczeń chroni wszystkie elementy systemu poprzez implementowanie wyższego poziomu bezpieczeństwa.

Proces wzmacniania zabezpieczeń ułatwia podejmowanie wszystkich decyzji dotyczących konfiguracji zabezpieczeń oraz zapewnia, że wszystkie ustawienia są właściwe i adekwatne do potrzeb. Do wzmocnienia bezpieczeństwa systemu AIX może być konieczna zmiana kilkuset ustawień konfiguracji zabezpieczeń.

Program Program AIX Security Expert udostępnia menu skupiające w jednym miejscu wspólne ustawienia konfiguracji zabezpieczeń. Ustawienia te stanowią efekt obszernych badań dotyczących prawidłowego zabezpieczania systemów UNIX. Zdefiniowano domyślne ustawienia zabezpieczeń spełniające potrzeby szerokiej gamy środowisk bezpieczeństwa (Wysoki, Średni i Niski poziom bezpieczeństwa). Ponadto zaawansowani administratorzy mają możliwość niezależnego określania każdego ustawienia konfiguracji zabezpieczeń.

Skonfigurowanie zbyt wysokiego poziomu bezpieczeństwa systemu może spowodować wyłączenie usług, których działanie jest pożądane. Na przykład usługi **telnet** i **rlogin** zostają wyłączone po ustawieniu wysokiego poziomu bezpieczeństwa, ponieważ w ich przypadku hasła logowania przesyłane są przez sieć w postaci niezaszyfrowanej. Jeśli w systemie zostanie skonfigurowany zbyt niski poziom zabezpieczeń, system taki będzie podatny na zagrożenia dotyczące bezpieczeństwa. Ponieważ każde przedsiębiorstwo dysponuje własnym zestawem wymagań związanych z bezpieczeństwem, predefiniowane ustawienia konfiguracyjne (wysoki poziom bezpieczeństwa, średni poziom bezpieczeństwa i niski poziom bezpieczeństwa) stanowią raczej doskonały punkt wyjścia do zdefiniowania własnej konfiguracji zabezpieczeń, a nie ostateczną jej wersję spełniającą wymagania konkretnego przedsiębiorstwa.

Praktycznym przykładem wykorzystania programu Program AIX Security Expert jest utworzenie systemu testowego (w realistycznym środowisku testowym) podobnego do środowiska produkcyjnego, w którym będzie przeprowadzana instalacja. Zainstaluj niezbędne aplikacje biznesowe i uruchom program Program AIX Security Expert z interfejsu GUI. Program Program AIX Security Expert przeanalizuje działający system w stanie zaufanym. W zależności od wybranej opcji bezpieczeństwa, program Program AIX Security Expert włączy ochronę przed skanowaniem portów, kontrolę, zablokuje porty sieciowe nieużywane przez aplikacje biznesowe i inne usługi oraz ustawi wiele innych zabezpieczeń. Po ponownym przetestowaniu z zastosowanymi konfiguracjami zabezpieczeń system jest gotowy do wdrożenia w środowisku produkcyjnym. Pliki XML programu Program AIX Security Expert definiujące strategię bezpieczeństwa lub konfigurację tego systemu można łatwo zaimplementować, tworząc taką samą konfigurację w podobnych systemach w przedsiębiorstwie.

Więcej informacji na temat wzmacniania zabezpieczeń można znaleźć w publikacji specjalnej NIST o numerze 800-70 zatytułowanej: NIST Security Configurations Checklist Program for IT Products.

Model SbD (Secure by Default)

Model Secure By Default (SbD) opiera się na koncepcji zainstalowania minimalnego zestawu oprogramowania w bezpiecznej konfiguracji.

Opcja instalacji systemu AIX Secure by Default (SbD) instaluje minimalną wersję zestawów plików serwera i klienta protokołu TCP, z wyłączeniem wrażliwych komend i plików. Częścią tej instalacji są zestawy plików **bos.net.tcp.client** i **bos.net.tcp.server**, zawierające wszystkie komendy i pliki poza aplikacjami umożliwiającymi transmisję haseł w sieci w formacie tekstu jawnego, takimi jak **telnet** i **ftp**. Ponadto z tych zestawów plików są wykluczane aplikacje, które można wykorzystać, takie jak **rsh**, **rcp** i **sendmail**.

Końcowym zautomatyzowanym procesem instalacji SbD jest narzucenie w programie Program AIX Security Expert ustawień konfiguracji zabezpieczeń najwyższego poziomu. Można to osiągnąć, uruchamiając komendę **aixpert** ze skryptu `/etc/firstboot`: `/usr/sbin/aixpert -f /etc/security/aixpert/core/SbD.xml -p 2>/etc/security/aixpert/log/firstboot.log`

Aby komputer ustawić w trybie innym niż SbD, można zmienić zmienną ODM *SbD_STATE* na sbd_disable, zainstalować ponownie zestawy plików **bos.net.tcp.client** i **bos.net.tcp.server**, a następnie użyć programu Program AIX Security Expert do ustawienia systemu w domyślnym poziomie zabezpieczeń.

Nie ma możliwości uzyskania systemu zainstalowanego w modelu SbD za pomocą instalacji migracyjnej lub zachowującej. Model SbD jest oddzielną ścieżką menu instalacji.

Uwaga: Gdy aktualizowany jest system w trybie SbD z pakietem serwisowym, zaktualizowany system nie będzie w trybie SbD po wykonaniu aktualizacji.

Możliwe jest uzyskanie bezpiecznie skonfigurowanego systemu bez korzystania z opcji instalacji SbD. Na przykład można skonfigurować w zwykłej instalacji opcje zabezpieczeń programu Program AIX Security Expert poziomu wysokiego, średniego lub niskiego.

Różnicę między systemem zainstalowanym według modelu SbD a instalacją zwykłą z konfiguracją zabezpieczeń programu Program AIX Security Expert wysokiego poziomu najlepiej ilustruje sprawdzenie komendy **telnet**. W obu przypadkach komenda **telnet** jest wyłączona. W instalacji SbD aplikacja lub plik binarny **telnet** nigdy nie jest instalowany w systemie.

Gdy używana jest instalacja SbD, poniższe usługi albo nie zostały zainstalowane w systemie w czasie instalacji, albo są wyłączone. Gdy niektóre z tych usług nie są zainstalowane w systemie, nie ma możliwości dostępu do nich ani uruchomienia tych komend w systemie. Gdy komendy te są potrzebne, nie należy używać opcji instalacji SbD. Ponadto, jeśli jakiekolwiek skrypty, programy zdalne lub zależne zestawy plików wymagają tych komend i programów, również nie należy używać opcji instalacji SbD.

Usługa	Program	Argumenty
bootps	/usr/sbin/bootpd	bootpd /etc/bootp
comsat	/usr/sbin/comsat	comsat
exec	/usr/sbin/rexecd	rexecd
finger	/usr/sbin/fingerd	fingerd
ftp	/usr/sbin/ftpd	ftpd
instsrv	/u/netinst/bin/instsrv	instsrv -r /tmp/netinstalllog /u/netinst/scripts
login	/usr/sbin/rlogind	rlogind
netstat	/usr/bin/netstat	netstat -f inet
ntalk	/usr/sbin/talkd	talkd
pcnfsd	/usr/sbin/rpc.pcnfsd	pcnfsd
rexd	/usr/sbin/rpc.rexd	rexd
rquotad	/usr/sbin/rpc.rquotad	rquotad
rstatd	/usr/sbin/rpc.rstatd	rstatd
rusersd	/usr/lib/netsvc/rusers/rpc.rusersd	rusersd
rwalld	/usr/lib/netsvc/rwall/rpc.rwalld	rwalld
shell	/usr/sbin/rshd	rshd
sprayd	/usr/lib/netsvc/spray/rpc.sprayd	sprayd
systat	/usr/bin/ps	ps -ef
talk	/usr/sbin/talkd	talkd
telnet	/usr/sbin/telnetd	telnetd -a
tftp	/usr/sbin/tftpd	tftpd -n
uucp	/usr/sbin/uucpd	uucpd

Rozszerzona strategia bezpieczeństwa przez LDAP

Protokół LDAP może służyć do dystrybucji plików konfiguracyjnych XML programu Program AIX Security Expert. Program Program AIX Security Expert umożliwia kopiowanie konfiguracji zabezpieczeń pomiędzy systemami. Umożliwia to utrzymanie identycznych konfiguracji zabezpieczeń w podobnych systemach. Taka spójność może zmniejszyć zagrożenia bezpieczeństwa.

Zalecane jest skonfigurowanie przy pomocy programu Program AIX Security Expert jednego systemu, ustawienie poziomu zabezpieczeń zgodnie ze strategiami bezpieczeństwa korporacji i skonfigurowanie środowiska, w którym będzie działał ten system. Taka konfiguracja jest przechwytywana do pliku `/etc/security/aixpert/core/appliedaixpert.xml`. Plik ten można następnie przenieść do

skonfigurowanego i zaufanego serwera LDAP. Inne systemy połączone z tym serwerem wykryją automatycznie ten plik konfiguracyjny XML za pomocą komendy **aixpertldap**.

Dowolny istniejący serwer LDAP można zaktualizować schematem aixpert, aby rozsyłać pliki XML konfiguracji aixpert do każdego połączonego klienta. Jeśli serwer LDAP nie ma zaktualizowanego schematu aixpert, należy zaktualizować schemat aixpert na serwerze LDAP komendą: `ldapmodify -c -D <bindDN> -w <bindPwd> -i /etc/security/ldap/sec.ldif`. Po zaktualizowaniu serwera LDAP schematem aixpert klienty mogą umieszczać swoje pliki konfiguracyjne XML na serwerze LDAP, korzystając z opcji -u komendy **aixpertldap**. Te pliki konfiguracyjne wymagają aktualizacji ręcznej.

Uwaga: Opcja wykorzystuje istniejący zaufany model LDAP. Użytkownicy z uprawnieniami zapisu na serwerze LDAP mogą modyfikować dane przesłane przez użytkowników innych maszyn. Podobnie, jeśli na kliencie LDAP jest słaby punkt zabezpieczeń, może on zostać wykorzystany do poznania statusu bezpieczeństwa innych klientów LDAP, ponieważ zostaną odczytane pliki konfiguracyjne LDAP programu Program AIX Security Expert powiązane z klientem.

Na przykład plik `appliedaixpert.xml` może być zapisany na serwerze LDAP pod nazwą **BranchOfficeSecurityProfile**. Albo zawierający inną konfigurację plik `appliedaixpert.xml` może zostać zapisany pod nazwą **InternetDirectAttachedSystemsProfile**. Jeśli inne systemy połączone z serwerem LDAP skonfigurowano, korzystając z programu Program AIX Security Expert, te profile bezpieczeństwa są przedstawiane jako opcje menu. Opcje te dają administratorowi systemu wybór profilu bezpieczeństwa najlepiej pasującego w danym środowisku i zgodnego z wytycznymi strategii bezpieczeństwa danej korporacji.

Program Program AIX Security Expert jest następnie używany do zabezpieczenia systemu. Pełna lista ustawień konfiguracji bezpieczeństwa zaimplementowanych w systemie jest przechwytywana do pliku `/etc/security/aixpert/core/appliedaixpert.xml`. Plik ten jest strategią bezpieczeństwa dla tego systemu. Strategia bezpieczeństwa jest porównywana w momencie użycia opcji Check Security (Sprawdź poziom bezpieczeństwa) programu Program AIX Security Expert. Można ją również skopiować i użyć w innych systemach, zapewniając spójność zabezpieczeń systemów w całym środowisku informatycznym. Są dwa sposoby kopiowania strategii bezpieczeństwa do innych systemów, ręcznie lub przez LDAP.

Program AIX Security Expert - kopiowanie strategii bezpieczeństwa

Program Program AIX Security Expert umożliwia kopiowanie strategii bezpieczeństwa pomiędzy systemami.

Program Program AIX Security Expert można uruchomić w jednym systemie i zastosować tę samą strategię bezpieczeństwa w innych systemach. Na przykład użytkownik Robert chce zastosować program Program AIX Security Expert w sześciu swoich systemach AIX. Stosuje on w systemie A ustawienia zabezpieczeń wysokiego, średniego lub niskiego poziomu bezpieczeństwa, bądź ustawienia standardowe systemu AIX. Testuje zgodność tego systemu z używanym środowiskiem. Jeśli satysfakcjonują go zastosowane ustawienia, może użyć tych samych w innych systemach AIX. Przenosi ustawienia z systemu A na system, na którym chce zastosować te same ustawienia zabezpieczeń, kopiując plik `/etc/security/aixpert/core/appliedaixpert.xml` z systemu A na inny.

Uwaga: Nie należy kopiować tego pliku do tego samego katalogi i z tą samą nazwą pliku w innym systemie, ponieważ komenda **aixpert** nadpisze plik `/etc/security/aixpert/core/appliedaixpert.xml` implementujący strategię bezpieczeństwa.

Należy skopiować strategię bezpieczeństwa systemu A do katalogu `/etc/security/aixpert/custom/`. Dzięki temu w innym system będzie można przeglądać strategię bezpieczeństwa systemu A i zastosować ją za pomocą interfejsu GUI programu Program AIX Security Expert do zarządzania systemem lub bezpośrednio, przy użyciu komendy **aixpert**.

Na przykład, jeśli strategia bezpieczeństwa komputera A, appliedaixpert.xml, została umieszczona w innych systemach pod nazwą `/etc/security/aixpert/custom/`*`StrategiaA`*, komenda `aixpert -f /etc/security/aixpert/custom/`*`StrategiaA`* natychmiast zastosuje tę strategię bezpieczeństwa, a system będzie miał taką samą konfigurację zabezpieczeń, jak komputer A. Ponadto, gdy strategia bezpieczeństwa komputera A znajduje się w tym katalogu, jest widziana przez konsole zarządzania systemem innych systemów i może być przez nie stosowana dzięki użyciu ścieżki programu Aix Security Expert -> Przegląd i zadania -> Dostosowane opcje -> StrategiaA.

Konfigurowalna strategia bezpieczeństwa ze zdefiniowanymi przez użytkownika regułami XML programu AIX Security Expert

Do skonfigurowania unikalnych strategii bezpieczeństwa można użyć plików XML.

Program Program AIX Security Expert rozpoznaje te pliki XML dynamicznie. Wszystkie tworzone niestandardowe pliki XML strategii bezpieczeństwa należy umieszczać w katalogu `/etc/security/aixpert/custom/` wraz z plikiem opisu. Gdy program Program AIX Security Expert jest uruchamiany z graficznego interfejsu konsoli, bogaty zestaw graficznych opcji XML w pliku DTD komendy aixpert będzie zrealizowany w pełni.

Plik DTD jest następujący:

```
<?xml version='1.0'?>

<!--START-->

<!ELEMENT AIXPertSecurityHardening (AIXPertEntry+)>

<!-- AIXPertEntry powinien zawierać tylko jedną instancję poniższych elementów. -->

<!ELEMENT AIXPertEntry (AIXPertRuleType,
        AIXPertDescription, AIXPertPrereqList, AIXPertCommand,
        AIXPertArgs,AIXPertGroup)>

<!-- Nazwa AIXPertEntry musi być unikalna. -->

<!ATTLIST AIXPertEntry
    name ID #REQUIRED
    function CDATA ""
>

<!ELEMENT AIXPertRuleType EMPTY>
<!ATTLIST AIXPertRuleType    type (LLS|MLS|HLS|DLS|SCBPS|Prereq) "DLS">
<!ELEMENT AIXPertDescription (#PCDATA)>
<!ELEMENT AIXPertPrereqList (#PCDATA)>
<!ELEMENT AIXPertCommand (#PCDATA)>
<!ELEMENT AIXPertArgs (#PCDATA)*>
<!ELEMENT AIXPertGroup (#PCDATA)*>
```

Nazwa AIXPertEntry jest nazwą unikalną w pliku XML. Nazwa ta będzie nazwą wybieralnego przycisku graficznego podczas przeglądania tego pliku z konsoli systemu przez ścieżkę programu Aix Security Expert -> Przegląd i zadania -> Dostosowane opcje -> <xml file=""></xml>.

<!ELEMENT AIXPertRuleType EMPTY>
Ten plik XML należy podać jako niestandardowy.

<!ATTLIST AIXPertRuleType type (LLS|MLS|HLS|DLS|SCBPS|Prereq|Custom) "DLS"
Ten plik XML należy podać jako niestandardowy.

<!ELEMENT AIXPertDescription (#PCDATA)>
Podczas przeglądania przy użyciu wyżej wspomnianego interfejsu graficznego tekst opisu jest wyświetlany jako okno wywoływane po umieszczeniu kursora myszy na tym przycisku.

<!ELEMENT AIXPertPrereqList (#PCDATA)>
Do tej reguły można wybrać regułę wymagania wstępnego. Reguła wymagania wstępnego musi zwrócić 0, aby komenda aixpert zaimplementowała tę regułę. Jeśli plik XML jest przeglądany w interfejsie graficznym, ta reguła będzie wyświetlona w szarym kolorze, o ile nie zostanie spełniona reguła wymagania wstępnego. Typem AIXPertRuleType reguły wymagania wstępnego musi być 'Prereq'.

Pole AIXPertDescription reguły wymagania wstępnego powinno zawierać opis warunków spełnienia tej reguły. Jeśli reguła niestandardowa jest szara z powodu niespełnienia jednej z reguł wymagań wstępnych, wyświetlane jest okno wywoływane reguły wymagania wstępnego, zawierające wyjaśnienie, jakie działania musi podjąć użytkownik, aby spełnić warunki wstępne.

<!ELEMENT AIXPertCommand (#PCDATA)>
Ten element musi zawierać pełną ścieżkę i komendę, którą komenda aixpert wykona dla tej reguły bezpieczeństwa, np. `/usr/bin/ls`.

<!ELEMENT AIXPertArgs (#PCDATA)*>
Ten element musi zawierać wszystkie argumenty dla powyższej komendy, np. -l.

<!ELEMENT AIXPertGroup (#PCDATA)*>
Można zgrupować zestaw reguł aixpert wyświetlanych w graficznym interfejsie. Na przykład całemu zestawowi reguł można nadać nazwę AIXPertGroup "Zabezpieczenia sieci".

Rygorystyczne sprawdzanie pod kątem słabych haseł

Ta opcja systemu AIX podczas zmiany hasła sprawdza je pod kątem możliwości odgadnięcia. Po zaznaczeniu tej opcji w programie Program AIX Security Expert, gdy użytkownik wybiera lub zmienia hasło, wykonywane jest dodatkowe sprawdzenie hasła. Sprawdzenie takie chroni przed użyciem słów ze słownika języka angielskiego i najczęstszych imion używanych w Stanach Zjednoczonych, zebranych w najnowszym spisie ludności USA.

Cele kontroli COBIT obsługiwane przez program AIX Security Expert

Oprócz wysokich, średnich, niskich, domyślnych i zaawansowanych opcji bezpieczeństwa systemu AIX, program Program AIX Security Expert obsługuje poziom sprawdzonych procedur bezpieczeństwa SOB-COBIT.

Kongres Stanów Zjednoczonych uchwalił ustawę 'Sarbanes-Oxley Act of 2002', aby ochronić inwestorów, zwiększając dokładność i wiarygodność informacji finansowych ujawnianych przez korporacje. Opcja kontroli celów COBIT pomaga administratorom systemów w konfigurowaniu, przekształcaniu i kontrolowaniu systemów informatycznych pod kątem zgodności z tą ustawą. Asystent konfiguracji SOX jest dostępny z wiersza komend aixpert. Opcja ta wspiera konfigurację zgodną z sekcją 404 ustawy Sarbanes-Oxley Act, natomiast asystent konfiguracji SOX programu AIX Security Expert automatycznie implementuje ustawienia bezpieczeństwa związane ze sprawdzonymi procedurami COBIT dla sekcji 404 ustawy SOX o kontroli wewnętrznej. Ponadto program AIX Security Expert udostępnia opcję kontroli SOX, zgłaszającą audytorowi, czy system jest już skonfigurowany w odpowiedni sposób. Umożliwia automatyczne skonfigurowanie systemu i pomaga w uzyskaniu zgodności z informatyczną częścią ustawy SOX oraz w zautomatyzowaniu procesu kontroli.

Ustawa SOX nie daje wytycznych dotyczących sposobu uzyskania przez strukturę informatyczną zgodności z sekcją 404, przemysł informatyczny skupia się na istniejących zarządzeniach przedstawionych szczegółowo na stronie www.isaca.org/. Są to dokładniej zarządzenia informatyczne objęte metodyką Control Objectives for Information and related Technology (COBIT).

Program Program AIX Security Expert obsługuje następujące cele kontroli:

- Wymuszenie strategii dotyczącej haseł
- Raporty naruszeń i działań zabezpieczeń
- Zapobieganie złośliwemu i nieuprawnionemu oprogramowaniu oraz wykrywanie i usuwanie go
- Architektura firewall i połączenia z sieciami publicznymi

Program Program AIX Security Expert nie obsługuje wszystkich atrybutów podanych w każdym celu kontroli. Obsługiwane atrybuty i odpowiadające im cele kontroli zebrano w poniższych tabelach:

Wymuszenie strategii dotyczącej haseł

Opis	Ustawienie zabezpieczeń
Maksymalny wiek hasła	maxage=13
Wymuszaj historię haseł	histsize=20
Minimalny wiek hasła	minage=1
Minimalna długość hasła	minlen=8
Zawiera co najmniej 6 znaków	Minalpha=6

Opis	Ustawienie zabezpieczeń
Podobieństwo do starego hasła	mindiff=4
Liczba dni przed ostrzeżeniem o utracie ważności hasła	pwdwarntime=14

Raport naruszeń i działań zabezpieczeń

Opis	Ustawienie zabezpieczeń	Uwagi
Kontrola włączona	tak	
Bez możliwości bezpośredniego logowania się jako użytkownik root	tak	
Włączona kontrola eskalacji uprawnień	tak	Program AIXpert wykorzystuje zdarzenie kontrolowane USER_SU. Należy się upewnić, że jest ono włączone.

Wykrywanie i usuwanie złośliwego oprogramowania

Program Program AIX Security Expert korzysta z opcji wykonywania zaufanego oprogramowania systemu AIX, sprawdzając, czy oprogramowanie nie zostało przez nikogo sfałszowane. Komenda **trustchk** sprawdza spójność obiektów zarejestrowanych w bazie danych zaufanego oprogramowania.

Konfigurowanie firewalla

Program Program AIX Security Expert włącza IPSec oraz reguły filtrowania w celu zapobiegania skanowaniu portów. Blokowane porty są wymienione w poniższej tabeli:

Usługa	Opis
Tcp/11, udp/11	Systat
Tcp/13, udp/13	Daytime
(RFC 867) Tcp/19, udp/19	Generator znaków
Tcp/25	SMTP (Simple Mail Transfer)
Tcp/43, udp/43	Whois (pseudonim)
Tcp/63, udp/63	Whois++
Tcp/67, udp/67	Serwer Bootstrap Protocol (bootps)
Tcp/68, udp/68	Klient Bootstrap Protocol (bootpc)
Tcp/69, udp/69	Proste przesyłanie plików
(tftp) Tcp/79, udp/79	Finger
Tcp/87	Private Terminal Link
Tcp/110	Protokół POP3
Udp/111	SUN Remote Procedure Call
Tcp/113	Usługa uwierzytelniania (auth)
Udp/123	NTP (Network Time Protocol)
Udp/161	SNMP

Usługa	Opis
Udp/162	SNMPTRAP
Tcp/194	Protokół IRC (Internet Relay Chat Protocol)
Tcp/443	Protokół HTTP over TLS/SSL
Tcp/511	PassGo
Tcp/514	Cmd (powłoka)
Tcp/520	Extended file name server (efs)
Tcp/540	Uucpd (uucp)
Tcp/546	Klient DHCPv6
Tcp/547	Serwer DHCPv6
Tcp/555	Dsf
tcp/559	TEEDTAP
tcp/593	HTTP RPC Ep Map
udp/635	RLS Dbase
tcp/666	Mdqs
tcp/777	Multiling HTTP
tcp/901	SNMPNSMERES
tcp/902	IDEAFARM-CHAT
tcp/903	IDEAFARM-CATCH
tcp/1024	Zarezerwowany

Stosowanie celów kontroli COBIT za pomocą programu AIX Security Expert

Aby zastosować w systemie poziom SCBPS, można użyć komendy **aixpert** –l s. Aby wygenerować dziennik kontroli, należy włączyć zdarzenie **AIXpert_apply**. Wszystkie niepowodzenia (zarówno związane z wymaganiami wstępnymi, jak i z instalacją) są wysyłane do standardowego wyjścia błędów (**stderr**) i do podsystemu kontrolującego, jeśli jest włączony.

Sprawdzanie zgodności z metodyką SOX-COBIT, opcja kontroli i kontroli wstępnej

Do sprawdzenia zgodności systemu z metodyką SOX-COBIT można użyć komendy **aixpert** –c –l s. Program Program AIX Security Expert sprawdza tylko zgodność z obsługiwanymi celami kontroli. Wszystkie naruszenia znalezione podczas sprawdzania są zgłaszane. Domyślnie są one wysyłane do standardowego wyjścia błędów (**stderr**).

Tej samej komendy (**aixpert** –c –l s) można również użyć do wygenerowania raportu kontroli zgodności z metodyką SOX-COBIT. Aby wygenerować raport kontroli, skonfiguruj i włącz podsystem kontrolujący. Upewnij się, że włączono zdarzenie kontrolowane **AIXpert_check**. Po skonfigurowaniu podsystemu kontrolującego ponownie uruchom komendę **aixpert** –c –l s. Komenda ta generuje protokół kontroli dla każdego celu kontroli, którego sprawdzenie zakończyło się niepowodzeniem. Pole **Status** protokołu kontroli będzie oznaczone **failed** (nie powiodło się). Protokół zawiera również przyczynę niepowodzenia, którą można przejrzeć po podaniu opcji -v komendy **auditpr**.

Dodanie opcji –p do komendy **aixpert** –c –l s powoduje ujęcie w raporcie kontroli również tych celów kontroli, których sprawdzenie zakończyło się pomyślnie. Pozycje te mają w polu statusu wpisaną wartość **Ok**.

Komenda **aixpert** -c -l s -p może służyć do wygenerowania szczegółowego raportu kontroli zgodności SOX-COBIT.

W zależności od użycia opcji –p, raport będzie zawierał rekord podsumowania. Rekord podsumowania zawiera informacje o liczbie przetworzonych reguł, liczbie reguł, których sprawdzanie zakończyło się niepowodzeniem (istniejące niezgodności) i poziom bezpieczeństwa, z którym porównywany jest sprawdzany system (w tym przypadku powinien to być poziom SCBPS).

AIX Security Expert - reguły dotyczące strategii haseł

Program Program AIX Security Expert udostępnia specjalne reguły dotyczące strategii haseł.

Bardzo dobre strategie haseł stanowią ważny element bezpiecznego systemu. Strategie haseł zapewniają, że hasła są trudne do odgadnięcia (zawierają odpowiednią kombinację znaków alfanumerycznych, cyfr i znaków specjalnych), tracą ważność w regularnych odstępach czasu, a po utracie ważności nie można ich ponownie wykorzystywać. Poniższa tabel zawiera reguły strategii haseł dla każdego ustawienia dotyczącego bezpieczeństwa.

Tabela 20. Program AIX Security Expert - reguły dotyczące strategii haseł

Etykieta przycisku	**Definicja**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Minimum number of characters (Minimalna liczba znaków)	Ustawia odpowiednią wartość atrybutu **mindiff** w pliku `/etc/security/user`. Określa ona minimalną liczbę znaków składających się na nowe hasło, które nie występowały w starym.	**Wysoki poziom bezpieczeństwa** 4 **Średni poziom bezpieczeństwa** 3 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Minimum age for password (Minimalny wiek hasła)	Ustawia odpowiednią wartość atrybutu **minage** w pliku `/etc/security/user`. Określa ona minimalną liczbę tygodni, które muszą upłynąć, zanim hasło będzie można zmienić.	**Wysoki poziom bezpieczeństwa** 1 **Średni poziom bezpieczeństwa** 4 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 20. Program AIX Security Expert - reguły dotyczące strategii haseł (kontynuacja)			
Etykieta przycisku	**Definicja**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Maximum age for password (Maksymalny wiek hasła)	Ustawia odpowiednią wartość atrybutu **maxage** w pliku `/etc/security/user`. Określa ona maksymalną liczbę tygodni, które muszą upłynąć, zanim hasło będzie można zmienić.	**Wysoki poziom bezpieczeństwa** 13 **Średni poziom bezpieczeństwa** 13 **Niski poziom bezpieczeństwa** 52 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Minimum length for password (Minimalna długość hasła)	Ustawia odpowiednią wartość atrybutu **minlen** w pliku `/etc/security/user`. Określa ona minimalną długość hasła.	**Wysoki poziom bezpieczeństwa** 8 **Średni poziom bezpieczeństwa** 8 **Niski poziom bezpieczeństwa** 8 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Minimum number of alphabetic characters (Minimalna liczba znaków alfabetu)	Ustawia odpowiednią wartość atrybutu **minalpha** w pliku `/etc/security/user`. Określa ona minimalną liczbę znaków alfabetu, które muszą wystąpić w haśle.	**Wysoki poziom bezpieczeństwa** 2 **Średni poziom bezpieczeństwa** 2 **Niski poziom bezpieczeństwa** 2 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 20. Program AIX Security Expert - reguły dotyczące strategii haseł (kontynuacja)

Etykieta przycisku	Definicja	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Password reset time (Czas do zresetowania hasła)	Ustawia odpowiednią wartość atrybutu **histexpire** w pliku `/etc/security/user`. Określa ona liczbę tygodni, które muszą upłynąć, zanim hasło będzie można zresetować.	Do atrybutu **histexpire** można przypisać wartość całkowitą z zakresu od 0 do 260. Do atrybutu **histexpire** można przypisać wartość 26, przez co użytkownik nie będzie w stanie ponownie wykorzystać hasła przez 6 miesięcy.	Tak
Maximum times a char can appear in a password (Maksymalna liczba wystąpień jednego znaku w haśle)	Ustawia odpowiednią wartość atrybutu **maxrepeats** w pliku `/etc/security/user`. Określa ona maksymalną liczbę wystąpień jednego znaku w haśle.	**Wysoki poziom bezpieczeństwa** 2 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 8	Tak
Password reuse time (Czas przed ponownym wykorzystaniem hasła)	Ustawia odpowiednią wartość atrybutu **histsize** w pliku `/etc/security/user`. Określa ona liczbę poprzednich haseł, których użytkownik nie może ponownie wykorzystać.	**Wysoki poziom bezpieczeństwa** 20 **Średni poziom bezpieczeństwa** 4 **Niski poziom bezpieczeństwa** 4 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 20. Program AIX Security Expert - reguły dotyczące strategii haseł (kontynuacja)			
Etykieta przycisku	**Definicja**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Time to change password after the expiration (Czas do zmiany hasła po utracie przez nie ważności)	Ustawia odpowiednią wartość atrybutu **maxexpired** w pliku `/etc/security/user`. Określa ona maksymalną liczbę tygodni po czasie ustalonym wartością atrybutu **maxage**, po upłynięciu których użytkownik będzie mógł zmienić nieważne hasło.	**Wysoki poziom bezpieczeństwa** 2 **Średni poziom bezpieczeństwa** 4 **Niski poziom bezpieczeństwa** 8 **Ustawienia standardowe systemu AIX** -1	Tak
Minimum number of non-alphabetic characters (Minimalna liczba znaków spoza alfabetu)	Ustawia odpowiednią wartość atrybutu **minother** w pliku `/etc/security/user`. Określa ona minimalną liczbę znaków spoza alfabetu, które muszą wystąpić w haśle.	**Wysoki poziom bezpieczeństwa** 2 **Średni poziom bezpieczeństwa** 2 **Niski poziom bezpieczeństwa** 2 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Password expiration warning time (Czas wygenerowania ostrzeżenia o utracie ważności przez hasło)	Ustawia odpowiednią wartość atrybutu **pwdwarntime** w pliku `/etc/security/user`. Określa ona liczbę dni przed utratą ważności przez hasło, kiedy system generuje ostrzeżenie o konieczności jego zmiany.	**Wysoki poziom bezpieczeństwa** 5 **Średni poziom bezpieczeństwa** 14 **Niski poziom bezpieczeństwa** 5 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

AIX Security Expert - definicje użytkowników, grup, systemu i haseł

Program Program AIX Security Expert umożliwia wykonywanie pewnych działań na definicjach użytkowników, grup i haseł.

Tabela 21. Program AIX Security Expert - definicje użytkowników, grup, systemu i haseł

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Check group definitions (Sprawdź definicje grup)	Powoduje sprawdzenie poprawności definicji grup. Uruchamia następującą komendę naprawiającą i zgłaszającą błędy: `% grpck -y ALL`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Brak wpływu	Nie
TCB update (Aktualizacja TCB)	Powoduje sprawdzenie i aktualizację TCB przy użyciu komendy **tcbck**. Uruchamia następującą komendę: `% tcbck -y ALL` **Uwaga:** Jeśli baza TCB jest wymagana w używanym systemie, ta reguła nie powiedzie się, gdy baza TCB nie jest włączona. Reguła wymagania wstępnego (prereqtcb) także nie powiedzie się i zostanie wygenerowane ostrzeżenie. **Wymaganie wstępne**: Baza TCB musi być wybrana podczas instalowania systemu.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Tak	Nie

Check file definitions (Sprawdź definicje plików)	Powoduje sprawdzenie i naprawienie bazy plików `/etc/objrepos/inventory` przy pomocy komendy **sysck**:
	`% sysck -i -f \`
	`/etc/security/sysck.cfg.rte`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Tak
		Ustawienia standardowe systemu AIX
		Brak wpływu
			Nie

Tabela 21. Program AIX Security Expert - definicje użytkowników, grup, systemu i haseł (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Check password definitions (Sprawdź definicje haseł)	Powoduje sprawdzenie poprawności definicji haseł. Uruchamia następującą komendę naprawiającą i zgłaszającą błędy: `% pwdck -y ALL`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Brak wpływu	Nie
Check user definitions (Sprawdź definicje użytkowników)	Powoduje sprawdzenie poprawności definicji użytkowników. Uruchamia następującą komendę naprawiającą i zgłaszającą błędy: `% usrck -y ALL`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Brak wpływu	Nie

AIX Security Expert - zalecenia dotyczące strategii logowania

Program Program AIX Security Expert udostępnia specjalne ustawienia dotyczące strategii logowania.

Uwaga: Aby uniknąć anonimowości w przypadku czynności związanych z bezpieczeństwem, które muszą być wykonywane przez użytkownika root, zaleca się, aby każdy użytkownik logował się najpierw za pomocą swojego własnego identyfikatora, a dopiero potem wykonywał *komendę* **su**, przełączając się na konto użytkownika root, a nie logował się od razu jako użytkownik root. Pozwoli to systemowi powiązać działania podejmowane przy użyciu konta użytkownika root z konkretnymi użytkownikami, gdy wielu z nich zna hasło użytkownika root.

Tabela 22. Program AIX Security Expert - zalecenia dotyczące strategii logowania

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Interval between unsuccessful logins (Odstęp czasu między nieudanymi logowaniami)	Ustawia odpowiednią wartość atrybutu **logininterval** w pliku `/etc/security/login.cfg`. Określa ona w sekundach przedział czasu, podczas którego wystąpienie pewnej liczby nieudanych prób logowania na porcie spowoduje wyłączenie portu. Na przykład, jeśli atrybut **logininterval** ma wartość 60, a wartością atrybutu **logindisable** jest 4, konto zostanie zablokowane, kiedy w ciągu jednej minuty wystąpią cztery nieudane próby logowania.	**Wysoki poziom bezpieczeństwa** 300 **Średni poziom bezpieczeństwa** 60 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Number of login attempts before locking the account (Liczba prób logowania przed zablokowaniem konta)	Ustawia odpowiednią wartość atrybutu **loginretries** w pliku `/etc/security/user`. Określa ona liczbę kolejnych prób logowania przypadających na konto, zanim zostanie ono zablokowane. Nie należy jej określać w stosunku do użytkownika root.	**Wysoki poziom bezpieczeństwa** 3 **Średni poziom bezpieczeństwa** 4 **Niski poziom bezpieczeństwa** 5 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Remote root login (Zdalne logowanie na konto użytkownika root)	Zmienia wartość atrybutu **rlogin** w pliku `/etc/security/user`. Określa ona, czy w systemie dozwolone jest zdalne logowanie na konto użytkownika root.	**Wysoki poziom bezpieczeństwa** Fałsz **Średni poziom bezpieczeństwa** Fałsz **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Prawda	Tak

Tabela 22. Program AIX Security Expert - zalecenia dotyczące strategii logowania (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Re-enable login after locking (Włącz logowanie ponownie po zablokowaniu)	Ustawia odpowiednią wartość atrybutu **loginreenable** w pliku `/etc/security/login.cfg`. Określa ona w sekundach czas, po upłynięciu którego port zostaje odblokowany po tym, jak został zablokowany przy użyciu atrybutu **logindisable**.	**Wysoki poziom bezpieczeństwa** 360 **Średni poziom bezpieczeństwa** 30 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Disable login after unsuccessful login attempts (Wyłącz logowanie po nieudanych próbach zalogowania)	Ustawia odpowiednią wartość atrybutu **logindisable** w pliku `/etc/security/login.cfg`. Określa ona liczbę nieudanych prób logowania na porcie, po wystąpieniu których port zostanie zablokowany.	**Wysoki poziom bezpieczeństwa** 10 **Średni poziom bezpieczeństwa** 10 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Login timeout (Limit czasu logowania)	Ustawia odpowiednią wartość atrybutu **logintimeout** w pliku `/etc/security/login.cfg`. Określa ona dozwolony czasu na wpisanie hasła.	**Wysoki poziom bezpieczeństwa** 30 **Średni poziom bezpieczeństwa** 60 **Niski poziom bezpieczeństwa** 60 **Ustawienia standardowe systemu AIX** 60	Tak

Tabela 22. Program AIX Security Expert - zalecenia dotyczące strategii logowania (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Delay between unsuccessful logins (Opóźnienie między nieudanymi logowaniami)	Ustawia odpowiednią wartość atrybutu **logindelay** w pliku `/etc/security/login.cfg`. Określa ona w sekundach opóźnienie pomiędzy nieudanymi logowaniami. Po każdym nieudanym logowaniu dodawane jest dodatkowe opóźnienie. Na przykład, jeśli atrybut **logindelay** ma wartość 5, po pierwszym nieudanym logowaniu terminal będzie czekał przez pięć sekund na następne żądanie. Po drugim nieudanym logowaniu terminal będzie czekał 10 sekund (2*5), a po trzecim nieudanym logowaniu terminal będzie czekał 15 sekund (3*5).	**Wysoki poziom bezpieczeństwa** 10 **Średni poziom bezpieczeństwa** 4 **Niski poziom bezpieczeństwa** 5 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Local login (Logowanie lokalne)	Zmienia wartość atrybutu **login** w pliku `/etc/security/user`. Określa ona, czy w systemie dozwolone jest logowanie z konsoli na konto użytkownika root.	**Wysoki poziom bezpieczeństwa** Fałsz **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Prawda	Tak

AIX Security Expert - zalecenia dotyczące strategii kontrolowania

Program Program AIX Security Expert udostępnia specjalne ustawienia dotyczące strategii kontrolowania.

Podobnie jak przy innych ustawieniach zabezpieczeń, także w przypadku kontrolowania binarnego, zanim zostaną zastosowane reguły kontrolowania wysokiego, średniego lub niskiego poziomu bezpieczeństwa, konieczne jest sprawdzenie zgodności z regułami analizy (sprawdzenie wymagań wstępnych). Kontrolowanie binarne wymaga wcześniejszego spełnienia następujących reguł analizy:

1. Wymaganiem wstępnym jest sprawdzenie, czy kontrola nie jest przeprowadzana w danej chwili. Jeśli kontrola jest w toku, oznacza to, że została wcześniej skonfigurowana i programowi Program AIX Security Expert nie wolno zmieniać istniejącej konfiguracji ani procedury.
2. W grupie woluminów, która jest udostępniana automatycznie, lub w istniejącym systemie plików `/audit` musi być przynajmniej 100 megabajtów wolnego miejsca.

Jeśli wymienione powyżej wymagania wstępne są spełnione, a w programie Program AIX Security Expert wybrano opcję kontrolowania, program Program AIX Security Expert skonfiguruje i włączy kontrolowanie w systemie w opisany poniżej sposób. Przycisk **Włącz binaudit** w programie Program AIX Security Expert ustawia strategię kontroli. Kontrolowanie musi być włączone w systemie.

1. Przed uruchomieniem kontrolowania należy utworzyć i podłączyć system plików JFS `/audit`. System plików musi mieć wielkość przynajmniej 100 megabajtów.

2. Kontrolowanie należy uruchomić w trybie binarnym. Plik `/etc/security/audit/config` należy skonfigurować w następujący sposób:

```
start:
            binmode = on
            streammode = off
bin:
            trail = /audit/trail
            bin1 = /audit/bin1
            bin2 = /audit/bin2
            binsize = 10240
            cmds = /etc/security/audit/bincmds
     .
     .
     itd.
```

3. Należy dodać wpisy dotyczące kontrolowania użytkownika root i zwykłego użytkownika dla wysokiego, średniego i niskiego poziomu bezpieczeństwa.
4. Kontrolowanie musi być włączane w momencie restartu systemu w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
5. Nowi użytkownicy muszą mieć włączone kontrolowanie w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa. Prowadzi do tego dodanie wpisu `auditclasses` do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default`.
6. Należy dodać zadanie programu cron (**cronjob**) pozwalające uniknąć zapełnienia systemu plików `/audit`.

Reguła wycofywania kontroli musi ją zamykać i anulować włączanie w momencie restartu systemu.

Poniższa tabela zawiera wartości ustawiane przez program Program AIX Security Expert w przypadku działania **Enable binaudit** (Włącz kontrolowanie binarne):

Tabela 23. Wartości ustawiane przez program Program AIX Security Expert dla funkcji włączania kontroli binarnej

Wysoki poziom bezpieczeństwa	**Średni poziom bezpieczeństwa**	**Niski poziom bezpieczeństwa**	**Ustawienia standardowe systemu AIX**

Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania:
`Użytkownik root:`
`General`
`Src`
`Mail`
`Cron`
`Tcpip`
`Ipsec`
`Lvm`
`Zwykły użytkownik:`
`General`
`Src`
`Cron`
`Tcpip`
W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis:
`auditclasses=general,SRC,\`
`cron,tcpip`
	Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania:
	`Użytkownik root:`
	`General`
	`Src`
	`Tcpip`
	`Zwykły użytkownik:`
	`General`
	`Tcpip`
	W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis:
	`auditclasses=general,`
	`tcpip`
		Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania:
		`Użytkownik root:`
		`General`
		`Tcpip`
		`Zwykły użytkownik:`
		`General`
		W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis:
		`auditclasses=general`
			Plik /etc/security/audit/config zawiera następujący wpis:
			`default=login`
			Klasa kontroli login jest zdefiniowana w następujący sposób:
			`login = USER_SU,`
			`USER_Login,`
			`USER_Logout,`
			`TERM_Logout,`
			`USER_Exit`
			Uwaga: Opcja ustawień standardowych wyłącza kontrolę.

Tabela 23. Wartości ustawiane przez program Program AIX Security Expert dla funkcji włączania kontroli binarnej (kontynuacja)

Wysoki poziom bezpieczeństwa	Średni poziom bezpieczeństwa	Niski poziom bezpieczeństwa	Ustawienia standardowe systemu AIX
Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania: **Użytkownik root:** general src mail cron tcpip ipsec lvm aixpert ***Zwykły użytkownik:*** general src cron tcpip W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis: `auditclasses=general,SRC, cron,tcpip`	Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania: **Użytkownik root:** general src tcpip aixpert ***Zwykły użytkownik:*** general tcpip W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis: `auditclasses=general, tcpip`	Dla użytkownika root i zwykłego użytkownika dodane zostają następujące wpisy dotyczące kontrolowania: **Użytkownik root:** general tcpip aixpert ***Zwykły użytkownik:*** general W celu włączania kontrolowania dla nowo tworzonych użytkowników do sekcji użytkownika w pliku `/usr/lib/security/mkuser.default` zostaje dodany następujący wpis: `auditclasses=general`	Tak

Co godzinę należy uruchamiać zadanie programu cron sprawdzające wielkość systemu plików `/audit`. Kiedy równanie wolnego obszaru dla kontroli (Audit Freespace Equation) przyjmuje wartość true, należy wykonać działania związane z kopiowaniem zapisu kontrolnego (Audit Trail Copy Actions). Równanie wolnego obszaru dla kontroli zostaje zdefiniowane w celu zapewnienia, że system plików `/audit` nigdy nie jest pełny. Kiedy system plików `/audit` zostanie zapełniony, wykonane zostaną działania związane z kopiowaniem zapisu kontrolnego (wyłączenie kontrolowania, utworzenie kopii zapasowej pliku `/audit/trail` w pliku `/audit/trailOneLevelBack`, a następnie ponowne włączenie kontrolowania).

AIX Security Expert - wpisy w pliku /etc/inittab

Program Program AIX Security Expert przekształca w komentarz pewne wpisy w pliku `/etc/inittab`, tak aby niektóre zadania nie były uruchamiane w momencie startu systemu.

Tabela 24. Program AIX Security Expert - wpisy w pliku /etc/inittab

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Disable **qdaemon**/ Enable **qdaemon** (Wyłącz demon qdaemon/ Włącz demon qdaemon)	Przekształca w komentarz następujący wpis w pliku /etc/inittab lub usuwa z niego znak komentarza: `qdaemon:2:wait:/usr/bin/startsrc –sqdaemon`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Przekształcenie w komentarz **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak
Disable **lpd** daemon/ Enable **lpd** daemon (Wyłącz demon lpd/Włącz demon lpd)	Przekształca w komentarz następujący wpis w pliku /etc/inittab lub usuwa z niego znak komentarza: `lpd:2:once:/usr/bin/startsrc -s lpd`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Przekształcenie w komentarz **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak

Tabela 24. Program AIX Security Expert - wpisy w pliku /etc/inittab (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable CDE/ Enable CDE (Włącz CDE/ Wyłącz CDE)	Jeśli w systemie nie skonfigurowano LFT, przekształca w komentarz następujący wpis w pliku /etc/inittab lub usuwa z niego znak komentarza: `dt:2:wait:/etc/rc.dt`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Przekształcenie w komentarz **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak
Disable **piobe** daemon/ Enable **piobe** daemon (Włącz demon piobe/ Wyłącz demon piobe)	Przekształca w komentarz następujący wpis w pliku /etc/inittab lub usuwa z niego znak komentarza: `piobe:2:wait:/usr/lib/lpd/pio/etc/pioinit >/dev/null 2>&1`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Przekształcenie w komentarz **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak

AIX Security Expert - ustawienia w pliku /etc/rc.tcpip

Program Program AIX Security Expert przekształca w komentarz pewne wpisy w pliku /etc/rc.tcpip, tak aby niektóre zadania nie były uruchamiane w momencie startu systemu.

Poniższa tabela zawiera wpisy w pliku /etc/rc.tcpip, które zostają przekształcone w komentarz, tak aby niektóre zadania nie były uruchamiane w momencie startu systemu.

Tabela 25. Program AIX Security Expert - ustawienia w pliku /etc/rc.tcpip			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable mail client/Enable mail client (Włącz klient pocztowy/ Wyłącz klient pocztowy)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip lub usuwa z niego znak komentarza: `start /usr/lib/sendmail "$src_running"`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak
Disable routing daemon (Wyłącz demon routingu)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/routed "$src_running" -q`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable **mrouted** daemon (Wyłącz demon mrouted)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/mrouted "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 25. Program AIX Security Expert - ustawienia w pliku /etc/rc.tcpip (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable **timed** daemon (Wyłącz demon timed)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/timed`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Tak	Tak
Disable **rwhod** daemon (Wyłącz demon rwhod)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/rwhod "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable print daemon (Wyłącz demon drukowania)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/lpd "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 25. Program AIX Security Expert - ustawienia w pliku /etc/rc.tcpip (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Disable SNMP daemon/ Enable SNMP daemon (Wyłącz demon SNMP/Włącz demon SNMP)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip lub usuwa z niego znak komentarza: `start /usr/sbin/snmpd "$src_running"`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Przekształcenie w komentarz **Niski poziom bezpieczeństwa** Wyłącza demon SNMP **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak
Stop DHCP Agent (Zatrzymaj agent DHCP)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/dhcprd "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Stop DHCP Server (Zatrzymaj serwer DHCP)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/dhcpsd "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 25. Program AIX Security Expert - ustawienia w pliku /etc/rc.tcpip (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Stop autoconf6 (Zatrzymaj autoconf6)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/autoconf6 “"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable DNS daemon (Wyłącz demon DNS)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/named "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable **gated** daemon (Wyłącz demon gated)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/gated "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 25. Program AIX Security Expert - ustawienia w pliku /etc/rc.tcpip (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Stop DHCP Client (Zatrzymaj klient DHCP)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/dhcpd "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable DPID2 daemon (Wyłącz demon DPID2)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/dpid2 "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable NTP daemon (Wyłącz demon NTP)	Przekształca w komentarz następujący wpis w pliku /etc/rctcpip: `start /usr/sbin/xntpd "$src_running"`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

AIX Security Expert - ustawienia w pliku /etc/inetd.conf

Program Program AIX Security Expert przekształca w komentarz pewne wpisy w pliku /etc/inetd.conf.

Podczas domyślnej instalacji systemu AIX zostaje włączona pewna liczba usług sieciowych, które potencjalnie mogą negatywnie wpłynąć na bezpieczeństwo systemu. Program Program AIX Security Expert wyłącza zbędne i niebezpieczne usługi, przekształcając w komentarz odpowiadające im wpisy w pliku `/etc/inetd.conf`. W przypadku ustawień standardowych systemu AIX z wpisów tych zostaje usunięty znak komentarza. Poniższa tabela zawiera wpisy w pliku `/etc/inetd.conf` które zostają przekształcone w komentarz, lub z których zostaje usunięty znak komentarza.

Tabela 26. Program AIX Security Expert - ustawienia w pliku `/etc/inetd.conf`

Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable **sprayd** in `/etc/inetd.conf` (Wyłącz sprayd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku `/etc/inetd.conf`: `sprayd sunrpc_udp udp wait root \ /usr/lib/netsvc/`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable UDP chargen service in `/etc/inetd.conf` (Wyłącz usługę chargen UDP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku `/etc/inetd.conf`: `chargen dgram udp wait root internal`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable telnet / Enable telnet (Wyłącz telnet /Włącz telnet)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`telnet stream tcp6 nowait root \`
	`/usr/sbin/telnetd telnetd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable UDP Echo service in /etc/inetd.conf (Wyłącz usługę Echo UDP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf: `echo dgram udp wait root internal`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Disable **tftp** in /etc/inetd.conf (Wyłącz tftp w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`tftp dgram udp6 SRC nobody \`
	`/usr/sbin/tftpd tftpd -n`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**

Disable **krshd** daemon (Wyłącz demon krshd)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`kshell stream tcp nowait root \`
	`/usr/sbin/krshd krshd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **rusersd** in /etc/inetd.conf (Wyłącz rusersd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`rusersd sunrpc_udp udp wait root \`
	`/usr/lib/netsvc/`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **rexecd** in /etc/inetd.conf / Enable **rexecd** in /etc/inetd.conf (Wyłącz rexecd w /etc/inetd.conf / Włącz rexecd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`exec stream tcp6 nowait root \`
	`/usr/sbin/rexecd rexecd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Przekształcenie w komentarz
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable POP3D (Wyłącz POP3D)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`pop3 stream tcp nowait root \`
	`/usr/sbin/pop3d pop3d`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **pcnfsd** in /etc/inetd.conf (Wyłącz pcnfsd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`pcnfsd sunrpc_udp udp wait root \`
	`/usr/sbin/rpc.pcnfsd pcnfsd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **bootpd** in /etc/inetd.conf (Wyłącz bootpd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`bootps dgram udp wait root \`
	`/usr/sbin/bootpd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable **rwalld** in /etc/inetd.conf (Wyłącz rwalld w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`rwalld sunrpc_udp udp wait root \`
	`/usr/lib/netsvc/`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable UDP discard service in /etc/inetd.conf (Wyłącz usługę discard UDP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`discard dgram udp wait root \`
	`internal`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable TCP daytime service in /etc/inetd.conf / Enable TCP daytime service in /etc/inetd.conf (Wyłącz usługę daytime TCP w /etc/inetd.conf / Włącz usługę daytime TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`daytime stream tcp nowait root \`
	`internal`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable **netstat** in /etc/inetd.conf (Wyłącz netstat w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`netstat stream tcp nowait nobody \`
	`/usr/bin/netstat`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **rshd** daemon/ Enable **rshd** daemon (Wyłącz demon rshd/ Włącz demon rshd)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`shell stream tcp6 nowait root \`
	`/usr/sbin/rshd rshd rshd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Przekształcenie w komentarz
		Niski poziom bezpieczeństwa
		Przekształcenie w komentarz
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable **cmsd** service in /etc/inetd.conf / Enable **cmsd** service in /etc/inetd.conf (Wyłącz usługę cmsd w /etc/inetd.conf / Włącz usługę cmsd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`cmsd sunrpc_udp udp wait root \`
	`/usr/dt/bin/rpc.cms cmsd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**

Disable **ttdbserver** service in /etc/inetd.conf / Enable **ttdbserver** service in /etc/inetd.conf (Wyłącz usługę ttdbserver w /etc/inetd.conf / Włącz usługę ttdbserver w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`ttdbserver sunrpc_tcp tcp wait \`
	`root /usr/dt/bin/`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable **uucpd** in /etc/inetd.conf / Enable **uucpd** in /etc/inetd.conf (Wyłącz uucpd w /etc/inetd.conf / Włącz uucpd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`uucp stream tcp nowait root \`
	`/usr/sbin/uucpd uucpd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Disable UDP time service in /etc/inetd.conf / Enable UDP time service in /etc/inetd.conf (Wyłącz usługę time TCP w /etc/inetd.conf / Włącz usługę time TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza: `time dgram udp wait root internal`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak

Disable TCP time service in /etc/inetd.conf / Enable TCP time service in /etc/inetd.conf (Wyłącz usługę time TCP w /etc/inetd.conf / Włącz usługę time TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`time stream tcp nowait root \`
	`internal`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable **rexd** in /etc/inetd.conf (Wyłącz rexd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`rexd sunrpc_tcp tcp wait root \`
	`/usr/sbin/tpc.rexd.rexd rexd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Tak
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable TCP chargen service in /etc/inetd.conf (Wyłącz usługę chargen TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`chargen stream tcp nowait root \`
	`internal`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **rlogin** in /etc/inetd.conf / Enable **rlogin** in /etc/inetd.conf (Wyłącz rlogin w /etc/inetd.conf / Włącz rlogin w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`login stream tcp6 nowait root \`
	`/usr/sbin/rlogind rlogind`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Przekształcenie w komentarz
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable talk in /etc/inetd.conf (Wyłącz talk w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`talk dgram udp wait root \`
	`/usr/sbin/talkd talkd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Przekształcenie w komentarz
		Niski poziom bezpieczeństwa
		Przekształcenie w komentarz
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable **fingerd** in /etc/inetd.conf (Wyłącz fingerd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`finger stream tcp nowait nobody \`
	`/usr/sbin/fingerd fingerd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable FTP / Enable FTP (Wyłącz FTP / Włącz FTP)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza:
	`ftp stream tcp6 nowait root \`
	`/usr/sbin/ftpd ftpd`
		Wysoki poziom bezpieczeństwa
		Przekształcenie w komentarz
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Anulowanie komentarza
			Tak

Disable IMAPD (Wyłącz IMAPD)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`imap2 stream tcp nowait root \`
	`/usr/sbin/imapd imapd`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable **comsat** in /etc/inetd.conf (Wyłącz comsat w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`comsat dgram udp wait root \`
	`/usr/sbin/comsat comsat`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable **rquotad** in /etc/inetd.conf (Wyłącz rquotad w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`rquotad sunrpc_udp udp wait root \`
	`/usr/sbin/rpc.rquotad`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Tak
		Niski poziom bezpieczeństwa
		Tak
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable UDP daytime service in /etc/inetd.conf / Enable UDP daytime service in /etc/inetd.conf (Wyłącz usługę daytime UDP w /etc/inetd.conf / Włącz usługę daytime UDP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf lub usuwa z niego znak komentarza: `daytime dgram udp wait root internal`	**Wysoki poziom bezpieczeństwa** Przekształcenie w komentarz **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Anulowanie komentarza	Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania

Disable **krlogind** in /etc/inetd.conf (Wyłącz krlogind w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`klogin stream tcp nowait root \`
	`/usr/sbin/krlogind krlogind`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable TCP Discard service in /etc/inetd.conf (Wyłącz usługę Discard TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf:
	`discard stream tcp nowait root \`
	`internal`
		Wysoki poziom bezpieczeństwa
		Tak
		Średni poziom bezpieczeństwa
		Brak wpływu
		Niski poziom bezpieczeństwa
		Brak wpływu
		Ustawienia standardowe systemu AIX
		Tak
			Tak

Disable TCP echo service in /etc/inetd.conf (Wyłącz usługę echo TCP w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf: `echo stream tcp nowait root internal`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 26. Program AIX Security Expert - ustawienia w pliku /etc/inetd.conf (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable **sysstat** in /etc/inetd.conf (Wyłącz sysstat w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf: `systat stream tcp nowait nodby \ /usr/bin/ps ps -ef`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable **rstatd** in /etc/inetd.conf (Wyłącz rstatd w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf: `rstatd sunrpc_udp udp wait root \ /usr/sbin/rpc.rstatd rstatd`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Disable dtspc in /etc/inetd.conf (Wyłącz dtspc w /etc/inetd.conf)	Przekształca w komentarz następujący wpis w pliku /etc/inetd.conf: `dtspc stream tcp nowait root \ /usr/dt/bin/dtspcd`	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

AIX Security Expert - wyłączanie bitu SUID komend

Niżej wymienione komendy domyślnie zostają zainstalowane z ustawionym bitem SUID. W przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa ustawienie tego bitu zostanie anulowane. W ustawieniach standardowych systemu AIX bit SUID zostanie w tych komendach przywrócony.

Tabela 27. Program AIX Security Expert - wyłączanie bitu SUID komend			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
hls_filepermgr	Menedżer uprawnień do plików: uruchamia komendę **fpm** z opcją high w celu usunięcia bitów setuid i setgid z komend uprzywilejowanych.	Wysoki poziom bezpieczeństwa	Tak
mls_filepermgr	Menedżer uprawnień do plików: uruchamia komendę **fpm** z opcją medium w celu usunięcia bitów setuid i setgid z komend uprzywilejowanych.	Średni poziom bezpieczeństwa	Tak
lls_filepermgr	Menedżer uprawnień do plików: uruchamia komendę **fpm** z opcją low w celu usunięcia bitów setuid i setgid z komend uprzywilejowanych.	Niski poziom bezpieczeństwa	Tak

AIX Security Expert - wyłączanie usług zdalnych

Program Program AIX Security Expert wyłącza niebezpieczne komendy w przypadku wysokiego i średniego poziomu bezpieczeństwa.

Niżej wymienione komendy i demony są często wykorzystywane do odnajdywania luk w zabezpieczeniach. W przypadku wysokiego i średniego poziomu bezpieczeństwa w komendach tych anulowane jest prawo wykonywania, a demony zostają wyłączone. Opcja niskiego poziomu bezpieczeństwa nie ma wpływu na te komendy i demony. W ustawieniach standardowych systemu AIX działanie tych komend i demonów zostaje włączone.

- **rcp**
- **rlogin**
- **rsh**
- **tftp**
- **rlogind**
- **rshd**
- **tftpd**

Tabela 28. Program AIX Security Expert - wyłączanie usług zdalnych

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Enable unsecure daemons (Włącz niebezpieczne demony)	Jeśli baza TCB jest włączona, powoduje ustawienie prawa wykonywania demonów **rlogind**, **rshd** i **tftpd**, a także zaktualizowanie bazy danych programu sysck informacjami o zmianie bitów trybu tych demonów. Jeśli baza TCB nie jest włączona, ustawione zostają prawa wykonywania demonów **rlogind**, **rshd** i **tftpd**.	**Wysoki poziom bezpieczeństwa** Brak wpływu **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Disable unsecure commands (Wyłącz niebezpieczne komendy)	1. Jeśli baza TCB jest włączona, powoduje usunięcie prawa wykonywania komend **rcp**, **rlogin**, **rsh** oraz **tftp**, a także zaktualizowanie bazy danych programu **sysck** informacjami o zmianie bitów trybu tych komend. Jeśli baza TCB nie jest włączona, usunięte zostaje prawo wykonywania komend **rcp**, **rlogin** i **rsh**. 2. Powoduje zatrzymanie bieżących instancji komend **rcp**, **rlogin**, **rsh**, **tftp** i **uftp**, chyba że jedna z nich jest procesem nadrzędnym programu Program AIX Security Expert. 3. Powoduje dodanie sekcji **tcpip:** do pliku `/etc/security/config` w celu ograniczenia wykorzystania **.netrc** w komendach **ftp** i **rexec**.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Enable unsecure commands (Włącz niebezpieczne komendy)	1. Jeśli baza TCB jest włączona, powoduje ustawienie prawa wykonywania komend **rcp**, **rlogin**, **rsh** i **tftp**, a także zaktualizowanie bazy danych programu **sysck** informacjami o zmianie bitów trybu tych komend. Jeśli baza TCB nie jest włączona, ustawione zostaje prawo wykonywania komend **rcp**, **rlogin** i **rsh**. 2. Powoduje usunięcie pliku `/etc/security/config`.	**Wysoki poziom bezpieczeństwa** Brak wpływu **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 28. Program AIX Security Expert - wyłączanie usług zdalnych (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Disable unsecure daemons (Wyłącz niebezpieczne demony)	1. Jeśli baza TCB jest włączona, powoduje usunięcie prawa wykonywania demonów **rlogind**, **rshd** i **tftpd**, a także zaktualizowanie bazy danych programu **sysck** informacjami o zmianie bitów trybu tych demonów. Jeśli baza TCB nie jest włączona, usunięte zostają prawa wykonywania demonów **rlogind**, **rshd** i **tftpd**. 2. Powoduje zatrzymanie bieżących instancji demonów **rlogind**, **rshd** i **tftpd**, chyba że jeden z nich jest procesem nadrzędnym programu Program AIX Security Expert.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Stop NFS daemon (Zatrzymaj demon NFS)	• Usuwa wszystkie podłączenia NFS. • Powoduje wyłączenie NFS. • Usuwa skrypt startowy NFS z pliku `/etc/inittab`.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Enable NFS daemon (Włącz demon NFS)	• Eksportuje wszystkie wpisy wymienione w pliku `/etc/exports`. • Dodaje wpis do pliku /etc/inittab powodujący uruchomienie `/etc/rc.nfs` w momencie startu systemu. • Natychmiast uruchamia `/etc/rc.nfs`.	**Wysoki poziom bezpieczeństwa** Brak wpływu **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

AIX Security Expert - usuwanie możliwości dostępu bez uwierzytelnienia

System AIX obsługuje kilka usług, które nie wymagają uwierzytelnienia użytkownika w momencie logowania do sieci.

Plik `/etc/hosts.equiv` i wszystkie lokalne pliki **$HOME**`/.rhosts` definiują hosty i konta użytkowników, które mogą uruchamiać zdalne komendy na hoście lokalnym bez konieczności podawania hasła. O ile taka możliwość nie jest jawnie wymagana, pliki te należy wyzerować.

Tabela 29. Program AIX Security Expert - usuwanie możliwości dostępu bez uwierzytelnienia			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Remove rhosts and netrc services (Usuń usługi rhosts i netrc)	Pliki `.rhosts` i `.netrc` przechowują nazwy użytkowników i hasła w postaci jawnego tekstu, który można łatwo wykorzystać.	**Wysoki poziom bezpieczeństwa** Usunięcie plików `.rhosts` i `.netrc` z katalogów osobistych wszystkich użytkowników, w tym użytkownika root. **Średni poziom bezpieczeństwa** Usunięcie plików `.rhosts` i `.netrc` z katalogów osobistych wszystkich użytkowników, w tym użytkownika root. **Niski poziom bezpieczeństwa** Usunięcie plików `.rhosts` i `.netrc` z katalogu osobistego użytkownika root. **Ustawienia standardowe systemu AIX** Usunięcie plików `.rhosts` i `.netrc` z katalogów osobistych wszystkich użytkowników, w tym użytkownika root.	Tak
Remove entries from `/etc/hosts.equiv` file (Usuń wpisy z pliku /etc/hosts.equiv)	Plik `/etc/hosts.equiv` oraz plik **$HOME**`/.rhosts` użytkownika lokalnego definiują użytkowników odległych hostów, którzy mogą zdalnie wykonywać komendy na hoście lokalnym. Jeśli ktoś na odległym hoście pozna szczegóły nazwy użytkownika i nazwy hosta, będzie mógł znaleźć sposób na wykonywanie zdalnych komend na hoście lokalnym bez uwierzytelnienia.	**Wysoki poziom bezpieczeństwa** Usuwa wszystkie wpisy w pliku `/etc/hosts.equiv`. **Średni poziom bezpieczeństwa** Usuwa wszystkie wpisy w pliku `/etc/hosts.equiv`. **Niski poziom bezpieczeństwa** Usuwa wszystkie wpisy w pliku `/etc/hosts.equiv`. **Ustawienia standardowe systemu AIX** Usuwa wszystkie wpisy w pliku `/etc/hosts.equiv`.	Tak

AIX Security Expert - strojenie opcji sieciowych

Strojenie odpowiednich wartości opcji sieciowych stanowi ważny element zabezpieczeń. Ustawienie wartości atrybutu związanego z siecią na wartość 0 powoduje wyłączenie danej opcji, a ustawienie wartości na 1 - jej włączenie.

Poniższa tabela zawiera ustawienia atrybutów sieciowych odpowiadające wysokiemu, średniemu i niskiemu poziomowi bezpieczeństwa. W tabeli znajdują się też informacje o tym, w jaki sposób proponowane wartości opcji sieciowych ułatwiają zapewnienie bezpieczeństwa sieci.

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option ipsrcrouteforward (Opcja sieciowa ipsrcrouteforward)	Wskazuje, czy system przekazuje pakiety kierowane według nadawcy. Wyłączenie opcji ipsrcrouteforward uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 1	Tak
Network option ipsrcrouteforward (Opcja sieciowa ipsrcrouteforward)	Wskazuje, czy mają być przetwarzane odebrane przekierowania.	**Wysoki poziom bezpieczeństwa** 1 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option clean_partial_conns (Opcja sieciowa clean_partial_conns)	Wskazuje, czy należy unikać ataków polegających na wykorzystaniu znaku synchronizacji (SYN).	**Wysoki poziom bezpieczeństwa** 1 **Średni poziom bezpieczeństwa** 1 **Niski poziom bezpieczeństwa** 1 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option ipsrcrouterecv (Opcja sieciowa ipsrcrouterecv)	Wskazuje, czy system akceptuje pakiety kierowane według nadawcy. Wyłączenie opcji ipsrcrouterecv uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option ipforwarding (Opcja sieciowa ipforwarding)	Wskazuje, czy jądro powinno przekazywać pakiety. Wyłączenie opcji ipforwarding uniemożliwia dotarcie przekierowanych pakietów do zdalnej sieci.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option ipsendredirects (Opcja sieciowa ipsendredirects)	Wskazuje, czy jądro powinno przesyłać sygnały przekierowania. Wyłączenie opcji ipsendredirects uniemożliwia dotarcie przekierowanych pakietów do zdalnej sieci.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 1	Tak

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option ip6srcrouteforward (Opcja sieciowa ip6srcrouteforward)	Wskazuje, czy system przekazuje pakiety IPv6 kierowane według nadawcy. Wyłączenie opcji ip6srcrouteforward uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 1	Tak
Network option directed_broadcast (Opcja sieciowa directed_broadcast)	Wskazuje, czy dozwolone jest rozgłaszanie kierowane do bramy. Wyłączenie opcji directed_broadcast ułatwia uniemożliwienie dotarcia przekierowanych pakietów do zdalnej sieci.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option tcp_pmtu_discover (Opcja sieciowa tcp_pmtu_discover)	Włącza lub wyłącza wykrywanie jednostki MTU dla ścieżki aplikacji TCP. Wyłączenie opcji tcp_pmtu_discover uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** 1	Tak

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option bcastping (Opcja sieciowa bcastping)	Zezwala na odpowiedzi na pakiety ICMP echo wysyłane na adres rozgłoszeniowy. Wyłączenie opcji bcastping uniemożliwia ataki typu smurf.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option icmpaddressmask (Opcja sieciowa icmpaddressmask)	Wskazuje, czy system odpowiada na żądania maski adresu ICMP. Wyłączenie opcji icmpaddressmask uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option udp_pmtu_discover (Opcja sieciowa udp_pmtu_discover)	Włącza lub wyłącza wykrywanie jednostki MTU dla aplikacji UDP. Wyłączenie opcji udp_pmtu_discover uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** 1	Tak

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option ipsrcroutesend (Opcja sieciowa ipsrcroutesend)	Wskazuje, czy aplikacje mogą wysyłać pakiety kierowane według nadawcy. Wyłączenie opcji ipsrcroutesend uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 1	Tak
Network option nonlocsrcroute (Opcja sieciowa nonlocsrcroute)	Informuje protokół IP, czy tylko pakiety kierowane według nadawcy mogą być adresowane do hostów poza siecią lokalną. Wyłączenie opcji nonlocsrcroute uniemożliwia dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak
Network option tcp_tcpsecure (Opcja sieciowa tcp_tcpsecure)	Chroni połączenia TCP przed słabymi punktami zabezpieczeń. Wartości: • 0 = brak ochrony • 1 = wysyłanie fałszywego SYN do nawiązanego połączenia • 2 = wysyłanie fałszywego RST do nawiązanego połączenia • 4 = wprowadzanie danych do nawiązanego połączenia TCP • 5-7 = połączenie powyższych słabych punktów zabezpieczeń	**Wysoki poziom bezpieczeństwa** 7 **Średni poziom bezpieczeństwa** 7 **Niski poziom bezpieczeństwa** 5 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 30. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia bezpieczeństwa sieciowego (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Network option sockthresh (Opcja sieciowa sockthresh)	Określa limit użycia pamięci sieciowej. Jeśli zostanie przekroczona wartość parametru strojonego sockthresh, nie są dozwolone żadne nowe połączenia z gniazdami. Określa maksymalną wielkość pamięci sieciowej, którą można przydzielić dla gniazd.	**Wysoki poziom bezpieczeństwa** 60 **Średni poziom bezpieczeństwa** 70 **Niski poziom bezpieczeństwa** 85 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Poniższe opcje sieciowe mają związek z wydajnością sieci, a nie z jej bezpieczeństwem.

Tabela 31. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia wydajności sieci			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Network option rfc1323 (Opcja sieciowa rfc1323)	Parametr strojony rfc1323 włącza opcję skalowania okna TCP.	**Wysoki poziom bezpieczeństwa** 1 **Średni poziom bezpieczeństwa** 1 **Niski poziom bezpieczeństwa** 1 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 31. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia wydajności sieci (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option tcp_sendspace (Opcja sieciowa tcp_sendspace)	Parametr strojony tcp_sendspace określa, ile wysyłanych danych aplikacja może buforować w jądrze, zanim zostanie zablokowana w wywołaniu send.	**Wysoki poziom bezpieczeństwa** 262144 **Średni poziom bezpieczeństwa** 262144 **Niski poziom bezpieczeństwa** 262144 **Ustawienia standardowe systemu AIX** 16384	Tak
Network option tcp_mssdflt (Opcja sieciowa tcp_mssdflt)	Domyślna maksymalna wielkość segmentu używanego w komunikacji ze zdalnymi sieciami.	**Wysoki poziom bezpieczeństwa** 1448 **Średni poziom bezpieczeństwa** 1448 **Niski poziom bezpieczeństwa** 1448 **Ustawienia standardowe systemu AIX** 1460	Tak
Network option extendednetstats (Opcja sieciowa extendednetstats)	Włącza gromadzenie obszerniejszych danych statystycznych na temat usług związanych z pamięcią sieciową.	**Wysoki poziom bezpieczeństwa** 1 **Średni poziom bezpieczeństwa** 1 **Niski poziom bezpieczeństwa** 1 **Ustawienia standardowe systemu AIX** Brak ograniczenia	Tak

Tabela 31. Program AIX Security Expert - strojenie opcji sieciowych w celu zwiększenia wydajności sieci (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Network option tcp_recvspace (Opcja sieciowa tcp_recvspace)	Parametr strojony tcp_recvspace określa, ile bajtów odbieranych danych system może buforować w kolejce gniazd odbiorczych jądra.	**Wysoki poziom bezpieczeństwa** 262144 **Średni poziom bezpieczeństwa** 262144 **Niski poziom bezpieczeństwa** 262144 **Ustawienia standardowe systemu AIX** 16384	Tak
Network option sb_max (Opcja sieciowa sb_max)	Parametr strojony sb_max określa górny limit liczby buforów gniazda umieszczonych w kolejce pojedynczego gniazda. Steruje on wielkością obszaru zajmowanego przez bufory umieszczone w kolejce do gniazda nadawcy lub gniazda odbiorcy.	**Wysoki poziom bezpieczeństwa** 1048576 **Średni poziom bezpieczeństwa** 1048576 **Niski poziom bezpieczeństwa** 1048576 **Ustawienia standardowe systemu AIX** 1048576	Tak

AIX Security Expert - reguły filtrowania IPsec

Program Program AIX Security Expert udostępnia następujące filtry IPsec.

Tabela 32. Program AIX Security Expert - reguły filtrowania IPsec			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Shun host for 5 minutes (Unikaj pakietów dla hosta przez 5 minut)	Przez pięć minut blokuj pakiety przeznaczone do kilku portów tcp i udp tego hosta, które są podatne na zagrożenia. Host nie będzie akceptować przez pięć minut żadnych pakietów kierowanych do tych portów.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Guard host against port scans (Chroń host przed skanowaniem portów)	Chroni przed skanowaniem portów. Każdy zdalny host przeprowadzający skanowanie portów jest blokowany przez pięć minut. Żadne pakiety pochodzące z tego zdalnego hosta nie będą akceptowane przez pięć minut.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak

AIX Security Expert - inne ustawienia

Program Program AIX Security Expert udostępnia inne dodatkowe ustawienia zabezpieczeń dla wysokiego, średniego i niskiego poziomu bezpieczeństwa.

Tabela 33. Program AIX Security Expert - inne ustawienia

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Remove dot from path root (Usuń kropkę z korzenia ścieżki)	Sprawdza występowanie kropek (.) w zmiennej środowiskowej PATH w plikach **$HOME**/.profile, **$HOME**/.kshrc, **$HOME**/.cshrc oraz **$HOME**/.login i powoduje ich usunięcie, jeśli występują. **Uwaga:** Usunięcie kropek występuje tylko wtedy, gdy pozycja w pliku zaczyna się od zmiennej środowiskowej PATH i zawiera kropki (.). Plik nie jest zmieniany, jeśli zmienna środowiskowa PATH zawiera inne zmienne lub jest ustawiona na wartość zwracaną z programu wywoływanego ze skryptu. Poniżej podano przykład ścieżki, która nie zostanie zmieniona. *pathprog* oznacza program zwracający łańcuch ścieżki: `PATH="$(pathprog)"` W tej ścieżce kropki są usuwane, zanim treść zmiennej *pathprog* zostanie ustalona, tak więc kropki istniejące w zwróconej ścieżce nie zostaną usunięte.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Tak	Tak
Limit system access (Ogranicz dostęp do systemu)	Zapewnia, że użytkownik root jest jedynym, użytkownikiem, któremu wolno wykonywać zadania **cron**.	**Wysoki poziom bezpieczeństwa** Sprawia, że użytkownik root jest jedynym użytkownikiem w pliku cron.allow i usuwa plik cron.deny. **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Powoduje usunięcie pliku cron.allow i usunięcie wszystkich wpisów z pliku cron.deny.	Tak

Tabela 33. Program AIX Security Expert - inne ustawienia (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Remove dot from /etc/environment (Usuń kropkę z pliku /etc/environment)	Powoduje usunięcie kropek (.) ze zmiennej środowiskowej **PATH** w pliku /etc/environment.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Tak	Tak
Remove dot from non-root path (Usuń kropkę ze ścieżki użytkownika innego niż root)	Powoduje usunięcie kropek (.) ze zmiennej środowiskowej **PATH** w plikach **$HOME**/.profile, **$HOME**/.kshrc, **$HOME**/.cshrc i **$HOME**/.login wszystkich użytkowników innych niż root. **Uwaga:** Usunięcie kropek występuje tylko wtedy, gdy pozycja w pliku zaczyna się od zmiennej środowiskowej PATH i zawiera kropki (.). Plik nie jest zmieniany, jeśli zmienna środowiskowa PATH zawiera inne zmienne lub jest ustawiona na wartość zwracaną z programu wywoływanego ze skryptu. Poniżej podano przykład ścieżki, która nie zostanie zmieniona. *pathprog* oznacza program zwracający łańcuch ścieżki: `PATH="$(pathprog)"` W tej ścieżce kropki są usuwane, zanim treść zmiennej *pathprog* zostanie ustalona, tak więc kropki istniejące w zwróconej ścieżce nie zostaną usunięte.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Nie
Add root user in /etc/ftpusers file (Dodaj użytkownika root do pliku /etc/ftpusers)	Powoduje dodanie nazwy użytkownika root do pliku /etc/ftpusers w celu wyłączenia możliwości zdalnego wykonywania komendy **ftp** przez tego użytkownika.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak

Tabela 33. Program AIX Security Expert - inne ustawienia (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Remove root user in `/etc/ftpusers` file (Usuń użytkownika root z pliku /etc/ftpusers)	Powoduje usunięcie nazwy użytkownika root z pliku `/etc/ftpusers` w celu umożliwienia zdalnego wykonywania komendy **ftp** przez tego użytkownika.	**Wysoki poziom bezpieczeństwa** Brak wpływu **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Tak	Tak
Set login herald (Ustaw zwiastun logowania)	Powoduje sprawdzenie, czy w pliku `/etc/security/login.cfg` nie jest określona wartość atrybutu herald. Jeśli używany jest zwiastun domyślny, należy go zmienić. Zwiastun można zmienić tylko wtedy, gdy ustawieniami narodowymi systemu są **en_US** lub inne ustawienia języka angielskiego. Jeśli kryteria te są spełnione, wartość atrybutu herald w domyślnej sekcji pliku `/etc/security/login.cfg` zostaje ustawiona na następującą: `Unauthorized use of this \ system is prohibited.\nlogin:` **Uwaga:** To ustawienie zabezpieczeń obowiązuje tylko dla nowych sesji. Nie ma ono wpływu na sesję, w której określono to ustawienie konfiguracyjne.	**Wysoki poziom bezpieczeństwa** herald="Unauthorized use of this system is prohibited.\nlogin:" **Średni poziom bezpieczeństwa** herald="Unauthorized use of this system is prohibited.\nlogin:" **Niski poziom bezpieczeństwa** herald="Unauthorized use of this system is prohibited.\nlogin:" **Ustawienia standardowe systemu AIX** herald=	Tak

Tabela 33. Program AIX Security Expert - inne ustawienia (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Remove guest account (Usuń konto użytkownika guest)	W przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa powoduje usunięcie z komputera konta użytkownika guest oraz wszystkich jego danych. W ustawieniach standardowych systemu AIX w systemie zostaje utworzone konto użytkownika guest. **Uwaga:** Administrator systemu musi jawnie określić hasło dla tego konta, ponieważ program Program AIX Security Expert nie umożliwia wykonywania działań wymagających interakcji z użytkownikiem.	**Wysoki poziom bezpieczeństwa** Powoduje usunięcie konta użytkownika guest i jego danych. **Średni poziom bezpieczeństwa** Powoduje usunięcie konta użytkownika guest i jego danych. **Niski poziom bezpieczeństwa** Powoduje usunięcie konta użytkownika guest i jego danych. **Ustawienia standardowe systemu AIX** Powoduje dodanie konta użytkownika guest do komputera.	Tak
Crontab permissions (Uprawnienia crontab)	Zapewnia, że zadania **crontab** użytkownika root należą wyłącznie do niego i tylko on ma prawo zapisu do nich.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Tak **Ustawienia standardowe systemu AIX** Brak wpływu	Tak
Enable X-Server access (Włącz dostęp do serwera X-Window)	Powoduje, że dostęp do serwera X-Window wymaga uwierzytelnienia.	**Wysoki poziom bezpieczeństwa** Uwierzytelnianie jest wymagane **Średni poziom bezpieczeństwa** Uwierzytelnianie jest wymagane **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Niepotrzebne	Nie

Tabela 33. Program AIX Security Expert - inne ustawienia (kontynuacja)

Etykieta przycisku	Opis	Wartość ustawiona przez program Program AIX Security Expert	Możliwość wycofania
Object creation permissions (Uprawnienia do tworzonych obiektów)	Ustawia odpowiednią wartość atrybutu **umask** w pliku `/etc/security/user`. Określa ona domyślne uprawnienia dostępu do tworzonych obiektów.	**Wysoki poziom bezpieczeństwa** 077 **Średni poziom bezpieczeństwa** 027 **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** 022	Tak
Set core file size (Ustaw wielkość pliku core)	Ustawia odpowiednią wartość atrybutu **core** w pliku `/etc/security/limits`. Określa ona wielkość pliku core dla użytkownika root. **Uwaga:** To ustawienie zabezpieczeń obowiązuje tylko dla nowych sesji. Nie ma ono wpływu na sesję, w której określono to ustawienie konfiguracyjne.	**Wysoki poziom bezpieczeństwa** 0 **Średni poziom bezpieczeństwa** 0 **Niski poziom bezpieczeństwa** 0 **Ustawienia standardowe systemu AIX** 2097151	Tak
Enable SED feature (Włącz opcję SED)	Włącza opcję Stack Execution Disable (Wyłączenie wykonywania stosu) i uruchamia komendę **sedmgr** na podanych plikach. **Uwaga:** Aby reguła stała się aktywna, niezbędny jest restart systemu.	**Wysoki poziom bezpieczeństwa** setidfiles (pliki setid) **Średni poziom bezpieczeństwa** Brak wpływu **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	

Tabela 33. Program AIX Security Expert - inne ustawienia (kontynuacja)			
Etykieta przycisku	**Opis**	**Wartość ustawiona przez program Program AIX Security Expert**	**Możliwość wycofania**
Root Password Integrity Check (Sprawdzenie integralności hasła użytkownika root)	Zapewnia, że hasło użytkownika root nie będzie słabe (łatwe do odgadnięcia). Atrybut dictionlist użytkownika root ma wartość `/etc/security/aixpert/dictionary/English`, dlatego komenda **passwd** może gwarantować, że ustawiane hasło użytkownika nie jest słabe.	**Wysoki poziom bezpieczeństwa** Tak **Średni poziom bezpieczeństwa** Tak **Niski poziom bezpieczeństwa** Brak wpływu **Ustawienia standardowe systemu AIX** Brak wpływu	Tak

AIX Security Expert - wycofywanie ustawień zabezpieczeń

Istnieje możliwość wycofywania niektórych ustawień i reguł zabezpieczeń programu Program AIX Security Expert.

Nie ma możliwości wycofania następujących ustawień i reguł zabezpieczeń programu Program AIX Security Expert:

- Ustawienie Check password definitions (Sprawdź definicje haseł) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
- Ustawienie Check user definitions (Sprawdź definicje użytkowników) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
- Ustawienie Check group definitions (Sprawdź definicje grup) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
- Ustawienie TCB update (Aktualizacja TCB) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
- Ustawienie Enable X-Server access (Włącz dostęp do serwera X-Window) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.
- Ustawienie Remove dot from non-root path (Usuń kropkę ze ścieżki użytkownika innego niż root) w przypadku wysokiego poziomu bezpieczeństwa i ustawień standardowych systemu AIX
- Ustawienie Remove guest account (Usuń konto użytkownika guest) w przypadku wysokiego, średniego i niskiego poziomu bezpieczeństwa.

AIX Security Expert - sprawdzanie poziomu bezpieczeństwa

Program Program AIX Security Expert może generować reporty na temat bieżących ustawień zabezpieczeń systemu i sieci.

Po skonfigurowaniu systemu przy pomocy programu Program AIX Security Expert (komenda `aixpert`) można użyć opcji Check Security (Sprawdź ustawienia zabezpieczeń) w celu wygenerowania raportu na temat różnych ustawień konfiguracyjnych. Jeśli pewne ustawienia zmieniono poza programem Program AIX Security Expert, opcja Check Security (Sprawdź ustawienia zabezpieczeń) programu Program AIX Security Expert pozwala zaprotokołować odpowiednie różnice w pliku `/etc/security/aixpert/check_report.txt`.

Niech, przykładowo, demon **talkd** będzie wyłączony w pliku `/etc/inetd.conf`, kiedy użytkownik ustawia opcję niskiego poziomu bezpieczeństwa. Jeśli później demon **talkd** zostanie włączony i

wykonana zostanie opcja Check Security (Sprawdź ustawienia zabezpieczeń), w pliku `check_report.txt` zostanie zaprotokołowana następująca informacja na ten temat:

```
coninetdconf.ksh: Service talk using protocol udp should be disabled, however it is enabled now.
```

Jeśli zastosowane ustawienia zabezpieczeń nie zostaną zmodyfikowane, plik `check_report.txt` będzie pusty.

Opcję Check Security (Sprawdź ustawienia zabezpieczeń) należy uruchamiać okresowo, a generowany przez nią raport należy przeglądać w celu stwierdzenia, czy nie dokonano modyfikacji ustawień zabezpieczeń zastosowanych przy pomocy programu Program AIX Security Expert. Opcję Check Security (Sprawdź ustawienia zabezpieczeń) należy uruchamiać także po dokonaniu każdej ważnej zmiany w systemie, takiej jak zainstalowanie lub zaktualizowanie oprogramowania.

Informacje pokrewne

Komenda aixpert

AIX Security Expert - pliki wykorzystywane przez program

Program Program AIX Security Expert tworzy i wykorzystuje pewną liczbę plików.

/etc/security/aixpert/core/aixpertall.xml
Jest to mająca format XML lista wszystkich możliwych ustawień zabezpieczeń.

/etc/security/aixpert/core/appliedaixpert.xml
Jest to mająca format XML lista zastosowanych ustawień zabezpieczeń.

/etc/security/aixpert/core/secaixpert.xml
Jest to mająca format XML lista zawierającą wybrane ustawienia zabezpieczeń zastosowane przy użyciu interfejsu GUI programu Program AIX Security Expert.

/etc/security/aixpert/log/aixpert.log
Zawiera protokół śledzenia zastosowanych ustawień zabezpieczeń. Program Program AIX Security Expert nie wykorzystuje narzędzia syslog, lecz zapisuje informacje bezpośrednio do pliku `/etc/security/aixpert/log/aixpert.log`.

Uwaga: Pliki XML i protokoły programu Program AIX Security Expert są tworzone z następującymi prawami dostępu:

/etc/security/aixpert/
`drwx------`

/etc/security/aixpert/core/
`drwx------`

/etc/security/aixpert/core/aixpertall.xml
`r--------`

/etc/security/aixpert/core/appliedaixpert.xml

/etc/security/aixpert/core/secaixpert.xml

/etc/security/aixpert/log
`drwx------`

/etc/security/aixpert/log/aixpert.log
`-rw-------`

/etc/security/aixpert/core/secundoaixpert.xml
`rw-------`

/etc/security/aixpert/check_report.txt
`rw-------`

AIX Security Expert - scenariusz zastosowania wysokiego poziomu bezpieczeństwa

Poniższy scenariusz ilustruje zastosowanie opcji High level security (Wysoki poziom bezpieczeństwa) programu Program AIX Security Expert.

Zastosowany w programie Program AIX Security Expert widok poziomów bezpieczeństwa pochodzi w części z dokumentu NIST zatytułowanego *Security Configuration Checklists Program for IT Products - Guidance for CheckLists Users and Developers* (poszukaj nazwy tej publikacji w serwisie WWW NIS: http://www.nist.gov/index.html). Jednakże pojęcia wysokiego, średniego i niskiego poziomu bezpieczeństwa mogą oznaczać różne rzeczy dla różnych użytkowników. Ważna jest dobra znajomość środowiska, w którym działa system. Wybór zbyt wysokiego poziomu bezpieczeństwa może doprowadzić do sytuacji, w której użytkownik sam sobie odetnie dostęp do komputera. Z kolei zbyt niski poziom bezpieczeństwa powoduje, że komputer staje się podatny na ataki.

W poniższym przykładzie przedstawione jest środowisko wymagające wysokiego poziomu bezpieczeństwa. Użytkownik Robert zamierza wykorzystywać swój system przy współudziale dostawcy usług internetowych. System będzie połączony bezpośrednio z Internetem, będzie działał jako serwer HTTP, będzie zawierał objęte szczególną ochroną dane na temat użytkowników i będzie administrowany zdalnie przez użytkownika Robert. System należy skonfigurować i przetestować w odizolowanej sieci lokalnej, a dopiero potem włączyć do Internetu we współpracy z dostawcą usług internetowych.

W tym środowisku właściwy jest wysoki poziom bezpieczeństwa, ale użytkownik Robert wymaga zdalnego dostępu do systemu. Wysoki poziom bezpieczeństwa nie zezwala na użycie takich programów komunikacyjnych, jak **telnet**, **rlogin**, **ftp** i innych, które przesyłają hasła w postaci jawnej przez sieć. Hasła takie mogą zostać łatwo podsłuchane przez kogoś w Internecie. Użytkownik Robert potrzebuje bezpiecznej metody zdalnego logowania, takiej jak **openssh**. Może się on zapoznać z pełną dokumentacją programu Program AIX Security Expert w celu stwierdzenia, czy w jego środowisku występuje szczególny element, który mógłby zostać zablokowany po zastosowaniu wysokiego poziomu bezpieczeństwa. Jeśli tak jest, może on anulować wybór tego elementu po wyświetleniu szczegółowego panelu zawierającego informacje na temat wysokiego poziomu bezpieczeństwa. Użytkownik Robert powinien także skonfigurować i uruchomić serwer HTTP lub inne usługi, które mają być realizowane przez jego system.

Kiedy użytkownik Robert wybierze opcję wysokiego poziomu bezpieczeństwa, program Program AIX Security Expert wykryje, że działające usługi są niezbędne, i nie zablokuje dostępu do ich portów. Dostęp do wszystkich innych portów będzie traktowany jak słaby punkt zabezpieczeń i zostanie zablokowany przez opcję wysokiego poziomu bezpieczeństwa. Po przetestowaniu tej konfiguracji, komputer użytkownika Robert będzie gotowy do działania w środowisku internetowym.

AIX Security Expert - scenariusz zastosowania średniego poziomu bezpieczeństwa

Poniższy scenariusz ilustruje zastosowanie opcji Medium level security (Średni poziom bezpieczeństwa) programu Program AIX Security Expert.

Użytkownik Alicja potrzebuje wzmocnić zabezpieczenia systemu, który ma być połączony z siecią przedsiębiorstwa oddzieloną od Internetu za pomocą korporacyjnego firewalla. Sieć jest bezpieczna i dobrze administrowana. System ten będzie używany przez dużą liczbę użytkowników, którzy potrzebują korzystać z systemu przy użyciu programów **telnet** i **ftp**. Użytkownik Alicja chce zastosować zwykłe ustawienia zabezpieczeń, takie jak ochrona przed skanowaniem portów, czy też określenie okresu ważności hasła, ale system musi być także dostępny przy użyciu większości zdalnych metod. W tym scenariuszu najbardziej odpowiedni dla systemu użytkownika Alicja jest średni poziom bezpieczeństwa.

AIX Security Expert - scenariusz zastosowania niskiego poziomu bezpieczeństwa

Poniższy scenariusz ilustruje zastosowanie opcji Low level security (Niski poziom bezpieczeństwa) programu Program AIX Security Expert.

Użytkownik Tomasz jest administratorem systemu od pewnego czasu. System znajduje się w odizolowanej i bezpiecznej sieci lokalnej. Jest wykorzystywany przez wielu użytkowników i realizuje szeroką gamę usług. Użytkownik chce podnieść obecny minimalny poziom bezpieczeństwa, ale nie może zablokować żadnej metody dostępu do systemu. Niski poziom bezpieczeństwa jest właściwym wyborem dla komputera użytkownika Tomasz.

Lista kontrolna czynności dotyczących bezpieczeństwa

Poniżej przedstawiono listę kontrolną czynności związanych z bezpieczeństwem, które należy wykonać zarówno w systemie nowo zainstalowanym, jak i istniejącym.

Chociaż lista ta nie jest kompletna, można ją wykorzystać jako podstawę do stworzenia listy kontrolnej dotyczącej bezpieczeństwa dla lokalnego środowiska.

- Instaluj nowy system AIX z bezpiecznego nośnika podstawowego. Podczas instalowania wykonaj następujące procedury:
  - Nie instaluj na serwerach środowisk graficznych w rodzaju CDE, GNOME lub KDE.
  - Zainstaluj wymagane poprawki w zakresie bezpieczeństwa i wszelkie zalecane poprawki poziomu konserwacyjnego i technologicznego. Najnowsze biuletyny serwisowe, porady z zakresu bezpieczeństwa i informacje na temat poprawek można znaleźć w serwisie WWW z poprawkami dla IBM System p eServer pod adresem http://www.ibm.com/support/fixcentral.
  - Utwórz kopię zapasową systemu po zainstalowaniu i zdeponuj ją w bezpiecznym miejscu.
- Zdefiniuj listę kontroli dostępu dla zastrzeżonych plików i katalogów.
- Zablokuj nieużywane konta użytkowników i konta systemowe, takie jak daemon, bin, sys, adm, lp i uucp. Nie zaleca się usuwania kont, ponieważ powoduje to usunięcie informacji o kontach, takich jak nazwy użytkowników, które w dalszym ciągu mogą być powiązane z danymi kopii zapasowej systemu. Utworzenie konta użytkownika dla usuniętego wcześniej identyfikatora użytkownika i odtworzenie kopii zapasowej w systemie może spowodować niezamierzone przydzielenie nowemu użytkownikowi praw dostępu do odtworzonego systemu.
- Regularnie przeglądaj pliki `/etc/inetd.conf`, `/etc/inittab`, `/etc/rc.nfs` i `/etc/rc.tcpip` i usuwaj wszelkie niepotrzebne demony i usługi.
- Sprawdź, czy poprawnie ustawiono uprawnienia do następujących plików:

```
-rw-rw-r-- root     system  /etc/filesystems
-rw-rw-r-- root     system  /etc/hosts
-rw------- root     system  /etc/inittab
-rw-r--r-- root     system  /etc/vfs
-rw-r--r-- root     system  /etc/security/failedlogin
-rw-rw---- root     audit   /etc/security/audit/hosts
```

- Zablokuj możliwość zdalnego logowania się na konto użytkownika root. Możliwość logowania się na konto użytkownika root powinna być ograniczona wyłącznie do konsoli systemowej.
- Włącz kontrolę systemu. Więcej informacji na ten temat zawiera sekcja “Kontrola - przegląd” na stronie 136.
- Włącz strategię kontroli logowania. Więcej informacji na ten temat zawiera sekcja “Kontrola logowania” na stronie 33.
- Zablokuj możliwość wykonywania przez użytkowników komendy `xhost`. Więcej informacji na ten temat zawiera sekcja “Uwagi dotyczące zarządzania środowiskami X11 i CDE” na stronie 39.
- Zablokuj możliwość zmiany zmiennej środowiskowej PATH bez zezwolenia. Więcej informacji na ten temat zawiera sekcja “Zmienna środowiskowa PATH” na stronie 55.
- Wyłącz komendy telnet, rlogin i rsh. Więcej informacji na ten temat zawiera sekcja “Bezpieczeństwo TCP/IP” na stronie 213.
- Włącz funkcje kontroli kont użytkowników. Więcej informacji na ten temat zawiera sekcja “Kontrola kont użytkowników” na stronie 52.
- Narzuć strategię rygorystycznych reguł dla haseł. Więcej informacji na ten temat zawiera sekcja “Hasła” na stronie 65.
- Określ limity pamięci dyskowej dla kont użytkowników. Więcej informacji na ten temat zawiera sekcja “Usuwanie skutków wystąpienia warunku przekroczenia limitu” na stronie 78.

- Ogranicz uprawnienia do uruchamiania komendy **su** dla kont administracyjnych. Sprawdzaj protokoły komendy **su** w pliku `/var/adm/sulog`.
- Włącz blokowanie ekranu w systemie X-Window.
- Ogranicz prawa dostępu do komend **cron** i **at** wyłącznie do kont, które muszą korzystać z tych komend.
- Utwórz alias komendy **ls**, który będzie wyświetlał pliki ukryte i ukryte znaki w nazwie pliku.
- Utwórz alias komendy **rm**, który uniemożliwi przypadkowe usunięcie plików z systemu.
- Wyłącz niepotrzebne usługi sieciowe. Więcej informacji na ten temat zawiera sekcja "Usługi sieciowe" na stronie 221.
- Często wykonuj kopie zapasowe systemu i sprawdzaj ich integralność.
- Zapisz się do grup dyskusyjnych i serwisów poświęconych tematyce bezpieczeństwa.

Podsumowanie informacji na temat powszechnych usług systemu AIX

W poniższej tabeli przedstawiono listę popularniejszych usług systemu AIX. Tabela ta może posłużyć jako punkt wyjściowy do zabezpieczenia systemu.

Przed przystąpieniem do zabezpieczania systemu, należy utworzyć kopię zapasową plików konfiguracyjnych, w tym w szczególności:

- `/etc/inetd.conf`
- `/etc/inittab`
- `/etc/rc.nfs`
- `/etc/rc.tcpip`

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/bootps	inetd	/etc/inetd.conf	Usługi protokołu bootp dla klientów bezdyskowych.	• Konieczne dla funkcji Zarządzanie Instalacją Sieciową (NIM) i zdalnego startowania systemów. • Działa współbieżnie z protokołem tftp. • Wyłączyć w większości przypadków.
inetd/chargen	inetd	/etc/inetd.conf	Generator znaków (tylko na potrzeby testów).	• Dostępny jako usługa protokołu TCP i UDP. • Umożliwia przeprowadzanie ataków polegających na spowodowaniu odmowy usługi (DoS). • Wyłączyć, chyba że przeprowadzane są testy sieci.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/cmsd	inetd	/etc/inetd.conf	Usługa kalendarza (używana przez środowisko CDE).	• Działa jako użytkownik root, powodując zagrożenie dla bezpieczeństwa. • Wyłączyć, chyba że usługa ta jest wymagana przez środowisko niż CDE. • Wyłączyć w serwerach baz danych zaplecza.
inetd/comsat	inetd	/etc/inetd.conf	Powiadamia o przychodzącej poczcie elektronicznej.	• Działa jako użytkownik root, powodując zagrożenie dla bezpieczeństwa. • Rzadko potrzebna. • Wyłączyć.
inetd/daytime	inetd	/etc/inetd.conf	Przestarzała usługa czasu (tylko na potrzeby testów).	• Działa jako użytkownik root. • Dostępny jako usługa protokołu TCP i UDP. • Umożliwia przeprowadzanie ataków polegających na spowodowaniu odmowy usługi (DoS) przy użyciu komendy PING. • Usługa jest przestarzała i jest obecnie używana tylko na potrzeby testów. • Wyłączyć.
inetd/discard	inetd	/etc/inetd.conf	Usługa /dev/null (tylko na potrzeby testów).	• Dostępna jako usługa protokołu TCP i UDP. • Umożliwia przeprowadzanie ataków polegających na spowodowaniu odmowy usługi (DoS). • Usługa jest przestarzała i jest obecnie używana tylko na potrzeby testów. • Wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/dtspc	inetd	/etc/inetd.conf	Element sterujący podprocesu CDE.	• Usługa ta jest uruchamiana automatycznie przez demon `inetd` w odpowiedzi na zgłoszone przez klienta CDE żądanie uruchomienia procesu na hoście demona. Powoduje to zwiększenie podatności na ataki. • Wyłączyć w serwerach zaplecza bez środowiska CDE. • Środowisko CDE może działać bez tej usługi. • Wyłączyć, z wyjątkiem sytuacji, w których usługa ta jest rzeczywiście niezbędna.
inetd/echo	inetd	etc/inetd.conf	Usługa echa (tylko na potrzeby testów).	• Dostępna jako usługa protokołu TCP i UDP. • Może być używana do przeprowadzania ataków DoS lub Smurf. • Używane do uzyskania echa w celu przejścia przez firewall lub uruchomienia procesu datastorm. • Wyłączyć.
inetd/exec	inetd	/etc/inetd.conf	Usługa zdalnego wykonywania komend.	• Działa jako użytkownik root. • Wymaga podania identyfikatora i hasła użytkownika, które przesyła następnie w postaci niezabezpieczonej. • Usługa ta jest szczególnie podatna na nasłuch. • Wyłączyć.
inetd/finger	inetd	/etc/inetd.conf	Program finger umożliwiający zasięganie informacji o użytkownikach.	• Działa jako użytkownik root. • Udostępnia osobom postronnym informacje dotyczące lokalnych systemów i użytkowników. • Wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/ftp	inetd	/etc/inetd.conf	Protokół przesyłania plików.	• Działa jako użytkownik root. • Identyfikator i hasło użytkownika są przesyłane w postaci jawnej, co umożliwia ich przechwycenie. • Należy wyłączyć tę usługę i użyć powszechnie dostępnego pakietu SSH.
inetd/imap2	inetd	/etc/inetd.conf	Protokół IMAP (Internet Mail Access Protocol).	• Należy używać najnowszej wersji serwera tej usługi. • Usługa jest konieczna tylko wtedy, gdy w systemie działa serwer poczty. W przeciwnym razie należy ją wyłączyć. • Identyfikator i hasło użytkownika są przesyłane w postaci jawnej.
inetd/klogin	inetd	/etc/inetd.conf	Logowanie w protokole Kerberos.	• Usługa włączona, jeśli w systemie używane jest uwierzytelnianie metodą Kerberos.
inetd/kshell	inetd	/etc/inetd.conf	Powłoka protokołu Kerberos.	• Usługa włączona, jeśli w systemie używane jest uwierzytelnianie metodą Kerberos.
inetd/login	inetd	/etc/inetd.conf	Usługa rlogin.	• Usługa narażona na podszywanie się pod adres IP lub pod serwer DNS. • Dane, w tym identyfikator i hasło użytkownika, są przesyłane w formie jawnej. • Działa jako użytkownik root. • Zamiast tej usługi należy używać programu SSH.
inetd/netstat	inetd	/etc/inetd.conf	Raportowanie bieżącego statusu sieci.	• Jeśli usługa ta jest uruchamiana w systemie, może ona potencjalnie udostępnić hakerom informacje o tym systemie. • Wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/ntalk	inetd	/etc/inetd.conf	Umożliwia użytkownikom prowadzenie ze sobą lokalnych rozmów.	• Działa jako użytkownik root. • Nie jest wymagana na serwerach produkcyjnych ani na serwerach zaplecza. • Wyłączyć, z wyjątkiem sytuacji, w których usługa ta jest rzeczywiście niezbędna.
inetd/pcnfsd	inetd	/etc/inetd.conf	Usługi systemu plików NFS dla komputerów PC.	• Należy wyłączyć tę usługę, jeśli nie jest ona wykorzystywana. • Jeśli potrzebna jest podobna usługa, należy skorzystać z programu Samba, ponieważ demon pcnfsd jest starszy od opublikowanej przez Microsoft specyfikacji usług SMB.
inetd/pop3	inetd	/etc/linetd.conf	Protokół POP (Post Office Protocol).	• Identyfikatory i hasła użytkowników są przesyłane w formie jawnej. • Usługa potrzebna tylko wtedy, gdy system działa jako serwer poczty i ma klientów, którzy korzystają z aplikacji obsługujących wyłącznie protokół POP3. • Jeśli aplikacje klientów obsługują protokół IMAP, należy używać tego protokołu, można także używać usługi POP3s. Korzysta ona z tunelu SSL (Secure Socket Layer). • Usługę należy wyłączyć, jeśli w systemie nie działa serwer poczty ani nie ma klientów, którzy potrzebują usług POP.
inetd/rexd	inetd	/etc/inetd.conf	Usługa zdalnego wykonywania komend.	• Działa jako użytkownik root. • Jest równorzędna z komendą **on**. • Usługę tę należy wyłączyć. • Zamiast niej lepiej jest używać komend **rsh** i **rshd**.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/quotad	inetd	/etc/inetd.conf	Informuje o limitach plikowych (dla klientów NFS).	• Usługa potrzebna tylko w przypadku korzystania z usług systemu plików NFS. • Usługę tę należy wyłączyć, chyba że jest wymagana do odpowiadania na komendę **quota**. • Jeśli usługa ta jest potrzebna, należy regularnie aktualizować poprawki dla tej usługi.
inetd/rstatd	inetd	/etc/inetd.conf	Serwer Kernel Statistics Server	• Jeśli wymagane jest monitorowanie systemów, należy użyć protokołu SNMP, a tę usługę wyłączyć. • Usługa wymagana w przypadku korzystania z komendy **rup**.
inetd/rusersd	inetd	/etc/inetd.conf	Informacje o zalogowanym użytkowniku.	• Usługa ta nie ma zasadniczego znaczenia. Wyłączyć. • Działa jako użytkownik root. • Udostępnia listę bieżących użytkowników systemu i jest równorzędna z komendą rusers.
inetd/rwalld	inetd	/etc/inetd.conf	Pisanie komunikatów do wszystkich użytkowników.	• Działa jako użytkownik root. • Jeśli w systemach są użytkownicy interaktywni, może być konieczne pozostawienie tej usługi. • Jeśli systemy pełnią rolę serwerów produkcyjnych i serwerów baz danych, usługa ta nie jest potrzebna. • Wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/shell	inetd	/etc/inetd.conf	Usługa rsh.	• Jeśli to możliwe, należy wyłączyć tę usługę. Zamiast niej należy korzystać z programu SSH. • Jeśli konieczne jest korzystanie z tej usługi, należy użyć opakowania TCP (TCP Wrapper) w celu uniemożliwienia podszywania się i ograniczenia ryzyka. • Usługa wymagana dla programu dystrybucji oprogramowania **Xhier**.
inetd/sprayd	inetd	/etc/inetd.conf	Testy Spray w ramach usług RPC.	• Działa jako użytkownik root. • Może być wymagana do celów diagnostycznych w razie problemów sieciowych z systemem plików NFS. • Usługę należy wyłączyć, jeśli nie korzysta się z systemu NFS.
inetd/systat	inetd	/etc/inted.conf	"Status raportu ps -ef"	• Umożliwia zdalne przeglądanie statusu procesu w systemie lokalnym. • Usługa ta jest domyślnie wyłączona. Należy sprawdzać okresowo, czy nie została ona włączona.
inetd/talk	inetd	/etc/inetd.conf	Dzieli ekran na dwie części pomiędzy dwóch użytkowników w sieci.	• Usługa niewymagana. • Używana wraz z komendą **talk**. • Udostępnia usługę UDP na porcie 517. • Usługę tę należy wyłączyć, chyba że potrzebne są wielokrotne interaktywne sesje rozmowy sieciowej dla użytkowników systemu UNIX.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/ntalk	inetd	/etc/inetd.conf	Usługa "new talk" dzieli ekran na dwie części pomiędzy dwóch użytkowników w w sieci.	• Usługa niewymagana. • Używana wraz z komendą **talk**. • Udostępnia usługę UDP na porcie 517. • Usługę tę należy wyłączyć, chyba że potrzebne są wielokrotne interaktywne sesje rozmowy sieciowej dla użytkowników systemu UNIX.
inetd/telnet	inetd	/etc/inetd.conf	Usługa telnet.	• Obsługuje zdalne sesje logowania, ale przesyła identyfikator i hasło w formie jawnej. • Jeśli to możliwe, należy wyłączyć tę usługę i zamiast niej użyć na potrzeby zdalnego dostępu programu SSH.
inetd/tftp	inetd	/etc/inetd.conf	Proste przesyłanie plików.	• Udostępnia usługę UDP na porcie 69. • Działa jako użytkownik root i może być wykorzystana do złamania zabezpieczeń. • Jest używana przez funkcję NIM. • Usługę tę należy wyłączyć, chyba że używana jest funkcja NIM lub konieczne jest startowanie bezdyskowych stacji roboczych.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inetd/time	inetd	/etc/inetd.conf	Przestarzała usługa czasu.	• Wewnętrzna funkcja demona **inetd** używana przez komendę **rdate**. • Dostępna jako usługa protokołu TCP i UDP. • Niekiedy używana do synchronizacji czasu w momencie startu. • Usługa przestarzała. Zamiast niej należy użyć usługi ntpdate. • Usługę można wyłączyć po sprawdzeniu, że start systemów, dla których usługa ta została wyłączona, odbywa się bez żadnych problemów.
inetd/ttdbserver	inetd	/etc/inetd.conf	Serwer baz danych ToolTalk (dla CDE)	• Usługa **rpc.ttdbserverd** działa jako użytkownik root i może być wykorzystana do złamania zabezpieczeń. • Określana jako usługa wymagana dla środowiska CDE, ale środowisko CDE może działać bez niej. • Nie powinna działać na serwerach zaplecza ani w żadnych innych systemach, dla których kwestie bezpieczeństwa są szczególnie ważne.
inetd/uucp	inetd	/etc/inetd.conf	Sieć UUCP.	• Usługę tę należy wyłączyć, chyba że używana jest aplikacja, która wykorzystuje program UUCP.
inittab/dt	init	skrypt /etc/rc.dt w /etc/inittab	Okno logowania do środowiska CDE.	• Uruchamia na konsoli serwer X11. • Obsługuje protokół xdcmp (X11 Display Manager Control Protocol), dzięki czemu inne stacje X11 mogą logować się do tego samego komputera. • Usługa powinna być używana tylko na osobistych stacjach roboczych. Nie należy z niej korzystać w systemach zaplecza.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inittab/dt_nogb	init	/etc/inittab	Okno logowania do środowiska CDE (BEZ startowania do środowiska graficznego).	• Wstrzymuje wyświetlanie środowiska graficznego do czasu pełnego zainstalowania systemu. • Takie same uwagi, jak dla usługi inittab/dt.
inittab/httpdlite	init	/etc/inittab	Serwer WWW dla komendy `docsearch`.	• Domyślny serwer WWW dla mechanizmu docsearch. • Usługę tę należy wyłączyć, chyba że dany komputer jest serwerem dokumentacji.
inittab/i4ls	init	/etc/inittab	Serwery menedżera licencji.	• Włączyć dla komputerów używanych do prac programistycznych. • Wyłączyć dla komputerów produkcyjnych. • Włączyć dla serwerów baz danych zaplecza, które wymagają zarządzania licencjami. • Udostępnia obsługę kompilatorów, oprogramowania baz danych i wszelkich innych produktów licencjonowanych.
inittab/imqss	init	/etc/inittab	Mechanizm wyszukiwania dla usługi "docsearch".	• Część domyślnego serwera dla mechanizmu docsearch. • Usługę tę należy wyłączyć, chyba że dany komputer jest serwerem dokumentacji.
inittab/lpd	init	/etc/inittab	Interfejs drukarki wierszowej BSD.	• Akceptuje zadania drukowania z innych systemów. • Usługę tę można wyłączyć i nie uniemożliwia to wysyłania zadań do serwera wydruków. • Należy wyłączyć tę usługę, sprawdzając wcześniej, że nie będzie to miało wpływu na funkcje drukowania.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
inittab/nfs	init	/etc/inittab	System NFS (Network File System) i usługi NIS (Net Information Services).	• Usługi NFS i NIS oparte na protokole UDP/RPC. • Zapewnia uwierzytelnianie w minimalnym zakresie. • Należy wyłączyć tę usługę dla komputerów zaplecza.
inittab/piobe	init	/etc/inittab	Postprocesor we/wy drukarki (na potrzeby drukowania).	• Obsługuje planowanie, buforowanie i drukowanie zadań wprowadzonych przez demon **qdaemon**. • Usługę tę należy wyłączyć, jeśli zadania drukowania nie są drukowane lokalnie tylko przesyłane na serwer.
inittab/qdaemon	init	/etc/inittab	Demon kolejki (na potrzeby drukowania).	• Wprowadza zadania drukowania do demona **piobe**. • Jeśli nie drukuje się z systemu lokalnego, usługę tę należy wyłączyć.
inittab/uprintfd	init	/etc/inittab	Komunikaty jądra.	• Zasadniczo niewymagane. • Wyłączyć.
inittab/writesrv	init	/etc/inittab	Pisanie komunikatów do terminali tty.	• Usługa używana wyłącznie przez interaktywnych użytkowników stacji roboczych UNIX. • Usługę tę należy wyłączyć na serwerach, bazach danych zaplecza i komputerach używanych do celów programistycznych. • Usługę tę należy włączyć na stacjach roboczych.
inittab/xdm	init	/etc/inittab	Tradycyjne zarządzanie terminalem X11.	• Nie włączać na serwerach zaplecza, serwerach produkcyjnych ani serwerach baz danych. • Nie uruchamiać w systemach programistycznych, chyba że wymagane są funkcje zarządzania terminalem X11. • Usługa ta może działać na stacjach roboczych, jeśli potrzebne są funkcje graficzne.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
rc.nfs/automountd		/etc/rc.nfs	Automatyczne systemy plików.	• Jeśli używany jest system NFS, należy włączyć tę usługę na stacjach roboczych. • Nie należy korzystać z funkcji automatycznego podłączania na serwerach programistycznych ani na serwerach zaplecza.
rc.nfs/biod		/etc/rc.nfs	Demon blokowych operacji we/wy (wymagany dla serwera NFS).	• Usługa włączana tylko na potrzeby serwera NFS. • Jeśli nie korzysta się z serwera NFS, należy wyłączyć tę usługę wraz z usługami nfsd i rpc.mountd.
rc.nfs/keyserv		/etc/rc.nfs	Bezpieczny serwer kluczy RPC.	• Zarządza kluczami wymaganymi dla bezpiecznych wywołań RPC. • Usługa ważna dla usług NIS+. • Należy wyłączyć tę usługę, jeśli *nie* korzysta się z systemu NFS ani z usług NIS i NIS+.
rc.nfs/nfsd		/etc/rc.nfs	Usługi NFS (wymagane dla serwera NFS).	• Słabe uwierzytelnianie. • Możliwość wykorzystania do złamania ramki stosu. • Należy włączyć tę usługę na serwerach plików NFS. • Jeśli usługa ta zostanie wyłączona, należy także wyłączyć usługi **biod**, **nfsd** i **rpc.mountd**.
rc.nfs/rpc.lockd		/etc/rc.nfs	Blokady plików NFS.	• Usługę należy wyłączyć, jeśli nie korzysta się z systemu NFS. • Usługę należy wyłączyć, jeśli nie korzysta się z blokad plików w sieci. • Demon **lockd** jest wymieniany na czarnej liście SANS Top Ten Security Threats (Dziesięć największych zagrożeń dla bezpieczeństwa).

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
rc.nfs/rpc.mountd		/etc/rc.nfs	Usługi podłączania plików w systemie NFS (wymagane dla serwera NFS).	• Słabe uwierzytelnianie. • Możliwość wykorzystania do złamania ramki stosu. • Usługę tę należy włączyć tylko na serwerach plików NFS. • Jeśli usługa ta zostanie wyłączona, należy także wyłączyć usługi **biod** i **nfsd**.
rc.nfs/rpc.statd		/etc/rc.nfs	Blokady plików NFS (w celu ich odzyskania).	• Implementuje blokady plików w systemie NFS. • Usługę należy wyłączyć, chyba że korzysta się z systemu NFS.
rc.nfs/rpc.yppasswdd		/etc/rc.nfs	Demon hasła usługi NIS (dla głównego systemu NIS).	• Usługa używana do manipulowania lokalnym plikiem haseł. • Wymagana tylko, gdy dany komputer jest głównym systemem NIS; należy ją wyłączyć we wszystkich innych przypadkach.
rc.nfs/ypupdated		/etc/rc.nfs	Demon aktualizacji systemu NIS (dla podrzędnego systemu NIS).	• Odbiera mapy baz danych systemu NIS dodawane z głównego systemu NIS. • Usługa wymagana tylko, gdy dany komputer jest podrzędnym systemem NIS w stosunku do głównego serwera NIS.
rc.tcpip/autoconf6		/etc/rc.tcpip	Interfejsy IPv6.	• Usługę należy wyłączyć, chyba że korzysta się z protokołu IP w wersji 6.
rc.tcpip/dhcpcd		/etc/rc.tcpip	Protokół DHCP (Dynamic Host Configure Protocol) - klient.	• Serwery zaplecza nie powinny korzystać z przekazywania w protokole DHCP. Usługę tę należy wyłączyć. • Jeśli dany host nie używa protokołu DHCP, usługę należy wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
rc.tcpip/dhcprd		/etc/rc.tcpip	Protokół DHCP (Dynamic Host Configure Protocol) - przekaźnik.	• Przechwytuje rozgłaszane żądania DHCP i przesyła je do serwera w innej sieci. • Zdublowana usługa świadczona przez routery. • Usługę tę należy wyłączyć, jeśli nie korzysta się z protokołu DHCP ani przekazywania informacji między sieciami.
rc.tcpip/dhcpsd		/etc/rc.tcpip	Protokół DHCP (Dynamic Host Configure Protocol) - serwer.	• Odpowiada na żądania DHCP wysyłane podczas przez klientów; przydziela klientom nazwę IP, numer, maskę podsieci i adres rozgłoszeniowy. • Usługę tę należy wyłączyć, jeśli nie korzysta się z protokołu DHCP. • Usługę tę należy wyłączyć dla serwerów produkcyjnych i serwerów zaplecza oraz hostów nie korzystających z protokołu DHCP.
rc.tcpip/dpid2		/etc/rc.tcpip	Przestarzała usługa SNMP.	• Usługę należy wyłączyć, chyba że korzysta się z protokołu SNMP.
rc.tcpip/gated		/etc.rc.tcpip	Bramowy routing między interfejsami.	• Emuluje funkcje routera. • Usługę tę należy wyłączyć i użyć zamiast niej protokołu RIP lub routera.
rc.tcpip/inetd		/etc/rc.tcpip	Usługi inetd.	• W systemie o najwyższym poziomie zabezpieczeń usługi te powinny być wyłączone, jednak nie praktykuje się tego zbyt często. • Wyłączenie tych usług spowoduje wyłączenie zdalnych usług powłoki, które są wymagane przez niektóre serwery poczty i WWW.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
rc.tcpip/mrouted		/etc/rc.tcpip	Routing rozsyłania grupowego	• Emuluje funkcje routera rozsyłania pakietów emisji grupowej między segmentami sieci. • Usługę tę należy wyłączyć. Zamiast niej należy użyć routera.
rc.tcpip/names		/etc/rc.tcpip	Serwer nazw DNS.	• Z usługi tej należy korzystać tylko wtedy, gdy dany komputer jest serwerem nazw DNS. • Usługę tę należy wyłączyć dla stacji roboczych oraz komputerów produkcyjnych i programistycznych.
rc.tcpip/ndp-host		/etc/rc.tcpip	Host protokołu IPv6.	• Usługę należy wyłączyć, chyba że korzysta się z protokołu IP w wersji 6.
rc.tcpip/ndp-router		/etc/rc.tcpip	Routing IPv6.	• Usługę należy wyłączyć, chyba że korzysta się z protokołu IP w wersji 6. Należy zastanowić się nad użyciem routera zamiast tej wersji protokołu IP.
rc.tcpip/portmap		/etc/rc.tcpip	Usługi RPC.	• Usługa wymagana. • Serwery RPC rejestrują się za pomocą demona **portmap**. Klienty, które chcą znaleźć usługi RPC, używają w tym celu demona **portmap**. • Usługę tę należy wyłączyć tylko wtedy, gdy uda się zredukować usługi RPC w takim stopniu, że jedynym działającym demonem jest **portmap**.
rc.tcpip/routed		/etc/rc.tcpip	Routing RIP między interfejsami.	• Emuluje funkcje routera. • Usługę tę należy wyłączyć, jeśli kierowaniem pakietów między sieciami zajmuje się router.
rc.tcpip/rwhod		/etc/rc.tcpip	Zdalny demon "who".	• Gromadzi dane i rozgłasza je do równorzędnych serwerów w tej samej sieci. • Usługę tę należy wyłączyć.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
rc.tcpip/sendmail		/etc/rc.tcpip	Usługa poczty elektronicznej.	• Działa jako użytkownik root. • Usługę tę należy wyłączyć, chyba że dany komputer działa jako serwer poczty. • Jeśli usługa ta jest wyłączona, należy wykonać jedną z poniższych czynności: – Umieścić wpis w tabeli crontab w celu wyzerowania kolejki. W tym celu należy użyć komendy **/usr/lib/sendmail -q**. – Skonfigurować usługi DNS w taki sposób, aby poczta adresowana do danego serwera była kierowana do jakiegoś innego systemu.
rc.tcpip/snmpd		/etc/rc.tcpip	Protokół SNMP (Simple Network Management Protocol).	• Usługę należy wyłączyć, jeśli nie monitoruje się systemu przy użyciu narzędzi SMTP. • Protokół SNMP może być wymagany na serwerach o znaczeniu krytycznym.
rc.tcpip/syslogd		/etc/rc.tcpip	Systemowy protokół zdarzeń.	• Wyłączanie tej usługi *nie* jest zalecane. • Jest ona podatna na ataki typu DoS. • Usługa wymagana w każdym systemie.
rc.tcpip/timed		/etc/rc.tcpip	Stary demon czasu.	• Usługę tę należy wyłączyć i zamiast niej użyć usługi xntp.
rc.tcpip/xntpd		/etc/rc.tcpip	Nowy demon czasu.	• Odpowiada za synchronizację zegarów między systemami. • Usługę tę należy wyłączyć. • Należy skonfigurować inne systemy jako serwery czasu i pozwolić im synchronizować się za pomocą zadania demona cron o nazwie ntpdate.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
logowanie dt		/usr/dt/config/Xaccess	Nieograniczone środowisko CDE.	• Jeśli nie udostępnia się logowania w środowisku CDE dla grupy stacji X11, można ograniczyć użycie komendy dtlogin do konsoli.
usługi anonimowego klienta FTP		użytkownik rmuser -p <nazwa użytkownika>	Anonimowe FTP.	• Udostępnienie anonimowego dostępu do serwera FTP uniemożliwia śledzenie wykorzystania serwera FTP przez konkretnych użytkowników. • Należy usunąć konto użytkownika ftp, o ile takie konto istnieje, w następujący sposób: **rmuser -p ftp**. • Dodatkowym zabezpieczeniem może być wpisanie w pliku `/etc/ftpusers` listy użytkowników, którzy nie powinni mieć dostępu do serwera FTP w danym systemie.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
anonimowy zapis na serwerze FTP			Anonimowe ładowanie plików na serwer FTP.	• Do użytkownika ftp nie powinny należeć żadne pliki. • Anonimowe ładowanie plików na serwer FTP stwarza potencjalne zagrożenie wprowadzenia do systemu kodu o nieprzewidzianym działaniu. • W pliku `/etc/ftpusers` należy wpisać nazwy użytkowników, którzy nie powinni mieć możliwości korzystania z tej funkcji. • Przykłady tworzonych przez system użytkowników, którzy nie powinni mieć możliwości anonimowego ładowania plików na serwer FTP to: root, daemon, bin.sys, admin.uucp, guest, nobody, lpd, nuucp, ladp. • Należy zmienić uprawnienia właściciela i grupy do plików `ftpusers` w następujący sposób: `chown root:system /etc/ftpusers`. • Należy ograniczyć uprawnienia do plików `ftpusers` w następujący sposób: `chmod 644 /etc/ftpusers`.
ftp.restrict			Połączenia protokołu ftp z kontami systemowymi.	• Żaden użytkownik z zewnątrz nie powinien mieć możliwości zastąpienia plików użytkownika root za pomocą pliku `ftpusers`.
root.access		/etc/security/user	Komendy rlogin/telnet na konto użytkownika root.	• Opcji rlogin w pliku `etc/security/user` należy nadać wartość "false". • Każdy, kto chce zalogować się jako użytkownik root, powinien najpierw zalogować się pod swoją własną nazwą, a następnie użyć komendy **su**, aby przełączyć się na konto użytkownika root; w ten sposób powstanie zapis kontrolny.

Usługa	Demon	Uruchamiana przez	Funkcja	Uwagi
snmpd.readWrite		/etc/snmpd.conf	Mechanizmy community readWrite w protokole SNMP.	• Jeśli *nie* korzysta się z protokołu SNMP, należy wyłączyć demon SNMP. • Należy wyłączyć opcje community private i community system w pliku `/etc/snmpd.conf`. • Wspólnotę 'public' należy ograniczyć do tych adresów IP, które monitorują lokalny system.
syslog.conf			Konfigurowanie demona syslogd.	• Jeśli nie skonfigurowano pliku `/etc/syslog.conf`, należy wyłączyć ten demon. • Jeśli wykorzystuje się plik `syslog.conf` do protokołowania komunikatów systemowych, należy pozostawić demon włączony.

Podsumowanie informacji na temat opcji usług sieciowych

Aby osiągnąć wyższy poziom bezpieczeństwa systemu, można zmienić wartości kilku opcji sieciowych na `0` (wyłączyć je) lub na 1 (włączyć je). Poniższa lista zawiera parametry, które mogą być używane wraz z komendą **no**.

Parametr	Komenda	Działanie
bcastping	/usr/sbin/no -o bcastping=0	Zezwala na odpowiedzi na pakiety ICMP echo wysyłane na adres rozgłoszeniowy. Wyłączenie tej opcji uniemożliwi wykonywanie ataków typu Smurf.
clean_partial_conns	/usr/sbin/no -o clean_partial_conns=1	Określa, czy możliwe jest unikanie ataków SYN (synchronizacja numeru kolejnego).
directed_broadcast	/usr/sbin/no -o directed_broadcast=0	Określa, czy dozwolone jest rozgłaszanie kierowane do bramy. Nadanie wartości 0 uniemożliwi wysyłanie kierowanych pakietów do sieci zdalnej.
icmpaddressmask	/usr/sbin/no -o icmpaddressmask=0	Określa, czy system odpowiada na żądania maski adresu ICMP. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.

Parametr	Komenda	Działanie
ipforwarding	/usr/sbin/no -o ipforwarding=0	Określa, czy jądro powinno przekazywać pakiety. Wyłączenie tej opcji uniemożliwi dostęp przekierowanych pakietów do sieci zdalnej.
ipignoreredirects	/usr/sbin/no -o ipignoreredirects=1	Określa, czy mają być przetwarzane odebrane przekierowania.
ipsendredirects	/usr/sbin/no -o ipsendredirects=0	Określa, czy jądro powinno przesyłać sygnały przekierowania. Wyłączenie tej opcji uniemożliwi dostęp przekierowanych pakietów do sieci zdalnej.
ip6srcrouteforward	/usr/sbin/no -o ip6srcrouteforward=0	Określa, czy system przekazuje pakiety IPv6 kierowane według nadawcy. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.
ipsrcrouteforward	/usr/sbin/no -o ipsrcrouteforward=0	Określa, czy system przekazuje pakiety kierowane według nadawcy. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.
ipsrcrouterecv	/usr/sbin/no -o ipsrcrouterecv=0	Określa, czy system akceptuje pakiety kierowane według nadawcy. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.
ipsrcroutesend	/usr/sbin/no -o ipsrcroutesend=0	Określa, czy aplikacje mogą wysyłać pakiety kierowane według nadawcy. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.
nonlocsroute	/usr/sbin/no -o nonlocsrcroute=0	Informuje protokół IP, że tylko pakiety kierowane według nadawcy mogą być adresowane do hosta poza sieć lokalną. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.

Parametr	Komenda	Działanie
tcp_icmpsecure	/usr/sbin/no -o tcp_icmpsecurer=1	Chroni połączenia TCP przed zatkaniem źródła ICMP (Internet Control Message Protocol) oraz atakami PMTUD (Path MTU Discovery - wykrywanie ścieżki MTU). Sprawdza ładunek komunikatu ICMP, aby określić, czy numer kolejny nagłówka TCP należy do dopuszczalnego zakresu. Wartości: 0=wyłączona (domyślnie); 1=włączona.
ip_nfrag	/usr/sbin/no -o ip_nfrag=200	Określa maksymalną liczbę fragmentów pakietu IP, które mogą jednocześnie znajdować się w kolejce składania fragmentów IP (wartość domyślna 200 oznacza, że w kolejce składania fragmentów IP może być do 200 fragmentów pakietu IP).
tcp_pmtu_discover	/usr/sbin/no -o tcp_pmtu_discover=0	Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.
tcp_tcpsecure	/usr/sbin/no -o tcp_tcpsecure=7	Chroni połączenia TCP przed słabymi punktami zabezpieczeń. Wartości: 0=brak zabezpieczeń; 1=wysłanie fałszywego SYN do nawiązanego połączenia; 2=wysłanie fałszywego RST do nawiązanego połączenia; 3=wstawianie danych do nawiązanego połączenia TCP; 5–7=kombinacja powyższych słabych punktów zabezpieczeń.
udp_pmtu_discover	/usr/sbin/no -o udp_pmtu_discover=0	Włącza lub wyłącza wykrywanie jednostki MTU dla ścieżki aplikacji TCP. Wyłączenie tej opcji uniemożliwi dostęp poprzez ataki z wykorzystaniem routingu według nadawcy.

Więcej informacji na temat opcji sieciowych zawiera publikacja *Zarządzanie wydajnością*.

Trusted AIX

Środowisko Trusted AIX włącza mechanizm MLS w systemie AIX.

Uwaga: Mechanizm MLS jest nazywany również bezpieczeństwem opartym na etykietach.

W przeciwieństwie do zwykłego systemu AIX, środowisko Trusted AIX z bezpieczeństwem opartym na etykietach implementuje etykiety dla wszystkich podmiotów i obiektów w systemie.

Uwaga: Opcje instalacji Trusted AIX włączają środowisko systemu AIX z bezpieczeństwem opartym na etykietach. Kontrole dostępu w takim systemie są oparte na etykietach, które zapewniają w środowisku MLS obsługę następujących elementów:

- Obiekty etykietowane: pliki, obiekty IPC, pakiety sieciowe i inne obiekty etykietowane.
- Etykietowane drukarki.
- Sieć zaufana: obsługa RIPSO i CIPSO w IPv4 i IPv6.

Należy zauważyć, że po wybraniu tego trybu instalacji nie ma możliwości powrotu do zwykłego środowiska systemu operacyjnego AIX bez wykonania instalacji nadpisującej zwykłego systemu AIX. Przed wybraniem tego trybu instalacji należy ocenić zapotrzebowanie na środowisko Trusted AIX. Więcej szczegółowych informacji o środowisku Trusted AIX można znaleźć w publicznie dostępnej dokumentacji AIX.

Standardowy system operacyjny AIX udostępnia zestaw opcji bezpieczeństwa, umożliwiających menedżerom danych i administratorom zapewnienie podstawowego bezpieczeństwa systemu i sieci. Podstawowe opcje bezpieczeństwa systemu AIX są następujące:

- Kontrola dostępu do sieci i systemu oparta na nazwie użytkownika i haśle.
- Uprawnienia dostępu do pliku dla użytkownika, grupy i reszty świata.
- Listy kontroli dostępu (ACL).
- Podsystem kontrolujący.
- Kontrola dostępu na podstawie ról (RBAC).

Środowisko Trusted AIX rozbudowuje te podstawowe opcje bezpieczeństwa systemu operacyjnego AIX, poprawiając i rozszerzając bezpieczeństwo systemu AIX w podsystemach sieciowych.

Środowisko Trusted AIX jest kompatybilne z funkcjami API systemu AIX. Dowolna aplikacja działająca w systemie AIX działa również w środowisku Trusted AIX. Jednak z uwagi na dodatkowe ograniczenia bezpieczeństwa, aplikacje niezaprojektowane dla bezpieczeństwa MLS mogą wymagać uprawnień do działania w środowisku Trusted AIX. Aby utworzyć profile aplikacji w takich sytuacjach, należy użyć komendy **tracepriv**.

Środowisko Trusted AIX rozszerza funkcje API systemu AIX o dodatkową funkcjonalność związaną z bezpieczeństwem. Umożliwiają one klientom tworzenie własnych bezpiecznych aplikacji, z wykorzystaniem funkcji API systemu AIX i nowych rozszerzeńTrusted AIX.

Środowisko Trusted AIX umożliwia systemom AIX przetwarzanie informacji na wielu poziomach bezpieczeństwa. Zostało zaprojektowane zgodnie z kryteriami rozszerzonego bezpieczeństwa B1 Departamentu Obrony Stanów Zjednoczonych i europejskich standardów ITSEC.

Informacje dotyczące bezpieczeństwa standardowego systemu AIX zawierają sekcje Zabezpieczenie podstawowego systemu operacyjnego i Zabezpieczenie sieci.

Wprowadzenie do środowiska Trusted AIX

W środowisku Trusted AIX rozszerzono bezpieczeństwo standardowego systemu operacyjnego AIX, udostępniając w systemie operacyjnym środowisko bezpieczeństwa oparte na etykietach.

Środowisko oparte na etykietach Trusted AIX można zainstalować, wybierając opcje w czasie instalacji. Po zainstalowaniu środowiska Trusted AIX nie ma możliwości powrotu do zwykłego środowiska systemu AIX bez wykonania instalacji nadpisującej zwykłego systemu AIX. Zainstalowane środowisko Trusted AIX obejmuje cały system AIX, włącznie z partycjami WPAR w nim utworzonymi. Z bezpieczeństwa opartego na etykietach (określanego również terminem zabezpieczenia wielopoziomowe, MLS) korzysta często przemysł obronny i wywiad, może również być używane w przemyśle. W tym celu należy dostosować etykiety dostępne w środowisku Trusted AIX. Świeża instalacja środowiska Trusted AIX udostępnia etykiety zgodne ze standardowymi implementacjami MLS.

Środowisko Trusted AIX składa się ze zwykłego systemu operacyjnego AIX z dodatkowymi pakietami i zestawami plików. Ponadto przełączniki jądra wymuszają działanie jądra w trybie Trusted AIX. System uruchomiony z dysku CD lub DVD uruchamia się w zwykłym środowisku AIX. Po wyświetleniu menu instalacji użytkownik instalujący może wybrać opcję Trusted AIX i uruchomić instalację plików związanych

z zabezpieczeniami MLS. Po zakończeniu instalacji użytkownik instalujący musi zainicjować sekwencję pierwszego uruchomienia. Podczas pierwszego uruchomienia asystent konfiguracji udostępnia menu dla różnych użytkowników, zostają skonfigurowani użytkownicy ISSO, SA i SO, a system kończy operację uruchomienia, uruchamiając zabezpieczenia MLS.

Środowisko Trusted AIX zwiększa bezpieczeństwo systemu dzięki czterem podstawowym elementom bezpieczeństwa informacji:

- Poufność
- Integralność
- Dostępność
- Odpowiedzialność

Do opcji zabezpieczających udostępnianych przez system AIX środowisko Trusted AIX dodaje następujące możliwości:

Etykiety czułości (Sensitivity labels - SL)
Wszystkie procesy i pliki są oznaczone zgodnie ze swoim poziomem bezpieczeństwa. Procesy mogą uzyskać dostęp tylko do obiektów znajdujących się w ich zasięgu bezpieczeństwa.

Etykiety integralności (Integrity labels - TL)
Wszystkie procesy i pliki są oznaczone zgodnie ze swoim poziomem integralności. Procesy o nie mogą zapisywać do plików o wyższym od własnego poziomie integralności. Procesy nie mogą odczytywać plików o niższym od własnego poziomie integralności.

Opcje bezpieczeństwa pliku
Poszczególne pliki mogą mieć dodatkowe opcje do kontroli operacji związanych z bezpieczeństwem.

Opcje bezpieczeństwa jądra
Cały system może mieć włączone lub wyłączone różne opcje bezpieczeństwa.

Uprawnienia
Wiele komend i wywołań systemowych jest dostępnych tylko dla procesów z konkretnymi uprawnieniami.

Autoryzacje
Każdemu użytkownikowi można nadać unikalny zestaw autoryzacji. Każda autoryzacja umożliwia użytkownikowi wykonanie konkretnych funkcji związanych z bezpieczeństwem. Autoryzacje są przypisywane użytkownikom za pośrednictwem ról.

Role
Funkcja kontroli dostępu w oparciu o role, będąca częścią środowiska Trusted AIX, umożliwia wybiórczą delegację obowiązków administracyjnych do użytkowników innych niż root. W tym celu w jedną rolę zbierane są odpowiednie autoryzacje, a następnie rola ta jest przypisywana użytkownikowi innemu niż root.

Poufność

Zagrożenia związane z ujawnianiem informacji stronom nieautoryzowanym to kwestia poufności.

Środowisko Trusted AIX udostępnia ponowne wykorzystanie obiektów oraz mechanizmy kontroli obiektów do ochrony wszystkich zasobów danych. System operacyjny gwarantuje dostęp do chronionych zasobów danych tylko specjalnie autoryzowanym użytkownikom, którzy nie mogą ani rozmyślnie, ani przypadkowo udostępnić tych zasobów nieautoryzowanym użytkownikom.

Administratorzy mogą zapobiegać zapisaniu newralgicznych plików na dyskietce lub innym nośniku wymiennym, wydrukowaniu na niechronionych drukarkach i przesłaniu siecią do nieautoryzowanych systemów zdalnych. Taka ochrona jest wymuszona przez system operacyjny i nie mogą jej ominąć ani złośliwi użytkownicy, ani nieuczciwe procesy.

Integralność

Zagrożenia związane z modyfikacją informacji przez nieuprawnione podmioty to kwestia integralności.

Środowisko Trusted AIX oferuje liczne mechanizmy zabezpieczeń zapewniające integralność zaufanej bazy przetwarzania i chronionych danych, niezależnie od tego, czy dane te są generowane w systemie, czy importowane z zasobów sieciowych. Różne mechanizmy zabezpieczeń kontroli dostępu gwarantują modyfikację informacji tylko przez autoryzowane podmioty. Aby zapobiec przejęciu lub zablokowaniu zasobów systemu przez złośliwych użytkowników lub wrogie procesy, w środowisku Trusted AIX wyeliminowano uprawnienie użytkownika root. Specjalne autoryzacje i role do administrowania pozwalają na rozdzielenie obowiązków administracyjnych tam, gdzie dotąd konieczne było nadanie użytkownikowi uprawnień użytkownika root.

Dostępność

Zagrożenia związane z dostępem do usług na hoście to kwestia dostępności. Na przykład, jeśli złośliwy program wypełni obszar plików tak, że nie można utworzyć nowego pliku, nadal widać system plików, ale nie ma zapewnionej dostępności.

Środowisko Trusted AIX chroni system przed atakami nieuprawnionych użytkowników i procesów mogących spowodować odmowę usługi. Nieuprawnione procesy nie mogą odczytywać chronionych plików i katalogów ani zapisywać w nich.

Odpowiedzialność

Zagrożenia związane z brakiem wiedzy o tym, które procesy wykonały dane działania w systemie to kwestie odpowiedzialności. Na przykład, jeśli nie można śledzić użytkownika lub procesu dokonującego zmian w systemie, nie można określić, jak w przyszłości zatrzymać takie działanie.

Rozszerzona opcja odpowiedzialności zapewnia identyfikację i uwierzytelnianie wszystkich użytkowników przed udzieleniem zezwolenia na dostęp do systemu. Usługa kontroli daje administratorowi zestaw zdarzeń kontrolowanych i zapis kontrolny wszystkich zdarzeń systemowych związanych z bezpieczeństwem.

Właściwości środowiska Trusted AIX

- Środowisko Trusted AIX jest instalowane z menu instalacyjnego systemu AIX. Podczas instalacji środowiska Trusted AIX można wybrać dodatkowe opcje.
- Środowiska Trusted AIX nie można cofnąć do zwykłego środowiska AIX bez wykonania instalacji nadpisującej zwykłego systemu AIX.
- Użytkownik root ma wyłączoną możliwość logowania się w środowisku Trusted AIX.
- Dowolne partycje WPAR utworzone w środowisku Trusted AIX będą działać również w środowisku bezpieczeństwa opartego na etykietach.
- Trusted AIX obsługuje zarówno obowiązkową kontrolę dostępu (Mandatory Access Control - MAC), jak i obowiązkową kontrolę integralności (Mandatory Integrity Control - MIC). Klient może zdefiniować oddzielne zestawy etykiet dla kontroli MAC i MIC.
- Plik kodowania etykiet znajduje się w katalogu `/etc/security/enc` i przechwytuje informacje translacji etykiety na plik binarny. Domyślny plik kodowania etykiet spełnia wymagania dotyczące nazewnictwa związanego z etykietami specyfikacji CMW (Compartmented Mode Workstations).
- Instalacje NIM są obsługiwane, jeśli są inicjowane przez klienta. Instalacja NIM narzucona przez serwer nie jest możliwa, ponieważ użytkownik root ma wyłączoną możliwość logowania się w systemach MLS.
- Do przechowywania etykiet w systemie AIX włączony został system plików JFS2 (J2) (używający atrybutów rozszerzonych w wersji 2). Inne systemy plików (na przykład J1 lub NFS) można podłączyć w środowisku Trusted AIX tylko jako jednopoziomowe systemy plików (etykieta jest przypisywana do punktu podłączenia).
- W środowisku Trusted AIX zostało wyłączone środowisko X.
- Trusted AIX obsługuje protokoły CIPSO i RIPSO do komunikacji sieciowej opartej na etykietach. Protokoły te są obsługiwane zarówno dla IPv4, jak i IPv6.

- Niektóre mechanizmy bezpieczeństwa systemu AIX są wspólne zarówno dla zwykłego środowiska AIX, jak i Trusted AIX. Dwa z tych mechanizmów to kontrola dostępu oparta na rolach (RBAC) i Zaufane wykonywanie (TE) do weryfikacji integralności.
- Ponieważ użytkownik root jest wyłączany podczas instalacji Trusted AIX, po pierwszym uruchomieniu po instalacji konieczne jest skonfigurowanie haseł użytkowników ISSO, SA i SO. Korzystanie z systemu można rozpocząć dopiero po utworzeniu tych haseł.
- Dokumentacja techniczna (Redbooks) opcji bezpieczeństwa systemu AIX 6 zawiera przykłady użycia oraz inne zagadnienia związane z systemem Trusted AIX.

Zabezpieczenia wielopoziomowe

Głównym zadaniem systemu zabezpieczeń jest egzekwowanie strategii bezpieczeństwa danego ośrodka, aby zagwarantować jego należytą dostępność i rzetelne przypisanie odpowiedzialności za wykonywane operacje.

Strategia bezpieczeństwa w systemie Trusted AIX stanowi zdefiniowany zestaw reguł określających typy dozwolonych operacji w systemie. Określają one mechanizmy odpowiedzialności użytkowników za wykonywane przez nich operacje oraz mechanizmy chroniące system operacyjny przed zmianami.

W systemie Trusted AIX dostęp do plików, katalogów, procesów i urządzeń jest regulowany za pomocą specjalnych mechanizmów kontroli dostępu i kryteriów identyfikacji użytkowników.

Wszystkie zdarzenia związane z utrzymaniem zabezpieczeń w systemie Trusted AIX są rejestrowane w postaci zapisu kontrolnego. Zapis kontrolny umożliwia indywidualne przypisywanie odpowiedzialności nawet w przypadku zastosowania programów modyfikujących efektywny i rzeczywisty identyfikator użytkownika, jak komenda **su**. Ponadto funkcje administracyjne w systemie Trusted AIX są zarezerwowane dla określonych osób dysponujących odpowiednią autoryzacją i najmniejszym koniecznym zestawem uprawnień (nadawany jest im najwęższy zestaw uprawnień umożliwiający użytkownikowi lub procesowi wykonanie danej operacji).

Identyfikacja i uwierzytelnianie

Mechanizmy identyfikacji i uwierzytelniania (I&A) mają gwarantować należytą identyfikację i uwierzytelnianie każdej osoby żądającej dostępu do systemu. Identyfikacja wymaga podania nazwy użytkownika, a uwierzytelnianie wymaga podania hasła.

Wszystkie konta w systemie Trusted AIX są chronione hasłem. Użytkownik z uprawnieniami ISSO może skonfigurować system w taki sposób, aby umożliwić użytkownikowi samodzielne określanie własnego hasła pod rygorem narzuconych wymogów co do jego długości i złożoności. Użytkownik ISSO może też określić minimalne i maksymalne okresy dezaktualizacji haseł niezależnie dla poszczególnych użytkowników, wprowadzając okresy ostrzegawcze przed ostateczną utratą ważności.

Mechanizmy identyfikacji i uwierzytelniania wymagają unikalności wszystkich nazw i identyfikatorów użytkowników. Konta bez ważnych haseł nie mogą być używane podczas logowania. Użytkownik z rolą ISSO musi określić początkowe hasło dla każdego nowego użytkownika. Każdemu użytkownikowi przypisuje się unikalny identyfikator używany dla celów kontroli.

Hasła są przechowywane tylko w postaci zaszyfrowanej. Nigdzie w systemie nie są zapisane hasła w zwykłej postaci tekstowej. Hasła zaszyfrowane znajdują się w specjalnym pliku, od którego dostęp jest zastrzeżony tylko dla uprzywilejowanych procesów. Więcej informacji zawiera opis komendy **passwd**.

W systemach Trusted AIX rozróżnia się dwa typy kont: konto systemowe i konto użytkownika. Konta systemowe są to konta o identyfikatorach poniżej 128. Z kontami systemowymi mogą być skojarzone hasła, jednak nie mogą one służyć do logowania w systemie.

Indywidualna kontrola dostępu

Indywidualna kontrola dostępu (DAC) to te aspekty zabezpieczeń, które znajdują się pod kontrolą właściciela pliku lub katalogu.

Uprawnienia w systemie UNIX

Użytkownik, który jest właścicielem zasobu, może wykonywać następujące czynności:

- Bezpośrednie nadawanie praw dostępu innym użytkownikom.
- Nadawanie innym użytkownikom praw dostępu do kopii.
- Udostępnienie programu umożliwiającego dostęp do oryginalnego zasobu (na przykład przy użyciu programów z ustawionym bitem SUID).

Przykładem funkcjonalności DAC jest tradycyjna metoda bitów uprawnień z systemu UNIX (właściciel/grupa/inne i odczyt/zapis/wykonanie).

Bity uprawnień umożliwiają użytkownikom nadawanie lub odbieranie praw dostępu do danych w pliku użytkownikom i grupom (w oparciu o kryterium znajomości). Ten typ praw dostępu opiera się na identyfikatorze użytkownika i jego przynależności do grup. Ze wszystkimi obiektami w systemie plików są skojarzone uprawnienia, określające zasady dostępu dla właściciela, grupy i innych użytkowników.

Właściciel pliku może także nadawać uprawnienia dostępu innym użytkownikom, zmieniając dla pliku prawa własności lub przynależność do grup za pomocą komend **chown** i **chgrp**.

umask

Bezpośrednio po utworzeniu pliku wszystkie bity uprawnień są włączone. Następnie pewne bity uprawnień zostają usunięte przez proces umask, włączony podczas logowania. Domyślna maska procesu umask ma zastosowanie do każdego pliku utworzonego przez powłokę użytkownika i każdej komendy uruchamianej z poziomu powłoki.

Domyślne ustawienie umask dla elementów jądra jest równe 000 (co oznacza pozostawienie wszystkich uprawnień dostępnych dla wszystkich użytkowników). System AIX ustawia maskę uprawnień jądra na 022, co powoduje wyłączenie bitów zapisu dla grupy i reszty użytkowników. Użytkownicy mogą jednak zmienić to ustawienie.

Uwaga: Zmieniając ustawienie umask na bardziej liberalne niż 022, należy zachować daleko idącą ostrożność. System, w którym pliki i procesy są objęte mniej restrykcyjnymi uprawnieniami, staje się ogólnie mniej bezpieczny.

Są dwie metody modyfikacji domyślnego ustawienia maski umask:

- Można zmienić wartości umask w plikach `.profile`, `.login` lub `.chsrc`. Zmiany te będą dotyczyły każdego pliku tworzonego w trakcie danej sesji logowania.
- Można określać ustawienia umask dla indywidualnych procesów, korzystając z komendy **umask**. Po uruchomieniu komendy **umask** wszystkie nowo tworzone pliki będą objęte nowym ustawieniem umask, dopóki nie nastąpi jedno z dwóch zdarzeń:
  - ponowne wywołanie komendy **umask**

    LUB
  - wyjście z powłoki, w której komenda **umask** została wywołana.

Uruchomienie komendy **umask** bez argumentów powoduje zwrócenie bieżącej wartości umask dla sesji.

Zaleca się rezygnację z określania maski w profilu użytkownika, aby sesja logowania mogła odziedziczyć wartość umask 022 z jądra. Wartości umask mniej restrykcyjne niż 022, należy stosować z najwyższą ostrożnością.

Jeśli potrzebne są dodatkowe uprawnienia do niektórych plików, należy je konfigurować, rozważnie stosując komendę **chmod** po utworzeniu plików.

Listy kontroli dostępu (ACL)

Oprócz standardowych bitów uprawnień i wartości umask systemu UNIX system AIX obsługuje także listy kontroli dostępu (ACL).

Bity uprawnień systemu UNIX kontrolują tylko dostęp dla właściciela pliku, jednej grupy oraz wszystkich użytkowników systemu. Za pomocą listy ACL właściciel pliku może określić uprawnienia dostępu dla dodatkowych użytkowników i grup. Podobnie jak bity uprawnień, listy ACL są skojarzone z indywidualnymi obiektami systemu, takimi jak plik lub katalog.

Bity uprawnień setuid i setgid

Bity uprawnień setuid i setgid (identyfikator użytkownika i identyfikator grupy) umożliwiają uruchamianie pliku programu z użyciem identyfikatora użytkownika lub grupy właściciela pliku, a nie identyfikatora użytkownika lub grupy osoby uruchamiającej program. W tym celu należy ustawić bity setuid i setgid skojarzone z plikiem. Umożliwia to tworzenie chronionych podsystemów, w których użytkownicy mogą otwierać i uruchamiać pewne pliki, nie będąc ich właścicielami.

Jeśli bit setgid zostanie ustawiony dla katalogu nadrzędnego podczas tworzenia obiektu, nowy obiekt będzie miał taką samą grupę, jak katalog nadrzędny, a nie grupę użytkownika, który utworzył obiekt. Jednak obiekty tworzone w katalogu z ustawionym bitem setuid będą należały do użytkownika, który utworzył obiekt, a nie do właściciela katalogu. Bity setuid/setgid katalogu nadrzędnego są dziedziczone przez tworzone w nim podkatalogi.

Bity uprawnień setuid i setgid stwarzają ryzyko naruszenia bezpieczeństwa. Program, którego właścicielem jest użytkownik root, mógłby mieć nieograniczony dostęp do systemu. Jednak w systemach Trusted AIX posługiwanie się uprawnieniami i innymi mechanizmami kontroli dostępu zasadniczo ogranicza to zagrożenie.

Elementy kontroli dostępu na podstawie ról

Trusted AIX obsługuje kontrolę dostępu na podstawie ról (Role Based Access Control - RBAC). Kontrola RBAC jest mechanizmem systemu operacyjnego, za pomocą którego funkcje użytkownika root/administratora systemu mogą być także wykonywane przez zwykłych użytkowników przy użyciu przypisanych do nich ról.

Głównymi elementami kontroli RBAC systemu AIX są:

Autoryzacje
Te łańcuchy określają uprawnioną operację, którą reprezentują i którą sterują bezpośrednio za pomocą nazwy. Na przykład łańcuch autoryzacji `aix.network.manage` definiuje funkcję zarządzania siecią w systemie operacyjnym AIX.

Uprawnienia
Uprawnienie jest atrybutem procesu, który umożliwia procesowi obejście konkretnych ograniczeń systemu. Uprawnienia są powiązane z procesem i zwykle można je uzyskać przez wykonanie uprawnionej komendy.

Role
Role w kontroli RBAC systemu AIX umożliwiają użytkownikom łączenie zbioru funkcji zarządzania w systemie i przypisywanie tych funkcji zwykłym użytkownikom, aby nimi zarządzali. Role w systemie AIX składają się z kolekcji autoryzacji (mogą to być zarówno autoryzacje systemowe, jak i autoryzacje niestandardowe) i innych ról (podról).

Więcej informacji na temat kontroli dostępu na podstawie ról zawiera sekcja dotycząca kontroli RBAC.

Obowiązkowa kontrola dostępu

Obowiązkowa kontrola dostępu to wymuszana przez system metoda ograniczania dostępu do obiektów w oparciu o czułość obiektu i poziom zezwoleń użytkownika. W odróżnieniu od niej, indywidualna kontrola dostępu jest wymuszona przez poszczególnych właścicieli plików, a nie przez system.

Korzystanie z etykiet na potrzeby MAC

System Trusted AIX wymusza ograniczenia MAC za pomocą systemu etykiet. W systemie Trusted AIX wszystkie nazwane obiekty mają etykiety czułości (SL), które identyfikują poziom czułości obiektu. Procesy także mają etykiety czułości. Etykiety SL procesów decydują o tym, na jakim poziomie zabezpieczeń informacje będą dostępne dla procesu. Na ogół proces musi mieć poziom czułości równy lub wyższy niż poziom obiektu, aby uzyskać dostęp do obiektu. Za pomocą etykiet SL można zabezpieczyć pliki przed zapisem lub całkowicie uniemożliwić dostęp do nich zwykłym użytkownikom.

Własne etykiety czułości mają wszystkie obiekty systemowe, takie jak pliki, obiekty IPC, połączenia sieciowe i procesy. Etykiety SL są automatycznie przydzielane w momencie utworzenia obiektu. Wszystkie zrzuty pamięci są uznawane za obiekty i system automatycznie przydziela im etykiety.

Obiekty istniejące już przed instalacją systemu Trusted AIX otrzymują domyślnie etykiety SYSTEM_LOW (SLSL) w chwili ich użycia już po instalacji systemu Trusted AIX. Etykiety SL obiektów nie są ustawiane w sposób permanentny. W celu ustawienia etykiety SL obiektu należy się posłużyć komendą **settxattr**. W przypadku obiektów tworzonych już po instalacji systemu Trusted AIX wartości etykiet SL obiektu są przejmowane z etykiet SL procesu tworzącego obiekt.

Użytkownicy i etykiety

System do każdego konta użytkownika przypisuje zakres poprawnych etykiet SL, zgodnie z domyślnym ustawieniem systemowym albo z indywidualnym ustawieniem użytkownika, a użytkownik może operować tylko w tym zakresie. Proces lub użytkownik mogą tworzyć pliki i katalogi tylko z aktualną etykietą procesu lub użytkownika oraz odczytywać i zapisywać pliki z poszanowaniem narzucanych przez system ograniczeń MAC.

Egzekwowanie ograniczeń MAC

Obowiązkowa kontrola dostępu jest egzekwowana, ilekroć proces usiłuje otworzyć obiekt systemu plików, odczytać atrybuty takiego obiektu, wysłać sygnał do procesu, przesłać dane z użyciem strumienia lub wysłać albo odebrać pakiet za pośrednictwem interfejsu sieciowego. Dostęp do wszelkich obiektów systemu plików jest możliwy tylko pod warunkiem jednoczesnego spełnienia kryteriów MAC i DAC. Kiedy użytkownik próbuje uzyskać dostęp do pliku, ograniczenia MAC są egzekwowane przed sprawdzeniem ograniczeń DAC, takich jak bity uprawnień lub listy kontroli dostępu (ACL).

Dostęp do obiektów systemu plików jest ograniczany nie tylko przez etykiety SL obiektu, lecz także przez etykiety SL katalogu, w którym się on znajduje. Dlatego obiekt systemu plików może być chroniony na innym poziomie czułości (SL katalogu) niż wskazywałaby na to etykieta SL samego obiektu. Obiekt systemu plików może mieć wiele nazw (dowiązań) w różnych katalogach. Wprawdzie każda nazwa (dowiązanie) jest chroniona z użyciem etykiet SL samego pliku docelowego, jednak efektywna ochrona poszczególnych dowiązań może być różna, ponieważ znajdują się one w katalogach mających różne poziomy zabezpieczeń.

Nazwa obiektu jest przechowywana w katalogu, w którym obiekt się znajduje. Dlatego każdy proces z dostępem do katalogu może odczytać nazwy wszystkich obiektów zawartych w tym katalogu. Jednak tylko procesy dysponujące odpowiednimi uprawnieniami mogą odczytywać lub zapisywać zawartość samych obiektów.

Wyświetlanie i modyfikowanie etykiet SL

Etykiety SL obiektów i procesów w systemie można przeglądać za pomocą komendy **lstxattr**. Do ich modyfikowania służy komenda **settxattr**.

Tylko użytkownicy mający odpowiednią autoryzację i procesy z odpowiednimi uprawnieniami mogą zmieniać etykiety SL pliku lub procesu.

Aby zmienić etykietę SL obiektu w systemie plików na SL o niższym poziomie za pomocą komendy **settxattr**, użytkownik musi mieć autoryzację `aix.mls.label.sl.downgrade`. Aby podnieść etykietę SL obiektu w systemie plików na wyższy poziom, użytkownik wymaga autoryzacji `aix.mls.label.sl.upgrade`. Podczas modyfikacji etykiet SL procesów użytkownik wymaga autoryzacji `aix.mls.proc.sl.upgrade` w celu podniesienia jej poziomu i autoryzacji `aix.mls.proc.sl.downgrade` w celu obniżenia poziomu.

Testy MAC dla deskryptorów otwartych plików

W operacjach odczytu/zapisu i prostego dostępu do pliku testy MAC są wykonywane w momencie odwołania się przez proces do pliku. Gdy proces już uzyska deskryptor pliku, może odczytywać i zapisywać dane w pliku, nawet jeśli w międzyczasie etykieta SL procesu zostanie obniżone do poziomu poniżej etykiety SL pliku. Jednak niektóre operacje, jak ustawianie właściciela pliku, uprawnień, etykiet i przywilejów, wiążą się z testem dostępu nawet już po uzyskaniu deskryptora pliku przez proces.

Oznacza to, że testy MAC i rozstrzyganie ścieżki katalogu partycjonowanego nie są wykonywane, dopóki proces korzysta z pliku przy użyciu jego deskryptora. Etykiety SL pliku i/lub procesu mogą się w tym czasie zmieniać i nie wpływa to na możliwość dostępu do pliku.

Obowiązkowa kontrola integralności
Obowiązkowa kontrola integralności to wymuszana przez system metoda ograniczania dostępu do obiektów oraz ich modyfikacji w oparciu o integralność obiektu i poziom zezwoleń użytkownika. Test MAC dotyczy czułości obiektu, natomiast MIC ma związek z jego wiarygodnością.

Korzystanie z etykiet na potrzeby MIC

System Trusted AIX wymusza ograniczenia MIC za pomocą systemu etykiet. W systemie Trusted AIX wszystkie nazwane obiekty mają etykiety integralności (TL), które identyfikują poziom integralności obiektu. Procesy także mają etykiety integralności. Etykiety TL procesów wskazują poziom integralności informacji, który jeszcze umożliwia procesowi dostęp. Im wyższy poziom TL, tym bardziej godny zaufania jest obiekt lub proces.

Aby zmodyfikować obiekt, proces musi być przynajmniej tak samo wiarygodny, jak ten obiekt. Dlatego proces musi mieć etykietę TL równą lub wyższą od etykiety TL obiektu. Na tej zasadzie etykiety integralności pozwalają ograniczać dostęp do pliku, umożliwiając tylko jego odczyt.

Oprócz tego proces nie może używać danych pochodzących z obiektu, który jest mniej godny zaufania niż sam proces. Oznacza to, że obiekt musi mieć etykietę TL równą lub wyższą od etykiety TL procesu.

Etykiety TL mają wszystkie obiekty systemowe, takie jak pliki i procesy. Etykiety TL są automatycznie przydzielane w momencie utworzenia obiektu. Wszystkie zrzuty pamięci są uznawane za obiekty i system automatycznie przydziela im etykiety.

Obiekty istniejące już przed instalacją systemu Trusted AIX otrzymują domyślnie etykiety SYSTEM_LOW (SLTL) w chwili ich użycia już po instalacji systemu Trusted AIX. Etykiety TL obiektów nie są ustawiane w sposób permanentny. W celu ustawienia etykiety TL obiektu należy się posłużyć komendą **settxattr**. W przypadku obiektów tworzonych już po instalacji systemu Trusted AIX ich etykiety TL są ustawiane zgodnie z poziomem integralności procesu tworzącego obiekt.

Użytkownicy i etykiety

System do każdego konta użytkownika przypisuje zakres poprawnych etykiet TL, zgodnie z domyślnym ustawieniem systemowym albo z indywidualnym ustawieniem użytkownika, a użytkownik może operować tylko w tym zakresie. Proces lub użytkownik mogą tworzyć pliki i katalogi tylko z aktualną etykietą procesu lub użytkownika oraz odczytywać i zapisywać pliki z poszanowaniem narzucanych przez system ograniczeń MIC.

Egzekwowanie ograniczeń MIC

Obowiązkowa kontrola integralności jest egzekwowana wszędzie tam, gdzie egzekwowana jest kontrola MAC. Dodatkowo kontrola MIC odbywa się przy okazji usuwania lub zmiany nazwy pliku lub katalogu.

Zmiana etykiet TL

Etykiety TL obiektów i procesów można przeglądać za pomocą komendy **lstxattr**. Do ich modyfikacji służy komenda **settxattr**.

Tylko użytkownicy mający odpowiednią autoryzację i procesy z odpowiednimi uprawnieniami mogą zmieniać etykiety TL pliku lub procesu. Aby zmienić etykietę TL obiektu w systemie plików na TL o niższym poziomie za pomocą komendy **settxattr**, użytkownik musi mieć autoryzację `aix.mls.label.tl.downgrade`. Aby podnieść TL obiektu w systemie plików na wyższy poziom, użytkownik wymaga autoryzacji `aix.mls.label.tl.upgrade`. Podczas modyfikacji etykiet TL procesów użytkownik wymaga autoryzacji `aix.mls.proc.tl.upgrade` w celu podniesienia jej poziomu i autoryzacji `aix.mls.proc.tl.downgrade` w celu obniżenia poziomu.

NOTL

Istnieje specjalna etykieta TL o nazwie NOTL, którą można stosować dla systemów plików, obiektów IPC oraz procesów. W odniesieniu obiektu lub procesu mającego etykietę NOTL nie są wykonywane żadne testy MIC. Tylko użytkownicy uprzywilejowani mogą ustawiać etykietę TL na wartość NOTL lub zmieniać TL z wartości NOTL na inną.

Testy MIC dla deskryptorów otwartych plików

W operacjach odczytu/zapisu i prostego dostępu do pliku testy MIC są wykonywane w momencie odwołania się przez proces do pliku. Gdy proces już uzyska deskryptor pliku, może odczytywać i zapisywać w pliku, nawet jeśli w międzyczasie etykieta TL procesu zostanie obniżone do poziomu poniżej TL pliku. Jednak niektóre operacje, jak ustawianie właściciela pliku, uprawnień, etykiet i przywilejów, wiążą się z testem dostępu nawet już po uzyskaniu deskryptora pliku przez proces. Oznacza to, że testy MIC nie są wykonywane, dopóki proces korzysta z pliku przy użyciu jego deskryptora. Etykiety TL pliku i/lub procesu mogą się w tym czasie zmieniać i nie wpływa to na możliwość dostępu do pliku.

Etykiety

Etykiety reprezentują poziomy bezpieczeństwa podmiotów i obiektów w systemach Trusted AIX. Używane w danym systemie etykiety oraz istniejące między nimi relacje definiuje użytkownik o uprawnieniach ISSO.

Etykiety czułości (Sensitivity labels - SL)

Etykiet SL powiązanych z każdym podmiotem lub obiektem używa się do wymuszenia obowiązkowej strategii kontroli dostępu opartej na modelu kontroli dostępu Bell-LaPadula.

Etykieta SL składa się z dwóch części:

- hierarchicznej klasyfikacji,
- zbioru jednego lub więcej pojemników.

W każdej instalacji serwera można zdefiniować nazwy etykiet i relacje między nimi w danym systemie. Administrator systemu może skonfigurować te nazwy i relacje zgodnie z wymaganiami strategii dla serwera w pliku kodowania etykiet.

Klasyfikacje etykiet SL

Klasyfikacje są uporządkowane hierarchicznie i oznaczają poziom czułości.

Na przykład, jeśli w danym ośrodku stosowane są klasyfikacje `Ściśle tajne`, `Tajne` i `Nieutajnione`, klasyfikacja `Ściśle tajne` jest bardziej restrykcyjna niż `Tajne` a `Tajne` jest bardziej restrykcyjna niż `Nieutajnione`. W systemie Trusted AIX można zdefiniować do 32 tysięcy hierarchicznie ułożonych poziomów klasyfikacji.

Działy SL

Działy są to tematy lub grupy robocze. Każdy dział ma nazwę, na przykład NATO lub CRYPTO.

Działy nie mają naturalnej hierarchii, lecz użytkownik ISSO może nałożyć ograniczenia, zgodnie z którymi działy i klasyfikacje mogą być łączone. W systemie Trusted AIX można zdefiniować do 1024 działów.

Komponenty etykiety SL

W postaci czytelnej dla użytkownika etykieta SL jest reprezentowana przez łańcuch elementów. Pierwszy element reprezentuje klasyfikację, a pozostałe - pojemniki. Elementy są oddzielone spacją.

Na przykład, jeśli plik zawiera ściśle tajne informacje o gospodarce polskiej, hierarchiczną klasyfikacją tego pliku może być ściśle tajne (ST), a pojemnikami mogą być Polska (P) i gospodarka (g). Etykieta SL w postaci czytelnej dla użytkownika będzie miała postać `ST P g` lub `Ściśle tajne Polska gospodarka`.

Relacje między etykietami SL

Użytkownik systemu powinien rozumieć relacje między etykietami i sposób użycia z etykiet.

Między etykietami MAC istnieją trzy typy relacji:

- Dominacja
- Równość
- Nieporównywalność

Dominacja

Mówi się, że jedna etykieta SL (L1) dominuje nad inną etykietą (L2) tylko wtedy, gdy prawdziwe są następujące warunki:

- klasyfikacja etykiety L1 jest równa klasyfikacji etykiety L2 lub ją przekracza,
- zbiór pojemników etykiety L1 całkowicie zawiera zbiór pojemników etykiety L2.

Na przykład, jeśli przyjmiemy, że jedna etykieta SL L1 określa ściśle tajne informacje za pomocą pojemników A i B (ST A B), a inna etykieta SL L2 określa tajne informacje za pomocą pojemnika A, ale nie pojemnika B (T A), to etykieta ST A B będzie dominować nad etykietą T A, ponieważ klasyfikacja ST dominuje nad klasyfikacją T a zbiór pojemników etykiety L1 całkowicie zawiera zbiór pojemników etykiety L2. W tym przykładzie etykieta L2 nie dominuje nad etykietą L1.

Tabela 34. Dominacja etykiety SL

L1		L2		Dominacja
Etykieta	**Pojemnik**	**Etykieta**	**Pojemnik**	
ŚCIŚLE TAJNE	A,B	TAJNE	A	L1 > L2

Równość

Mówi się, że jedna etykieta SL (L1) jest równa innej etykiecie SL (L2) tylko wtedy, gdy prawdziwe są następujące warunki:

- klasyfikacja etykiety L1 jest równa klasyfikacji etykiety L2,
- zbiór pojemników etykiety L1 jest identyczny ze zbiorem pojemników etykiety L2.

Jeśli dwie etykiety są równe, to każda etykieta dominuje drugą etykietę. Na przykład, jeśli przyjmiemy, że jedna etykieta SL dla pliku określa ściśle tajne informacje za pomocą pojemnika A (ST A), a druga etykieta SL określa inny plik ze ściśle tajnymi informacjami zdefiniowanymi za pomocą pojemnika A (także ST A), to te etykiety SL są sobie równe i dominują jedna nad drugą.

Tabela 35. Równość etykiet SL

L1		L2		Dominacja
Etykieta	**Pojemnik**	**Etykieta**	**Pojemnik**	
ŚCIŚLE TAJNE	A	ŚCIŚLE TAJNE	A	L1 = L2

Nieporównywalność

Dwie etykiety SL mogą być rozłączne (etykieta L1 nie jest równa etykiecie L2, etykieta L1 nie dominuje nad etykietą L2, ani etykieta L2 nie dominuje nad etykietą L1). Mówi się, że jedna etykieta SL (L1) jest nieporównywalna z inną etykietą SL (L2) tylko wtedy, gdy następujący warunek jest prawdziwy:

- zbiór pojemników etykiety L1 niecałkowicie zawiera zbiór etykiety L2 i zbiór pojemników etykiety L2 niecałkowicie zawiera zbiór etykiety L1; dlatego etykiety L1 i L2 uważa się za rozłączne.

Na przykład, jeśli przyjmiemy, że plik z etykietą L1 zawiera ściśle tajne informacje w pojemnikach A i B (ST A B) i L2 jest etykietą dla pliku z informacjami klasyfikowanymi w pojemniku C (K C), to etykieta L1 jest nieporównywalna z etykietą L2.

Tabela 36. Nieporównywalne etykiety SL				
L1		**L2**		**Dominacja**
Etykieta	**Pojemnik**	**Etykieta**	**Pojemnik**	
ŚCIŚLE TAJNE	A, B	KLASYFIKOWANE	C	-

Etykiety integralności (Integrity labels - TL)
Etykiety TL reprezentują poziom zaufania względem obiektu systemowego lub procesu. Pod względem struktury etykiety TL przypominają etykiety SL z tą różnicą, że etykiety TL mają tylko klasyfikacje hierarchiczne, a nie mają działów.

Proces może zmodyfikować lub usunąć obiekt tylko pod warunkiem, że etykieta TL procesu dominuje nad etykietą TL obiektu. Proces może usunąć lub zmienić nazwę obiektu tylko w przypadku, gdy etykieta TL procesu dominuje zarówno nad etykietą TL obiektu, jak i nad etykietą TL katalogu zawierającego obiekt. Proces może mieć dostęp do obiektu tylko wtedy, gdy etykieta TL obiektu dominuje nad etykietą TL procesu.

Aby ustalić etykietę TL obiektu lub procesu, należy użyć komendy **lstxattr**. Aby zmienić etykietę TL obiektu lub procesu, należy użyć komendy **settxattr**.

Etykiety podmiotów i obiektów
W systemie Trusted AIX procesy są identyfikowane jako podmioty, a każdy proces ma etykiety SL.

Etykieta SL używana do testów MAC jest nazywana efektywną SL (ESL). Etykieta ESL musi należeć do zakresu zezwoleń procesu. Zakres zezwoleń jest definiowany przez ograniczenie dolne i górne. Ograniczenie górne nosi nazwę maksymalnego zezwolenia (Max CL), a ograniczenie dolne to zezwolenie minimalne (Min CL). Etykiety ESL, Max CL i Min CL są przechowywane w strukturze uprawnień procesu oraz przypisywane podczas tworzenia procesu. Etykieta Max CL musi dominować nad etykietami Min CL i ESL, a etykieta ESL musi dominować nad etykietą Min CL. Do wyświetlania listy i ustawiania etykiet SL procesów służą komendy **settxattr** i **lstxattr**.

Dostęp do różnych obiektów w systemie powinien podlegać kontroli. Obiekt taki może być dowolnego z poniższych typów:

- proces,
- pliki (pliki danych lub binarne),
- obiekty IPC, pakiety sieciowe itp.

Wszystkie obiekty i podmioty w systemie MLS mają etykiety.

Katalog
Z katalogami skojarzone są zakresy etykiet SL definiowane przez maksymalną i minimalną SL. Maksymalna SL powinna dominować nad minimalną SL lub być jej równa. Wszystkie pliki zawarte w katalogu należą tego zakresu.

Pliki
Pliki zwykłe są skojarzone z dwiema etykietami SL, których wartości jednak są zawsze sobie równe. Efektywnie więc mają tylko jedną etykietę SL. Różne wartości obu etykiet SL mogą mieć dowiązania symboliczne.

Pliki specjalne
Pliki specjalne, takie jak urządzenia, tty i fifo mają przypisane minimalną i maksymalną etykietę SL. Katalogi, pliki i pliki specjalne mają tylko jedną etykietę integralności (TL), natomiast procesom przypisuje się minimalną i maksymalną etykietę TL.

Proces
Wszystkie procesy są skojarzone z zakresem minimalnej i maksymalnej czułości zezwoleń, jak również z zakresem minimalnej i maksymalnej integralności zezwoleń. Wartości te są dziedziczone jako odpowiednie wartości zezwoleń użytkownika. Poziomy czułości i integralności, na których proces jest wykonywany, są nazywane odpowiednio efektywnymi poziomami czułości i integralności.

Etykiety zezwoleń użytkownika
Użytkownikom przydziela się etykiety zezwoleń o maksymalnym i minimalnym poziomie czułości (SCL) oraz etykiety zezwoleń o maksymalnej i minimalnej integralności (TCL).

Etykiety zezwoleń o maksymalnym i minimalnym poziomie czułości

Każdy użytkownik ma określoną etykietę maksymalnej czułości zezwolenia (maks. SCL). Etykieta SL czułości efektywnej użytkownika musi być dominowana przez etykietę SL czułości maksymalnej. Etykieta SCL (czułości maksymalnej) to sposób uniemożliwiania pewnym użytkownikom wglądu w dane o krytycznym znaczeniu. Etykieta min. SCL pozwala zapobiegać sytuacjom, w którym użytkownicy mający wysoki poziom w systemie zabezpieczeń przesyłaliby dane użytkownikom z niskim poziomem uprawnień.

Na przykład załóżmy, że użytkownik A ma etykiety maks. SCL i min. SCL równe PUBLIC_A, a użytkownik B ma etykiety maks. SCL i min. SCL równe PUBLIC_B. Gdyby nie było min. SCL, użytkownik A mógłby przekazywać informacje użytkownikowi B, logując się z użyciem etykiety efektywnej SL IMPL_LO i zapisując dane w pliku dostępnym do odczytu dla użytkownika B. Jednak ponieważ min. etykieta SCL jest określona, użytkownik A musi logować się na poziomie PUBLIC_A i może zapisywać pliki tylko na poziomie PUBLIC_A. Pliki zapisane na poziomie PUBLIC_A nie będą dostępne do odczytu dla użytkownika B.

Etykiety zezwoleń o maksymalnej i minimalnej integralności

Każdy użytkownik ma także określoną etykietę maksymalnej integralności zezwolenia (maks. TCL). Efektywna etykieta TL użytkownika musi być dominowana przez etykietę maks. TCL. Etykieta maks. TCL to sposób uniemożliwiania pewnym użytkownikom wglądu w dane o krytycznym znaczeniu. Etykieta min. TCL także pozwala zapobiegać sytuacjom, w którym użytkownicy mający wysoki poziom w systemie zabezpieczeń przesyłaliby dane użytkownikom z niskim poziomem uprawnień.

Etykiety obiektów systemu plików
Wszystkie pliki zawierają informacje dotyczące zabezpieczeń. Nowo tworzony plik dziedziczy SL od procesu, dzięki któremu powstał. SL informacji w pliku można podnosić lub obniżać, odpowiednio podnosząc lub obniżając SL samego pliku.

Katalogom przypisywana jest minimalna i maksymalna etykieta SL podczas tworzenia katalogu. Po utworzeniu oba te parametry są takie same i równe efektywnej etykiecie SL procesu tworzącego, co w efekcie daje katalog jednopoziomowy. Zmiana tych etykiet SL jest dopuszczalna tylko z poziomu kont użytkowników mających wymagane uprawnienia i autoryzacje. Nowe obiekty w tym katalogu mogą być tworzone tylko pod warunkiem, że efektywna etykieta SL procesu tworzącego nowy obiekt mieści się w zakresie etykiet SL katalogu.

Okno jest zazwyczaj tworzone jako odrębny proces potomny z etykietą SL dziedziczoną jako efektywna etykieta SL użytkownika. Urządzenia (na przykład pseudoterminale związane z oknami) także mają skojarzone etykiety SL. Potok nazwany, będący urządzeniem do komunikacji między procesami, dziedziczy efektywną etykietę SL procesu tworzącego ten potok. Strumień, będący urządzeniem służącym jako dwukierunkowy kanał wymiany danych między procesami, także dziedziczy efektywną etykietę SL procesu tworzącego strumień.

Wszystkie urządzenia mają minimalne i maksymalne etykiety SL. Maksymalna etykieta SL musi dominować nad minimalną etykietą SL. Domyślnie minimalne i maksymalne etykiety SL są sobie równe. Proces może uzyskać dostęp do urządzenia w trybie odczytu tylko pod warunkiem, że etykieta SL procesu dominuje nad minimalną etykietą SL urządzenia lub katalogu. Proces może uzyskać dostęp do urządzenia w trybie do zapisu tylko w przypadku, gdy etykieta SL procesu znajduje się w zakresie definiowanym przez minimalne i maksymalne etykiety SL urządzenia lub katalogu.

Opcje bezpieczeństwa pliku

Obiekty mogą być oznaczane opcjami bezpieczeństwa pliku (FSF), które decydują o sposobie postępowania z takimi obiektami przez procesy. Temat Opcje bezpieczeństwa pliku zawiera listę opcji FSF wraz z uprawnieniami wymaganymi do ich ustawiania. Procesy nie mają własnych opcji bezpieczeństwa pliku.

Usuwanie plików
Obiekt można usunąć z systemu plików tylko wtedy, gdy podane poniżej stwierdzenia są prawdziwe.

- Proces próbujący usunąć obiekt musi widzieć nazwę pliku w katalogu zawierającym ten plik. Oznacza to, że proces musi mieć dostęp do przeszukiwania każdego katalogu w ścieżce poniżej katalogu, z którego obiekt ma być usunięty i proces musi mieć efektywną etykietę SL dominującą nad każdym z tych katalogów. Aby wyświetlić nazwę pliku, należy użyć komendy **ls**.
- Proces musi mieć prawo do zapisu w katalogu, z którego obiekt jest usuwany.

Drukowanie plików
Podsystem drukarek automatycznie oznacza odpowiednimi etykietami czułości wszystkie dane wyjściowe. Każdemu zadaniu drukowania automatycznie udostępniana jest strona banera i ostatnia strona, które zawierają wszystkie etykiety i oznaczenia dotyczące bezpieczeństwa.

Tworzenie i odtwarzanie kopii zapasowych plików
Podczas zapisywania danych na dyskach lub taśmach w systemie AIX za pomocą komendy **backup** są do nich dołączane etykiety SL.

Aby importować lub eksportować dane bez etykiet z taśm lub dysków za pomocą komend **backup** i **restore**, wymagana jest autoryzacja SO. Podczas zapisywania danych bez etykiet jest im przypisywana domyślna etykieta SL SYSTEM_LOW w przypadku plików i zakres etykiet SL od SYSTEM_LOW do SYSTEM_HIGH w przypadku katalogów.

Etykiety obiektów IPC
Wszystkie funkcje IPC w systemie AIX dotyczą tworzenia i dostępu do obiektów pośrednich.

W systemie AIX są zdefiniowane trzy różne funkcje IPC:

- kolejki komunikatów,
- semafory,
- pamięć współużytkowana.

Ich działanie polega na tworzeniu i odczytywaniu obiektów pośrednich, nazywanych obiektami IPC, służących do komunikacji między procesami. Każdy obiekt IPC jest chroniony przez zestaw atrybutów podobnych do atrybutów chroniących pliki. Są to:

- identyfikator użytkownika i identyfikator grupy właściciela obiektu;
- identyfikator użytkownika i identyfikator grupy twórcy obiektu;
- tryb dostępu do zasobu, analogiczny do bitów uprawnień dostępu do pliku. Dla każdego obiektu można określić prawa dostępu do odczytu zapisu i wykonania dla wszystkich użytkowników, dla grupy i dla właściciela obiektu.
- numer kolejny pozwalający śledzić wykorzystanie zasobu;
- klucz identyfikujący zasób.

Podobnie jak w przypadku innych obiektów systemowych, system Trusted AIX uzupełnia te atrybuty o dodatkowe atrybuty bezpieczeństwa. W systemie Trusted AIX wszystkie obiekty IPC mają także następujące atrybuty:

- etykieta czułości (SL);
- etykieta integralności (TL).

Za pomocą komendy **settxattr** można wyświetlać wszystkie atrybuty bezpieczeństwa obiektu IPC. Odczytywanie atrybutów obiektu IPC wymaga uprawnień DAC_READ i MAC_READ względem obiektu.

Dostęp do obiektów IPC
Obiekty IPC są tworzone, usuwane i używane za pośrednictwem kilku wywołań systemowych, które omówiono w odpowiednim rozdziale podręcznika programisty systemu Trusted AIX. Typowi użytkownicy nie wykonują tych operacji. W tym temacie przedstawiono ogólny przegląd reguł obowiązujących podczas tworzenia, usuwania i używania obiektów IPC.

Aby uzyskać dostęp do obiektu IPC, proces musi pomyślnie przejść testy uprawnień DAC, MIC i MAC.

Test uprawnień DAC zależy od trybu (właściciel, grupa lub świat) obiektu oraz od identyfikatorów użytkownika i grupy dla procesu. Proces ma wobec obiektu IPC uprawnienia właściciela DAC, jeśli efektywny UID procesu jest identyczny z UID właściciela obiektu lub UID twórcy obiektu. To samo dotyczy uprawnień dla grupy DAC.

Uprawnienia dostępu MAC zależą od etykiet SL procesu i obiektu. Uprawnienia dostępu MIC zależą od etykiet TL procesu i obiektu.

Reguły dostępu do zawartości obiektu IPC są takie same, jak w przypadku atrybutów obiektu IPC. Aby odczytać zawartość lub atrybuty obiektu IPC, wymagane są prawa dostępu `DAC READ`, `MIC READ` i `MAC READ`. Aby wykonać operację zapisu w obiekcie IPC, wymagane są uprawnienia `DAC WRITE`, `MIC WRITE` i `MAC WRITE`.

Dostęp do atrybutów obiektu IPC objęty jest bardziej rygorystycznymi obostrzeniami niż jego zawartość. Zmiana atrybutów obiektu IPC wymaga tym samym większych uprawnień. Aby zmodyfikować standardowe atrybuty systemu AIX, takie jak tryb, proces wymaga uprawnień dostępu do obiektu na poziomie `DAC OWNER` i `MAC WRITE`. Aby zmienić etykietę SL obiektu IPC, proces wymaga wszystkich następujących uprawnień:

- `PV_SL_PROC`
- `DAC OWNER` (tylko zmiana na wersję wcześniejszą)
- `DAC WRITE`
- `MAC WRITE`
- `PV_SL_UG`, aby podnieść etykietę SL, lub `PV_SL_DG`, aby obniżyć etykietę SL
- `PV_MAC_CL` w przypadku istniejącej lub nowej etykiety SL poza zezwoleniem procesu
- `MIC WRITE`

Aby zmienić TL obiektu IPC, proces wymaga wszystkich następujących uprawnień:

- `PV_TL`
- `DAC OWNER`
- `MAC WRITE`
- `MIC WRITE`

Dodatkowo, aby można było zablokować i odblokować segment pamięci wspólnej, proces musi mieć uprawnienie `PV_KER_IPC_O`. Proces wymaga także uprawnienia `PV_KER_IPC`, aby można było zmienić parametr `msg qbytes` kolejki komunikatów w podprogramie msgctl.

Pojęcia pokrewne

“Programowanie w systemie Trusted AIX” na stronie 490
Bezpieczeństwo systemu zależy od oprogramowania zaufanej bazy przetwarzania (baza TCB), sprzętu i oprogramowania wbudowanego. Obejmuje to całe jądro systemu operacyjnego, wszystkie sterowniki urządzeń i moduły STREAMS systemu System V, rozszerzenia jądra oraz wszystkie programy zaufane. Wszystkie pliku używane przez te programy w procesie podejmowania decyzji dotyczących bezpieczeństwa także stanowią część bazy TCB.

Tworzenie i usuwanie obiektów IPC

Podczas tworzenia obiektów IPC nie obowiązują żadne ograniczenia. Kiedy proces tworzy obiekt IPC, obiekt ten dziedziczy etykiety SL i TL procesu.

Tryb dostępu do obiektu IPC należy określić przy użyciu wywołania systemowego, które tworzy obiekt.

Aby usunąć obiekt IPC, proces musi mieć względem niego uprawnienia `DAC OWNER`, `MIC WRITE` i `MAC WRITE`.

Sieć zaufana

Dla rozszerzonych atrybutów bezpieczeństwa zaawansowanych systemów bezpieczeństwa konieczny jest zestaw wymagań dotyczących bezpiecznej sieci. Sieć AIX Trusted Network obsługuje szereg uznanych standardów dotyczących sieci, w tym opcje Revised Internet Protocol Security Option (RIPSO) i

Commercial Internet Protocol Security Option (CIPSO) RFC1108 Departamentu Obrony Stanów Zjednoczonych.

AIX zapewnia obsługę sieci zaufanej zarówno dla IPv4, jak i dla IPv6. Podczas komunikowania się z innymi systemami zaufanymi etykieta SL jest hermetyzowana w opcjach IP zgodnie ze standardami CIPSO/RIPSO. Sprawdzenia MAC są wymuszane w warstwie IP dla etykiet SL, które są wysyłane lub odbierane w pakietach. Dozwolony zakres etykiet jest skonfigurowany za pomocą reguł sieci. Reguły sieci składają się z reguł hosta i reguł interfejsu. AIX Trusted Network instaluje tylko domyślne reguły interfejsu (po jednej regule dla skonfigurowanego interfejsu). Aby zezwolić na bardziej szczegółowe filtrowanie, można skonfigurować reguły hosta. Do skonfigurowania reguł hosta i interfejsu można użyć komendy `netrule`. Do operacji obsługiwanych przez komendę `netrule` należą: dodawanie, usuwanie, nasłuchiwanie i odpytywanie reguł.

Do zainicjowania podsystemu sieci zaufanej i konserwacji bazy danych reguł sieci zaufanej można także użyć komendy `tninit`.

Wyłączenie użytkownika root
Konto użytkownika root jest wyłączone w systemach Trusted AIX. Ma to przede wszystkim na celu zminimalizowanie uszkodzeń, które może spowodować w systemie jeden użytkownik z wszystkimi uprawnieniami.

Wszystkie typy logowania w systemie jako użytkownik root są wyłączone. Tylko komenda **su** umożliwia zalogowanie użytkownika root. Procesom, których właścicielem jest użytkownik root, nie przypisano żadnych uprawnień specjalnych. Programy setuid i inne niż setuid, których właścicielem jest użytkownik root, działają tak jak wcześniej, gdy były wywoływane przez autoryzowanego użytkownika. W przypadku nieautoryzowanych użytkowników program będzie działać, jeśli bity trybu DAC lub list ACL zezwalają na wykonanie, ale programowi nie zostaną przypisane żadne uprawnienia, tak więc program może nie być w stanie wykonać uprawnionych operacji, gdy będzie uruchamiany przez nieautoryzowanych użytkowników. Dlatego nowo instalowanym aplikacjom należy przypisać odpowiednie uprawnienia, jeśli będą one wykonywały uprawnione operacje.

Zadania administrowania systemem mogą wykonywać użytkownicy, którym przypisano rolę Osoby odpowiedzialnej za bezpieczeństwo systemu informacyjnego (ISSO), Administratora systemu (SA) lub Osoby odpowiedzialnej za bezpieczeństwo (SO). Te role umożliwiają jakiemukolwiek użytkownikowi wykonanie zadań administrowania systemem.

Uwaga: Podczas instalacji systemu Trusted AIX dla atrybutu **su** konta użytkownika root ustawiana jest wartość `false`. Aby umożliwić dostęp do konta użytkownika root innym użytkownikom administracyjnym, autoryzowany użytkownik ISSO musi zresetować wartość tego atrybutu na `true`, używając komendy **chuser** i przypisując hasło do tego konta.

Obsługa etykiet podczas kontroli
Podstawowa funkcja podsystemu kontroli to monitorowanie i rejestrowanie zdarzeń związanych z bezpieczeństwem systemu.

Dane udostępniane przez podsystem kontroli umożliwiają rejestrowanie informacji następującego typu:

- próby naruszenia strategii bezpieczeństwa;
- działania związane z systemem bezpieczeństwa i zakończone powodzeniem.

Podsystem kontroli daje użytkownikowi następujące możliwości:

- ustalanie, które zdarzenia mają podlegać kontroli;
- włączanie i wyłączanie kontroli w trakcie pracy systemu;
- płynne przełączanie plików z zapisami kontrolnymi bez utraty informacji;
- przekształcanie danych kontroli do postaci czytelnej dla człowieka;
- wybieranie i przetwarzanie podzbiorów danych kontroli.

Podczas konfigurowania podsystemu kontroli użytkownik ISSO powinien dobrze wiedzieć, co powinno być kontrolowane, jakie mają być warunki prowadzenia kontroli oraz jak należy inicjować i zatrzymywać

kontrolę. Temat Ogólne informacje o kontroli zawiera szczegółowe informacje o konfigurowaniu, uruchamianiu, zatrzymywaniu, administrowaniu i weryfikowaniu systemu kontroli.

Podsystem kontroli zachowuje swój bieżący stan i jest automatycznie uruchamiany ponownie w tym samym stanie po zamknięciu systemu, awarii zasilania, awarii systemu lub w innych okolicznościach powodujących nagłe przerwanie pracy. Podsystem kontroli może się automatycznie wyłączyć, zamknąć system lub zmienić pliki kontroli, jeśli zaistnieje sytuacja uniemożliwiająca dalszy zapis danych w obecnie używanym pliku kontroli. Pliki kontroli mogą być automatycznie przełączane, gdy system plików zapełni się do zadanego poziomu. Jednak w przypadku krytycznej awarii zasilania jest możliwa utrata pewnej liczby rekordów kontroli.

Katalogi wielopoziomowe i partycjonowane
Katalog wielopoziomowy jest to standardowy katalog, któremu zamiast pojedynczej etykiety SL przypisano ich cały zakres. Użytkownik widzi katalog partycjonowany jako pojedynczy katalog. Jednak pliki widoczne z poziomu użytkownika w rzeczywistości znajdują się w ukrytym podkatalogu partycjonowanego katalogu.

Katalogi wielopoziomowe
Katalog wielopoziomowy jest to standardowy katalog, któremu zamiast pojedynczej etykiety SL przypisano ich cały zakres.

Aby przeglądać nazwy plików w katalogu wielopoziomowym, proces musi działać na poziomie bezpieczeństwa wyższym niż minimalna SL katalogu. Aby tworzyć lub usuwać pliki, proces musi operować na poziomie czułości należącym do zakresu SL katalogu wielopoziomowego.

Każdy plik w katalogu wielopoziomowym ma własną etykietę SL i jest chroniony przez standardowe ograniczenia MAC. Jednak każdy proces z dostępem do katalogu może odczytać nazwy wszystkich obiektów zawartych w tym katalogu. Tak więc proces może mieć zezwolenie MAC do odczytu i zapisu w katalogu, lecz może nie mieć uprawnień do odczytu lub zapisu niektórych plików w tym katalogu, mimo że widzi pełną listę ich nazw.

Katalogi partycjonowane
Katalog partycjonowany jest widoczny dla użytkownika jako jeden katalog. Jednak pliki widziane przez użytkownika w rzeczywistości znajdują się w ukrytym podkatalogu katalogu partycjonowanego.

Istnienie katalogów wielopoziomowych pociąga za sobą ryzyko związane z bezpieczeństwem. Proces działający na wysokim poziomie bezpieczeństwa może odczytać plik będący na niższym poziomie bezpieczeństwa, a następnie utworzyć pliki na tym samym wysokim poziomie bezpieczeństwa. Chociaż opcje MAC uniemożliwiają procesom o niższym poziomie bezpieczeństwa odczyt nowych plików, procesy o niższym poziomie bezpieczeństwa nadal widzą nazwy nowych plików. Jeśli proces o wysokim poziomie bezpieczeństwa nada nowym plikom nazwy w oparciu o zawartość oryginalnego pliku o wysokim poziomie bezpieczeństwa, to procesy o niższym poziomie bezpieczeństwa mogą uzyskać dostęp do informacji o wyższym poziomie bezpieczeństwa, odczytując nazwy nowych plików.

Gdy tworzony jest katalog partycjonowany i proces adresuje ten katalog, system tworzy ukryty podkatalog o takiej samej etykiecie SL, jak proces adresujący. Jeśli następnie ten proces utworzy plik, zostanie on utworzony w tym ukrytym podkatalogu. Katalog partycjonowany może zawierać wiele takich ukrytych podkatalogów, ale proces adresujący katalog partycjonowany będzie widział tylko pliki w ukrytym podkatalogu o takiej samej etykiecie SL, jak jego własna. Gdy proces tworzy katalog potomny podkatalogu partycjonowanego, to ten katalog potomny jest partycjonowanym pod-podkatalogiem.

Katalogowi partycjonowanemu przypisywany jest zakres etykiet SL od SYSTEM_LOW do SYSTEM_HIGH. W ten sposób proces może uzyskać dostęp do katalogów partycjonowanych.

Użytkownicy mający autoryzację **aix.mls.pdir.mkdir** mogą tworzyć katalogi partycjonowane, używając komendy **pdmkdir**. Puste katalogi partycjonowane można usuwać za pomocą komendy **pdrmdir**. Do zmiany zwykłego katalogu w katalog partycjonowany można użyć komendy **pdset**. Nie istnieje komenda, która by umożliwiała zmianę katalogu partycjonowanego w zwykły katalog.

W obrębie tego samego katalogu partycjonowanego można tworzyć dowiązanie pliku między jednym podkatalogiem partycjonowanym a wszystkimi innymi istniejącymi podkatalogami partycjonowanymi o wyższej etykiecie SL. Dzięki temu wszystkie procesy z dostępem do tego podkatalogu partycjonowanego

lub do podkatalogów partycjonowanych wyższego poziomu w tym samym katalogu partycjonowanym mają dostęp do tego pliku. Do dowiązywania plików można używać komendy **pdlink**.

Tryby dostępu do katalogu partycjonowanego
Do procesu jest przypisywany jeden z dwóch trybów: tryb rzeczywisty lub tryb wirtualny. Tryb ten określa, w jaki sposób proces widzi katalogi partycjonowane.

Proces w trybie rzeczywistym traktuje katalogi partycjonowane jak standardowe katalogi wielopoziomowe. Dostęp do wszystkich podkatalogów partycjonowanych można uzyskać w taki sam sposób, jak do standardowych katalogów, przy czym podlega on zwykłym ograniczeniom DAC, MIC i MAC. Proces w trybie rzeczywistym może uzyskać dostęp do katalogu partycjonowanego i przejrzeć wszystkie podkatalogi, zgodnie z ograniczeniami DAC, MIC i MAC.

Proces w trybie wirtualnym nigdy nie może wejść do katalogu partycjonowanego. Zamiast tego jest on przekierowywany do podkatalogu partycjonowanego, którego obie - maksymalna i minimalna - etykiety SL są równe efektywnej etykiecie SL procesu.

Proces w trybie rzeczywistym może uruchomić komendę w trybie wirtualnym za pomocą komendy **pdmode** (na przykład: `pdmode ls`). Podobnie, proces w trybie wirtualnym może uruchomić komendę w trybie rzeczywistym także za pomocą komendy **pdmode** (na przykład: `pdmode -r ls`). Wymaga to jednak autoryzacji `aix.mls.pdir.mode`. Mając taką autoryzację, można przełączyć się z powłoki działającej w trybie wirtualnym do powłoki działającej w trybie rzeczywistym, uruchamiając komendę `pdmode -r sh`. Podczas działania w trybie rzeczywistym nie jest wymagana autoryzacja w celu uruchomienia programu w trybie wirtualnym.

Wyświetlanie i zmienianie typów katalogów
Aby wyświetlić typ katalogu jako części atrybutu `secflags`, można użyć komendy **lstxattr**. `FSF_PDIR` wskazuje katalog partycjonowany, `FSF_PSDIR` wskazuje podkatalog partycjonowany, a `FSF_PSSDIR` wskazuje podkatalog podkatalogu partycjonowanego. Aby zmienić zwykły typ katalogu na typ katalogu partycjonowanego, należy użyć komendy **pdset**.

Administrowanie systemem Trusted AIX

Zarządzanie systemem Trusted AIX obejmuje wiele czynników specyficznych dla systemu Trusted AIX.

Instalacja systemu Trusted AIX

System Trusted AIX może zostać włączony tylko w ramach instalacji podstawowego systemu operacyjnego przy użyciu opcji `Model ochrony` z menu instalacji.

Opcja migracji dla systemu Trusted AIX nie jest obsługiwana. W przypadku instalacji zachowującej wymagany jest system plików JFS2. W przypadku bezobsługowej instalacji sieciowej informacje o hasłach powiązanych z domyślnymi kontami administracyjnymi zawiera Tabela 37 na stronie 460.

Tabela 37. Hasła dla domyślnych użytkowników administracyjnych

Użytkownik	**Hasło**
isso	isso
sa	sa
so	so

Tryby uruchamiania

Dostępne są dwa tryby uruchamiania, tryb konfigurowania i tryb pracy, które umożliwiają konfigurowanie i konserwację systemu oraz wykonywanie codziennych operacji.

Po uruchomieniu systemu jest on początkowo dostępny w trybie konfigurowania. Po zainicjowaniu systemu tryb uruchamiania zostaje zmieniony na tryb pracy.

Tryb konfigurowania jest używany do konserwacji i odzyskiwania systemu. Gdy system jest startowany w trybie pojedynczego użytkownika, system ten ma minimalną konfigurację, a sieć jest wyłączona. Trybu

konfigurowania używa się do administrowania newralgicznymi częściami systemu dotyczącymi bezpieczeństwa.

Tryb pracy jest standardowym trybem, w jakim działa system. System jest przełączany do tego trybu, gdy wszystkie zadania, które muszą przejść do domyślnego poziomu działania, zostały zakończone.

Tryb uruchamiania systemu można wyświetlić za pomocą komendy **getrunmode** i zmodyfikować za pomocą komendy **setrunmode**.

Opcje bezpieczeństwa jądra
Opcje bezpieczeństwa jądra służą do włączania i wyłączania niektórych funkcji bezpieczeństwa, jak wymuszanie sprawdzania etykiet, sprawdzania etykiet integralności podczas operacji odczytu oraz do innych celów.

Jądro sprawdza stan opcji bezpieczeństwa jądra przed wymuszaniem testów bezpieczeństwa. Opcje te są obsługiwane tylko w przypadku, gdy jest aktywny model Trusted AIX. W przestrzeni użytkownika opcje te są przechowywane w bazie danych ODM. Zależnie od trybu działania systemu, jądro może sprawdzać obecność odpowiednich opcji zabezpieczeń jądra.

Tabela 38. Opcje zabezpieczeń jądra i wartości domyślne

Opcja zabezpieczeń jądra	Włączona	Wyłączona	Wartość domyślna w trybie wykonawczym	Wartość domyślna w trybie konfiguracyjnym
tnet_enabled	Funkcjonalność sieci zaufanej jest dostępna.	Funkcjonalność sieci zaufanej nie może być używana ani konfigurowana.	Wyłączona	Wyłączona
tl_write_enforced	Wymuszanie MIC w operacjach zapisu, usuwania i zmiany nazwy.	Konfiguracja wykluczająca używanie etykiet TL do testów przy zapisie.	Włączona	Włączona
tl_read_enforced	Wymuszanie MIC w operacjach odczytu.	Konfiguracja wykluczająca używanie etykiet TL do testów przy odczycie.	Wyłączona	Wyłączona
sl_enforced	Wymuszanie MAC.	Konfiguracja wykluczająca używanie etykiet SL do testów przy kontroli dostępu.	Włączona	Wyłączona
trustedlib_enabled	Opcja FSF_TLIB jest uwzględniana dla obiektów systemu plików.	Opcje FSF_TLIB nie są uwzględniane.	Wyłączona	Wyłączona

Ustawianie parametrów jądra
Jądro systemu Trusted AIX można skonfigurować w taki sposób, aby wymuszane były ograniczenia dotyczące bezpieczeństwa zgodnie ze strategiami serwera.

Konfigurację bezpieczeństwa można przeglądać za pomocą komendy **getsecconf** i zmieniać za pomocą komendy **setsecconf**. Dostępne są następujące konfigurowalne parametry jądra:

- wymuszanie etykiety czułości,
- wymuszanie integralności odczytu,

- wymuszanie integralności zapisu,
- zaufana sieć,
- zaufana biblioteka.

Te parametry można skonfigurować tylko wtedy, gdy system jest uruchomiony w trybie konfigurowania.

Konfigurowanie pliku /etc/security/enc/LabelEncodings
Etykiety dla systemu są definiowane w pliku `/etc/security/enc/LabelEncodings`, przy czym możliwe jest ich konfigurowanie dla każdego serwera.

Etykiety mogą być konfigurowane po zainstalowaniu systemu Trusted AIX.

System Trusted AIX ma zdefiniowaną etykietę SL `SYSTEM LOW` (`SLSL`), nad którą dominują wszystkie inne etykiety czułości w systemie, a także etykietę SL `SYSTEM HIGH` (`SHSL`), która dominuje nad wszystkimi innymi etykietami czułości. Na podobnej zasadzie, etykieta TL `SYSTEM LOW` (`SLTL`) jest zdominowana przez wszystkie inne etykiety integralności w systemie, a etykieta TL `SYSTEM HIGH` (`SHTL`) sama dominuje nad wszystkimi innymi etykietami integralności. Definicje te oznaczają najmniejsze i największe wartości SL i TL z pliku `/etc/security/enc/LabelEncodings`.

Podczas uruchamiania systemu Trusted AIX etykiety systemu są pobierane z pliku `/etc/security/enc/LabelEncodings` do jądra. Etykiety mogą być też pobierane do jądra za pomocą komendy **setsyslab**. Etykiety systemowe zdefiniowane w jądrze można wyświetlić przy użyciu komendy **getsyslab**. Po wprowadzeniu modyfikacji w pliku `/etc/security/enc/LabelEncodings` zaleca się ponowne uruchomienie systemu.

Komentarze można umieszczać w pliku `/etc/security/enc/LabelEncodings` wszędzie tam, gdzie może się rozpocząć słowo kluczowe. Komentarze rozpoczynają się znakiem `*` i są interpretowane jako komentarze do końca wiersza.

Plik `/etc/security/enc/LabelEncodings` zawiera informacje o wersji oraz wymienione poniżej sekcje obowiązkowe. Każda sekcja powinna się rozpoczynać od jednego z poniższych słów kluczowych, po którym następuje dwukropek (`:`).

- classifications
- information labels
- sensitivity labels
- clearances
- channels
- printer banners
- accreditation range

Na początku pliku `/etc/security/enc/LabelEncodings` znajduje się wpis `VERSION`. Wpis ten zawiera sekwencję znaków, wśród których mogą być spacje.

W sekcji mogą znajdować się dowolne z wymienionych niżej słów kluczowych. Po tych słowach kluczowych powinien następować średnik (`;`):

name=*nazwa*
Słowo kluczowe definiujące pełną nazwę klasyfikacji lub działu.

sname=*nazwa*
Słowo kluczowe służące do definiowania skróconych nazw. Opcjonalne.

aname=*nazwa*
Alternatywne słowo kluczowe dla klasyfikacji. Opcjonalne.

value=*wartość*
Słowo kluczowe pozwalające określić wewnętrzną wartość klasyfikacji lub działu.

compartments=*bit*
Słowo kluczowe służące do określenia, który bit działu powinien mieć wartość 0 lub 1, jeśli słowo znajduje się w etykiecie.

Ulepszenia formatu kodowania etykiet w systemie Trusted AIX

Format kodowania etykiet opisany w dokumencie Defense Intelligence Agency Document DDS-2600-6216-93 nie uwzględnia etykiet integralności.

Domyślnie etykiety czułości są używane jako etykiety integralności. System Trusted AIX zapewnia obsługę opcjonalnej sekcji etykiet integralności, która może się różnić od sekcji etykiet czułości. Zapewnia to swobodę stosowania innych nazw klasyfikacji i wartości dla etykiet czułości i integralności. Na przykład etykiety czułości mogą mieć przedrostki SL, a etykiety integralności - przedrostki TL, jak poniżej:

Tabela 39. Nazwy klasyfikacyjne i wartości etykiet czułości.

name	**sname**	**value**
`name= SL IMPLEMENTATION LOW`	`sname= SL_IMPL_LO`	`value= 0`
`name= SL UNCLASSIFIED`	`sname= SL_U`	`value= 20`
`name= SL PUBLIC`	`sname= SL_PUB`	`value= 40`
`name= SL SENSITIVE`	`sname= SL_SEN`	`value= 60`
`name= SL RESTRICTED`	`sname= SL_RES`	`value= 80`
`name= SL CONFIDENTIAL`	`sname= SL_CON`	`value= 100`
`name= SL SECRET`	`sname= SL_SEC`	`value= 120`
`name= SL TOP SECRET`	`sname= SL_TS`	`value= 140`

Tabela 40. Nazwy klasyfikacyjne i wartości etykiet integralności.

name	**sname**	**value**
`name= TL IMPLEMENTATION LOW`	`sname= TL_IMPL_LO`	`value= 0`
`name= TL UNCLASSIFIED`	`sname= TL_U`	`value= 20`
`name= TL PUBLIC`	`sname= TL_PUB`	`value= 40`
`name= TL SENSITIVE`	`sname= TL_SEN`	`value= 60`
`name= TL RESTRICTED`	`sname= TL_RES`	`value= 80`
`name= TL CONFIDENTIAL`	`sname= TL_CON`	`value= 100`
`name= TL SECRET`	`sname= TL_SEC`	`value= 120`
`name= TL TOP SECRET`	`sname= TL_TS`	`value= 140`

Sekcja etykiet integralności podlega następującym regułom:

- Sekcja "INTEGRITY LABELS" powinna występować po sekcji "NAME INFORMATION LABELS". W przypadkach, gdy administrator nie zdefiniował opcjonalnej sekcji "NAME INFORMATION LABELS", sekcja "INTEGRITY LABELS" powinna się znajdować po sekcji "ACCREDITATION RANGE".
- W pliku kodowania etykiet powinna być tylko jedna sekcja "INTEGRITY LABELS". Ta sama sekcja dotyczy obiektów i podmiotów.
- Nowa sekcja "INTEGRITY LABELS" jest opcjonalna. W razie jej braku należy korzystać z klasyfikacji podanych w obowiązkowej sekcji "CLASSIFICATIONS".
- Sekcja "INTEGRITY LABELS" powinna być podobna do sekcji "CLASSIFICATIONS". Powinna ona zawierać następujące słowa kluczowe: **"name="**, **"sname="**, **"aname="** i **"value="**. Słowa kluczowe **"initial compartments="** i **"initial markings="**, obecne w sekcji "CLASSIFICATIONS", nie mogą występować w sekcji "INTEGRITY LABELS".
- Zakres danych dla parametru **"value="** jest taki sam, jak obowiązujący w sekcji CLASSIFICATIONS – od 0 do 32000.

Uruchamianie systemu
Zabezpieczenia systemu są wywoływane automatycznie podczas procedury startowej systemu. Należy sprawdzić, czy parametry bezpieczeństwa wyświetlane podczas procedury startowej są poprawne dla systemu.

Konfiguracyjny tryb uruchomienia systemu
Tryb konfiguracyjny służy do konserwowania i przywracania systemu.

System uruchomiony w trybie jednego użytkownika uzyskuje minimalną konfigurację, bez obsługi sieci.

Tryb działania podczas uruchamiania
Trybu działania używa się podczas działania codziennego.

Zwykle system powinien zostać uruchomiony w trybie wielodostępu. Jeśli program autoryzacji startu odbierze poprawną nazwę i hasło użytkownika, system przechodzi do trybu działania, wyświetlany jest ekran konsoli uwierzytelniania logowania, a sprawdzeni użytkownicy mogą się zalogować.

Mechanizmy bezpieczeństwa, takie jak etykiety czułości, indywidualne kontrole dostępu, obowiązkowe kontrole dostępu, sprawdzenia uprawnień, identyfikowanie, uwierzytelnianie oraz autoryzacje, są aktywne zarówno w trybie konfigurowania, jak i w trybie działania - zależnie od odpowiednich opcji konfiguracji bezpieczeństwa. Więcej informacji na ten temat zawiera opis komendy **getsecconf**.

Zaleca się, aby system pracował wyłącznie w trybie działania, dzięki czemu wszystkie oczekiwane funkcje systemu będą dostępne.

Proces uruchomienia systemu
Plik `/etc/inittab` w systemach Trusted AIX został wzbogacony o nowe skrypty startowe. Nowe skrypty to `rc.mls.boot`, `rc.mls.net` i `rc.mls`, wykonywane w podanej kolejności.

Czynności wykonywane w skrypcie `rc.mls.boot` to:

1. Wykonanie interaktywnego testu integralności, aby uzyskać od użytkownika informacje dotyczące obsługi poszczególnych rozbieżności (przy użyciu komendy **trustchk**).
2. Ustawienie opcji bezpieczeństwa trybu konfiguracji jądra (przy użyciu komendy **setsecconf**).
3. Ustawienie etykiet systemowych (minimalne i maksymalne etykiety czułości i integralności).
4. Wyświetlenie opcji bezpieczeństwa trybu konfiguracji jądra na ekranie.

Czynności wykonywane w skrypcie `rc.mls.net` to:

1. Zainicjowanie podsystemu Trusted AIX.
2. Jeśli plik `/etc/security/rules.int` istnieje, załadowanie bazy danych reguł do jądra.

Czynności wykonywane w skrypcie `rc.mls` to:

1. Zainicjowanie podsystemu Trusted AIX.
2. Jeśli plik `/etc/security/rules.int` istnieje, załadowanie bazy danych reguł do jądra.

Uwaga: Wszelkie modyfikacje skryptów startowych mogą spowodować nieprawidłowe działanie systemu.

Konfigurowanie uruchamiania systemu
Nie jest to zalecane, jednak można wyłączyć uwierzytelnianie i sprawdzanie integralności systemu w trakcie jego uruchamiania.

Jeśli uwierzytelnianie i sprawdzanie integralności systemu nie są wyłączone, podczas uruchamiania systemu operator musi być fizycznie obecny przy konsoli.

Wyłączanie uwierzytelniania BOOT
Uwierzytelnianie BOOT można wyłączyć, wywołując komendę **rmitab bootauth** lub korzystając z menu SMIT.

Wyłączanie testu integralności systemu
Automatyczny test integralności wykonywany podczas startu systemu można wyłączyć, usuwając wiersz komendy `trustchk` ze skryptu **rc.mls.boot**.

Zamykanie systemu
Zamknięcie systemu jest operacją wymagającą uprawnień, która jest zabezpieczona za pomocą autoryzacji `aix.system.boot.shutdown`.

System może zamknąć każdy użytkownik pełniący rolę S0 lub inną rolę mającą tę autoryzację.

Odzyskiwanie zaufane
Zasilanie systemu może niekiedy zostać wyłączone przy nieprecyzyjnym stanie. Może to być spowodowane przerwą w zasilaniu, przypadkowym wyłączeniem zasilania lub awarią sprzętu. Trusted AIX może w takich okolicznościach odzyskać sprawność operacyjną bez specjalnych procedur restartowania.

Gdy system jest restartowany, wszystkie mechanizmy zabezpieczeń są aktywne bez względu na sposób wyłączenia zasilania systemu. Podczas procedury uruchamiania systemu wszystkie systemy plików są automatycznie sprawdzanie pod kątem uszkodzeń, zanim użytkownicy będą mogli się zalogować. Skrypty uruchamiające wykonują komendę **fsck**, aby zabezpieczyć lub uczynić niedostępnymi dla nieautoryzowanych użytkowników wszystkie pliki, które zostały uszkodzone lub mogą powodować naruszenie bezpieczeństwa.

Komenda **trustchk** zgłasza wszystkie niespójności w atrybutach bezpieczeństwa plików lub katalogów i wyświetla użytkownikowi interaktywną zachętę do naprawienia tych atrybutów. Komendę **trustchk** należy uruchamiać za każdym razem, gdy integralność systemu plików mogła zostać naruszona. Więcej informacji na ten temat zawiera opis komendy **trustchk**.

Logowanie
Każdy użytkownik systemu Trusted AIX powinien mieć przypisane odpowiednie poziomy czułości i integralności zezwoleń, aby można było zalogować się w systemie.

Zezwolenia użytkownika są definiowane jako atrybuty w pliku `/etc/security/user`. Atrybuty `minsl` i `maxsl` definiują zezwolenie czułości dla użytkownika. Atrybuty `mintl` i `maxtl` definiują zezwolenie integralności użytkownika. Atrybuty `defsl` i `deftl` określają efektywne poziomy czułości i integralności użytkownika przy logowaniu.

Atrybuty zezwoleń mogą być modyfikowane za pomocą komend `chuser` i `chsec` i wyświetlane za pomocą komend `lsuser` i `lssec`.

Użytkownicy mogą wyświetlać własne etykiety, jednak nie mogą ich zmieniać. Aby wyświetlić poziomy zezwoleń innych użytkowników, wymagane jest uprawnienie `aix.mls.clear.read`. Aby modyfikować zezwolenia, konieczne jest uprawnienie `aix.mls.clear.write`.

Aby logowanie było możliwe, muszą być spełnione wszystkie poniższe reguły dominacji:

- Wartość `minsl` musi być zdominowana przez wartość `defsl`.
- Wartość `defsl` musi być zdominowana przez wartość `maxsl`.
- Wartość `mintl` musi być zdominowana przez wartość `deftl`.
- Wartość `deftl` musi być zdominowana przez wartość `maxtl`.

Pożądane poziomy efektywnej czułości i integralności podczas logowania można określić za pomocą opcji **–e** i **–t** w wywołaniu komendy **login**. Więcej informacji zawiera opis komendy **login**.

Aby zalogować się z poziomem czułości wykraczającym poza zakres akredytacji systemu, należy dysponować uprawnieniem `aix.mls.label.outsideaccred`.

System Trusted AIX nie umożliwia logowania się przy użyciu systemowych kont użytkowników (konta z identyfikatorem użytkownika poniżej 128).

Przyczyny niepowodzeń logowania się
Próba zalogowania się może zakończyć się niepowodzeniem z wielu przyczyn.

Próba zalogowania nie powiedzie się, jeśli prawdziwe jest którekolwiek z następujących stwierdzeń:

- wpisano niepoprawny identyfikator logowania,
- wpisano niepoprawne hasło,

- konto jest oznaczone jako zablokowane, ponieważ liczba poprzednich nieudanych prób zalogowania się dla tego konta przekracza limit systemowy,
- port logowania jest oznaczony jako zablokowany, ponieważ liczba poprzednich nieudanych prób zalogowania się dla tego portu przekracza limit systemowy,
- identyfikator logowania nie ma ważnych zezwoleń,
- podana etykieta (lub domyślny poziom wrażliwości lub integralności dla tego identyfikatora logowania, jeśli nie określono etykiety) jest niepoprawna, nie mieści się w zezwoleniach dla tego identyfikatora logowania, nie mieści się w zezwoleniach dla urządzenia logowania lub nie mieści się w zakresie akredytacji systemu,
- użytkownik nie ma dostępu DAC do nazwy ścieżki programu powłoki logowania lub konto użytkownika nie ma dostępu DAC exec do programu powłoki logowania,
- użytkownik nie ma dostępu MAC lub MIC do odczytu do nazwy ścieżki programu powłoki logowania lub nie ma dostępu MAC lub MIC do odczytu do programu powłoki logowania,
- identyfikator UID identyfikatora logowania jest mniejszy niż 128.

Przełączanie użytkownika za pomocą komendy su
W systemie Trusted AIX, gdy zostanie wywołana komenda **su** z opcją **-**, zezwolenia bieżącego użytkownika muszą dominować nad poziomem zezwoleń nowego użytkownika.

Dla etykiety czułości i integralności muszą zostać spełnione następujące warunki:

- maksymalne zezwolenia bieżącego użytkownika muszą dominować nad maksymalnymi zezwoleniami nowego użytkownika,
- minimalne zezwolenia nowego użytkownika muszą dominować nad minimalnymi zezwoleniami bieżącego użytkownika,
- efektywne zezwolenia bieżącego użytkownika muszą być zdominowane przez maksymalne zezwolenia nowego użytkownika i muszą dominować nad minimalnymi zezwoleniami nowego użytkownika.

Obowiązki użytkownika związane z bezpieczeństwem
Użytkownicy mają pewne obowiązki, których muszą być świadomi, które muszą rozumieć i których muszą przestrzegać. Użytkownicy nie mogą ujawniać swoich haseł, muszą zgłaszać zmiany w swoim statusie, zgłaszać podejrzane naruszenia bezpieczeństwa i wykonywać inne czynności.

Hasła

Hasła należy zapamiętać i nie należy ich zapisywać na żadnym nośniku. Jeśli inny użytkownik pozna hasło, może to naruszyć bezpieczeństwo informacji w systemie.

Najbardziej oczywistym zagrożeniem dla zabezpieczenia hasłem jest ujawnienie hasła. Najprostszym sposobem zabezpieczenia konta przed nieautoryzowanym dostępem przez użytkownika, który poznał hasło, jest okresowa zmiana hasła. Hasła należy zmieniać wystarczająco często, aby ograniczyć prawdopodobieństwo naruszenia bezpieczeństwa w czasie obowiązywania danego hasła. Im dłuższy jest okres używania pojedynczego hasła, tym więcej jest możliwości naruszenia bezpieczeństwa.

Jeśli użytkownicy mogą sami określać hasła, nowe hasła muszą zawierać co najmniej sześć znaków, w tym co najmniej dwie litery i jedną cyfrę. Hasło nie powinno odzwierciedlać żadnych osobistych ani zawodowych aspektów użytkownika (na przykład nie może zawierać imienia lub nazwiska przyjaciela, imienia lub nazwiska samego użytkownika, imienia zwierzęcia domowego, zajmowanego stanowiska) i nie powinno być powszechnym słowem, które można znaleźć w słowniku. Schematy służące do odgadnięcia hasła często skanują jeden lub więcej słowników i listę elementów osobistych, takich jak imię i nazwisko użytkownika, imiona dzieci lub zwierząt oraz daty urodzin.

Hasła mogą mieć ograniczony czas życia określony przez użytkownika ISSO. Jeśli hasło utraci ważność i użytkownik będzie próbował zalogować się, zostanie on powiadomiony o konieczności zmiany hasła i o tym, że logowanie będzie możliwe po zmianie hasła. Zaleca się, aby hasła użytkowników były zmieniane w określonym czasie życia hasła. Jeśli istnieje jakiekolwiek podejrzenie, że hasło użytkownika zostało ujawnione, należy je natychmiast zmienić.

Pozostawienie nienadzorowanego systemu

Nigdy nie należy pozostawiać nienadzorowanego systemu, gdy użytkownik jest zalogowany w aktywnej sesji. Gdy użytkownik musi oddalić się od komputera, nawet na krótko, bezwzględnie należy wylogować się z systemu przed oddaleniem się od komputera.

Zarządzanie bezpiecznym systemem

Zarządzanie bezpiecznym systemem komputerowym obejmuje tworzenie i wymuszanie strategii bezpieczeństwa oraz regularne monitorowanie systemu.

Poniższa lista powinna służyć jako punkt początkowy do opracowania strategii zarządzania opcjami bezpieczeństwa systemu użytkownika.

- Maksymalny poziom bezpieczeństwa w zakresie akredytacji systemu nie powinien być wyższy niż maksymalny poziom bezpieczeństwa w miejscu, w którym znajduje się system.
- Sprzęt tworzący system powinien znajdować się w bezpiecznym miejscu. Ogólnie najbezpieczniejszymi miejscami są pomieszczenia wewnętrzne nieznajdujące się na parterze.
- Fizyczny dostęp do sprzętu tworzącego system powinien być ograniczony, monitorowany i udokumentowany.
- Kopie zapasowe systemu i nośniki archiwalne należy przechowywać w bezpiecznym miejscu, innym niż miejsce, w którym znajduje się sprzęt tworzący system. Fizyczny dostęp do tego miejsca należy ograniczyć w ten sam sposób, jak dostęp do sprzętu tworzącego system.
- Dostęp do podręczników obsługi i dokumentacji administracyjnej należy ograniczyć do sytuacji, gdy uzyskanie odpowiednich informacji jest niezbędne.
- Restarty systemu, awarie zasilania i zamknięcia systemu należy rejestrować. Uszkodzenia systemów plików należy rejestrować, a wszystkie pliki, których te uszkodzenia dotyczą, należy przeanalizować pod kątem potencjalnych naruszeń strategii bezpieczeństwa.
- Instalacje nowych programów, importowanych lub utworzonych, należy ograniczyć i monitorować. Nowe programy należy dokładnie sprawdzić i przetestować przed uruchomieniem.
- Nietypowe lub nieoczekiwane zachowanie jakiegokolwiek oprogramowania systemowego należy udokumentować i zaraportować, a jego przyczynę należy określić.
- Gdy tylko jest to możliwe, co najmniej dwie osoby powinny administrować systemem. Jedna osoba powinna pełnić rolę użytkownika `isso`, a druga - użytkownika `sa`.
- Nie należy używać uprawnienia PV_R00T. Wykonywanie programów uprawnionych przez użytkowników ISSO, SA lub SO powinno być wystarczające do administrowania systemem.
- Informacje kontrolne należy gromadzić w dziennikach i regularnie przeglądać. Należy odnotowywać nieregularne lub nietypowe zdarzenia, a ich przyczynę należy zbadać.
- Należy zminimalizować liczbę logowań z wykorzystaniem ról `isso`, `sa` i `so`.
- Liczbę programów setuid i setgid należy zminimalizować, a programy te należy używać wyłącznie w zabezpieczonych podsystemach.
- Uprawnienia przypisywane nowym programom należy określić i zminimalizować, przeglądając uprawnienia przypisane istniejącym programom.
- Atrybuty bezpieczeństwa plików i katalogów należy regularnie sprawdzać za pomocą komendy **`trustchk`**.
- Wszystkie hasła powinny zawierać co najmniej 8 znaków. Sprawdzenie tego powinien regularnie wykonywać użytkownik ISSO.
- Wszyscy użytkownicy powinni mieć poprawną domyślną powłokę logowania. Sprawdzenie tego powinien regularnie wykonywać użytkownik SA.
- Identyfikatory zwykłych użytkowników nie powinny być identyfikatorami systemowymi. Sprawdzenie tego powinien regularnie wykonywać użytkownik SA. Identyfikator systemowy to taki, którego numer UID jest mniejszy niż 128.

Konfiguracja systemu
Użytkownicy ISSO i SA muszą wykonać określone kroki, aby poprawnie skonfigurować system. Użytkownik ISSO jest przede wszystkim odpowiedzialny za zarządzanie bezpieczeństwem, podczas gdy użytkownik SA jest przede wszystkim odpowiedzialny za wykonanie codziennych zadań administracyjnych.

Podane poniżej zadania są wykonywane przez użytkownika ISSO.

- Instalowanie i konfigurowanie podstawowych funkcji bezpieczeństwa, w tym kontroli systemu, rozliczania i bezpieczeństwa urządzeń, które można przydzielać.
- Modyfikowanie skryptów uruchamiania systemu w plikach `/etc/rc.mls` i `/etc/rc.mls.boot`, aby spełnić wymagania strategii bezpieczeństwa serwera.

  Uwaga: Zmiany wprowadzone w skryptach uruchamiania systemu nie są częścią konfiguracji wartościowanej i należy się nimi zająć przed akredytowaniem systemu.
- Konfigurowanie systemowych parametrów logowania.
- Konfigurowanie systemowych parametrów haseł.
- Konfigurowanie zakresu etykiety SL dla urządzeń tty, który umożliwi użytkownikom zalogowanie się w obrębie zakresów etykiet SL podanych dla portów urządzeń tty. Więcej informacji na ten temat zawiera opis komendy **chsec**.
- Konfigurowanie etykiet SL urządzeń systemowych, takich jak napędy taśm i napędy dyskietek. Więcej informacji na ten temat zawiera opis komendy **setsecattr**.
- Ustawianie konfigurowalnych opcji zabezpieczających systemu.

  Uwaga: Zmiany wprowadzone w konfigurowalnych opcjach zabezpieczających nie są częścią konfiguracji wartościowanej i należy się nimi zająć przed akredytowaniem systemu. Zmiana ustawień konfiguracji domyślnej może spowodować, że system będzie działał w trybie niższego poziomu bezpieczeństwa.
- Konfigurowanie zaufanej bazy danych bezpieczeństwa na potrzeby zaufanego startu i zaufanego odzyskiwania. Więcej informacji na ten temat zawiera opis komendy **trustchk**.
- Konfigurowanie grup użytkowników w systemie.

Użytkownicy ISSO i SA wspólnie konfigurują drukarki. Użytkownik SA konfiguruje drukarki w systemie, a użytkownik ISSO konfiguruje zakres etykiet SL drukarek.

Konfiguracja sieci
Użytkownik ISSO jest przede wszystkim odpowiedzialny za bezpieczeństwo sieci, natomiast użytkownik SA ponosi głównie odpowiedzialność za codzienne administrowanie siecią. Użytkownicy ISSO i SA muszą współpracować, aby zapewnić prawidłową konfigurację sieci.

System bezpieczeństwa sieci podczas instalacji systemu Trusted AIX jest konfigurowany z użyciem ustawień domyślnych. Może on także przekazywać etykiety czułości do innych hostów z systemem Trusted AIX istniejących w sieci. Użytkownik ISSO instaluje i konfiguruje podstawowe funkcje sieciowe dostarczane z systemem. Użytkownik ISSO także konfiguruje tabele sieciowe i wywołuje komendę **tninit** w celu zapisania baz danych.

Dostęp do sieci
Podczas nawiązywania połączenia sieciowego z systemem innym niż Trusted AIX lub z systemem Trusted AIX, który nie korzysta z funkcji Trusted Networking, niektóre atrybuty bezpieczeństwa mogą nie być przekazywane przez system inny niż Trusted AIX. W takim przypadku system Trusted AIX stosuje domyślne mechanizmy zabezpieczeń. Domyślne mechanizmy zabezpieczeń ustala administrator systemu.

Konfigurowanie kont użytkowników
Użytkownicy ISSO i SA wspólnie konfigurują konta użytkowników w systemie. Użytkownik ISSO jest przede wszystkim odpowiedzialny za zarządzanie atrybutami użytkowników związanymi z bezpieczeństwem, podczas gdy użytkownik SA jest przede wszystkim odpowiedzialny za obsługę innych atrybutów użytkowników.

Użytkownik ISSO wykonuje podane poniżej zadania dla każdego użytkownika:

- konfigurowanie zezwoleń; więcej informacji na ten temat zawierają opisy komend **chsec** i **chuser**;
- konfigurowanie ról i autoryzacji;
- konfigurowanie grup użytkowników;
- ustawianie poziomu zezwoleń katalogu osobistego; więcej informacji na ten temat zawiera opis komendy **settxattr**;
- ustawianie hasła;
- ustawianie masek kontroli.

Podane poniżej zadania są wykonywane przez użytkownika SA.

- konfigurowanie kont użytkowników,
- informowanie użytkownika ISSO o nowych kontach użytkowników wymagających ustawienia atrybutów bezpieczeństwa.

Konfiguracja systemu plików
W systemie Trusted AIX jest dostępna obsługa większości systemów plików, jednak obsługa atrybutów rozszerzonych związanych z bezpieczeństwem obiektów systemu plików dla systemu Trusted AIX jest zapewniana tylko w środowisku JFS2 z dodatkiem EAv2.

System plików JFS2 z EAv1 jest przekształcany do EAv2 podczas podłączania do systemu Trusted AIX. Pliki w takich systemach plików JFS2 nie mają atrybutów bezpieczeństwa. System odwołuje się do tych plików, korzystając z domyślnych atrybutów SYSTEM_LOW. Atrybuty bezpieczeństwa dla plików można ustawić przy użyciu komendy **settxattr**.

W środowisku sieciowym katalog znajdujący się w jednym systemie może być wyznaczony jako współużytkowany, co oznacza, że katalog ten może być podłączany i używany w innych systemach w sieci, tak jakby był katalogiem głównym systemu plików na lokalnej partycji dysku.

System plików może być wielopoziomowy (MLFS) lub jednopoziomowy (SLFS). W systemie typu MLFS każdy obiekt plikowy ma własną etykietę, natomiast w systemie typu SLFS wszystkie obiekty mają takie same etykiety, jak punkt podłączenia. W systemach typu SLFS nie są obsługiwane katalogi wielopoziomowe ani katalogi partycjonowane.

Dostęp do systemu plików
Kiedy w procesie ma miejsce próba dostępu do obiektu w systemie plików, system sprawdza prawa dostępu do komponentów w każdej ścieżce osobno.

Jeśli proces nie ma dostępu do wyszukiwania względem wszystkich katalogów w ścieżce, nie uzyska dostępu do obiektu. W razie użycia ścieżki względnej system sprawdza uprawnienia dostępu do bieżącego katalogu, bez względu na to, czy na początku ścieżki wystąpiło jawne odwołanie do bieżącego katalogu w postaci kropki (`.`).

Zarządzanie siecią zaufaną
Zarządzanie siecią zaufaną obejmuje wiele zagadnień, w tym konfigurację i bazę danych konfiguracji, specyfikację reguł i składnię netrule, flagi sieci zaufanej i opcje RIPSO/CIPSO.

Ostrzeżenie o konfiguracji domyślnej
Funkcje obsługi sieci w systemie AIX Trusted Network zostały tak zaprojektowane, aby umożliwić uzyskanie każdej potencjalnie przydatnej konfiguracji. Jednak modyfikowanie konfiguracji od wartości domyślnych bez należytej znajomości systemu AIX Trusted Network może być ryzykowne.

Przez niewłaściwe skonfigurowanie komputera można automatycznie obniżyć lub podnieść poziom zabezpieczeń informacji lub też całkowicie usunąć dane systemu bezpieczeństwa. Dlatego wartości domyślne w tabelach sieciowych mogą zmieniać tylko użytkownicy dobrze znający funkcje systemu AIX Trusted Network.

Konfiguracyjna baza danych systemu AIX Trusted Network
Konfiguracja sieci w momencie uruchomienia systemu jest ustalana w oparciu o zawartość plików `rules.host` i `rules.int`.

W przypadku domyślnej instalacji systemu Trusted AIX nie istnieją reguły hosta ani pliki reguł. W celu zapisania nowych lub zmodyfikowanych reguł do pliku można użyć komendy **netrule** z opcją **-u**. Pliki te mają postać binarnych baz danych, na których można operować przy użyciu komendy **tninit**. Aby korzystać z komendy **tninit**, użytkownik musi dysponować uprawnieniem `aix.mls.network.init`.

Wyświetlanie bazy danych reguł systemu AIX Trusted Network
Zawartość bazy danych reguł systemu AIX Trusted Network można wyświetlić za pomocą działania **disp** komendy **tninit**.

Wprowadź następującą komendę, aby dołączyć rozszerzenia **.host** i **.int** do członu *nazwa_pliku* podczas generowania nazw plików bazy danych z regułami hosta oraz z regułami interfejsu. Zawartości obu plików będą wysyłane w czytelnej postaci przez strumień standardowego wyjścia.

```
tninit disp nazwa_pliku
```

Wprowadź następującą komendę, aby wyświetlić domyślną konfigurację startową:

```
tninit disp /etc/security/rules
```

Ładowanie bazy danych reguł systemu AIX Trusted Network
Komenda **tninit** odczytuje zestaw baz danych reguł systemu AIX Trusted Network i ładuje je do jądra, przez co staje się on zestawem aktywnym. Nazwy plików tabel akredytacji hosta i interfejsu są określone tą samą metodą, jak działanie **tninit disp**.

Opcjonalna flaga **-m** określa, że system powinien zachować istniejące reguły hosta. Jeśli flaga **-m** nie zostanie użyta, wszystkie istniejące reguły hosta zostają usunięte przed załadowaniem nowego zestawu aktywnego. Po podaniu flagi **-m** istniejący zestaw reguł jest łączony z nowym zestawem reguł hosta, przy czym w razie konfliktu pierwszeństwo mają nowe reguły. Wszystkie reguły interfejsu są zastępowane, bez względu na użycie flagi **-m**.

Następująca komenda powoduje załadowanie nowych reguł z zachowaniem poprzedniego zestawu reguł:

```
tninit -m load /dir/dir/nazwa_pliku
```

Komenda powoduje użycie pliku podanego w parametrze *nazwa_pliku* i dołączenie rozszerzeń **.host** i **.int** w celu utworzenia dwóch plików, które składają się na bazę danych.

Zapisywanie bazy danych reguł AIX Trusted Network
Do ładowania i zapisywania bazy danych reguł używana jest podobna semantyka.

Do podanej nazwy pliku dodawane jest rozszerzenie **.int** i **.host**, co powoduje utworzenie dwóch plików używanych do przechowywania bazy danych. Działanie save wykonywane przez komendę **tninit** powoduje zapisanie wszystkich reguł, które obecnie są aktywne w jądrze.

Aby utworzyć domyślny zbiór reguł, należy użyć komendy **netrule**, aby dostosować reguły jądra do żądanej strategii bezpieczeństwa serwera, a następnie uruchomić komendę **tninit**. Wykonanie poniższej komendy spowoduje utworzenie plików `/etc/security/rules.int` i `/etc/security/rules.host`:

```
tninit save /etc/security/rules
```

Konfiguracja jądra systemu AIX Trusted Network
Za pomocą komendy **netrule** można kompletnie skonfigurować zestaw reguł jądra systemu AIX Trusted Network odpowiednio do strategii zabezpieczeń danego ośrodka. Wymagane jest do tego uprawnienie względem pliku `aix.mls.network.config`.

Komenda **netrule** może także służyć do manipulowania regułami hosta i interfejsu sieciowego dla jądra. Więcej informacji zawiera opis komendy **netrule**.

Każdy interfejs w systemie musi mieć skojarzoną regułę. Próba usunięcia reguły interfejsu powoduje przywrócenie jej domyślnego stanu. Dodanie nowej reguły interfejsu powoduje zastąpienie przez nią

reguły bieżącej. Domyślną regułę interfejsu można wyświetlić za pomocą zapytania dotyczącego reguły interfejsu z podaniem nazwy interfejsu "default." Na przykład: `# netrule iq default`

Składnia komendy netrule
Składnia komendy **netrule** podlega osobnym regułom w kontekście hostów i interfejsów.

W kontekście hostów komenda **netrule** ma następującą składnię:

netrule h l [**i** | **o** | **io**]

netrule h q { **i** | **o** } *specyfikacja_reguły_hosta_źródłowego specyfikacja_reguły_hosta_docelowego*

netrule h - [{ **i** | **o** } [**u**] [*specyfikacja_reguły_hosta_źródłowego specyfikacja_reguły_hosta_docelowego*]

netrule h + { **i** | **o** } [**u**] *specyfikacja_reguły_hosta_źródłowego specyfikacja_reguły_hosta_docelowego* [*opcje*] [*opcje_RIPSO/CIPSO*] *bezpieczeństwo*

W kontekście interfejsów komenda **netrule** ma następującą składnię:

netrule i l

netrule i q *interfejs*

netrule i + [**u**] *interfejs* [*opcje*] [*opcje_RIPSO/CIPSO*] *bezpieczeństwo*

Pierwszy element, h lub `i`, wskazuje operację na hoście lub interfejsie sieciowym.

W następnej kolejności określana jest operacja. Dostępne są trzy różne działania:

l
Wyświetlenie listy wszystkich reguł

q
Zapytanie o konkretną regułę

-
Usunięcie reguły hosta lub przywrócenie reguły interfejsu do stanu domyślnego

+
Dodanie lub zastąpienie reguły

Trzeci element w regułach hosta określa typ reguły. W przypadku reguł hosta rozróżnia się reguły dla komunikacji przychodzącej i wychodzącej. Reguły wejściowe dotyczą wszystkich pakietów przychodzących, natomiast reguły wyjściowe odnoszą się do wszystkich pakietów wychodzących. Opcja `i` wyróżnia regułę wejściową, a o regułę wyjściową, natomiast opcja `io` lub brak opcji wskazuje regułę dla pakietów przychodzących i wychodzących. Jeśli podczas dodawania reguły hosta lub interfejsu zostanie określony ostatni element u, spowoduje to odpowiednią modyfikację pliku `/etc/security/rules.host` lub `/etc/security/rules.int` po pomyślnym wykonaniu operacji dodania lub usunięcia reguły.

Specyfikacja reguł w systemie AIX Trusted Network
Reguły interfejsu wymagają wprowadzenia nazwy interfejsu sieciowego. Reguły hosta są znacznie bardziej elastyczne, dlatego wymagają określania reguł według bardziej złożonego schematu.

Aby określić interfejs, należy wprowadzić nazwę interfejsu sieciowego, którego reguła ma dotyczyć. Nazwy interfejsów sieciowych mają postać typu `en0`. Do wyświetlenia nazw interfejsów sieciowych można użyć komendy **ifconfig -a**. Należy określić konkretny interfejs, podając tylko jego nazwę. Nie można określić portu, protokołu ani maski podsieci.

Reguły hosta wymagają definiowania według bardziej złożonego schematu. System AIX Trusted Network korzysta z najbardziej szczegółowej spośród reguł mających zastosowanie. Na przykład strategia danego ośrodka może być skonfigurowana w taki sposób, aby reguła hosta z maską 24 dotyczyła wszystkich hostów w podsieci, jednak pojedynczy host w sieci może być objęty osobną, bardziej szczegółową regułą i ona właśnie będzie miała zastosowanie w jego przypadku. Inna, bardziej szczegółowa reguła może też dotyczyć konkretnego portu TCP tego hosta. Dzięki wysokiej elastyczności konfiguracyjnej systemu AIX Trusted Network można łatwo zrealizować rozmaite strategie bezpieczeństwa, odpowiednio do wymagań aplikacji. Dokładna składnia to:

host_źródłowy [**/***maska*] [**=** *proto*] [**:***początek_zakresu_portów* [**:***koniec_zakresu_portów*]]

host_docelowy [**/***maska*] [**=** *proto*] [**:***początek_zakresu_portów* [**:***koniec_zakresu_portów*]]

host_źródłowy
Nazwa hosta, adres IPv4 lub adres IPv6 hosta źródłowego.

host_docelowy
Nazwa hosta, adres IPv4 lub adres IPv6 hosta docelowego.

maska
Maska podsieci. Liczba określa liczbę uwzględnianych bitów z ramki MSB. Jeśli zapis pary adres IPv4/podsieć ma postać *a*.*b*.*c*.*d*/*e*, *e* jest liczbą z zakresu od 0 do 32. Wartość ta określa liczbę jedynek na początku maski podsieci. Na przykład, dla adresu IPv4, `/24` określa maskę sieci `255.255.255.0`, która w zapisie 32-bitowym ma postać `11111111.11111111.11111111.00000000`. Są to 24 jedynki, po których następuje osiem zer.

proto
Numer lub nazwa protokołu, zapisana w pliku `/etc/protocols` (na przykład `=tcp`).

początek_zakresu_portów
Port TCP lub UDP, do którego odnosi się reguła lub początek zakresu, jeśli reguła ma dotyczyć całego zakresu portów. Może to być numer albo nazwa usługi UDP lub TCP, zapisany w pliku `/etc/services`.

koniec_zakresu_portów
Górna granica zakresu portów.

Opis opcji systemu AIX Trusted Network
System AIX Trusted Network ma dwa klastry opcji. Jeśli nie zostaną one określone, używane są dla nich wartości domyślne.

Opcje **-d** i **-r** są używane w sposób następujący:

-d *drop*

drop
Konfiguracja systemu AIX Trusted Network może przewidywać porzucanie wszystkich pakietów.

r
Porzucanie wszystkich pakietów na tym interfejsie.

n
Wszystkie pakiety na tym interfejsie nie będą automatycznie porzucane (domyślne ustawienie interfejsu).

i
Użycie domyślnych ustawień interfejsu (domyślne ustawienie hosta, tylko ustawienie hosta).

-f*rflag***:***tflag*

rflag
Wymagana opcja bezpieczeństwa dla pakietów przychodzących (odbieranych).

r
Tylko RIPSO.

c
Tylko CIPSO.

e
Albo CIPSO, albo RIPSO.

n
Ani CIPSO, ani RIPSO (domyślne ustawienie systemowe).

a
Brak ograniczeń.

i
Użycie ustawień domyślnych interfejsu/systemu (domyślne).

tflag
Obsługa opcji zabezpieczeń dla pakietów wychodzących (wysyłanych).

r
RIPSO dla nagłówków IP wszystkich pakietów wychodzących.

c
CIPSO dla nagłówków IP wszystkich pakietów wychodzących.

i
Użycie domyślnych ustawień interfejsu (domyślne ustawienie hosta, tylko ustawienie hosta).

Opcje RIPSO/CIPSO
Podsystem AIX Trusted Network obsługuje opcje konfigurowania etykietowania pakietów CIPSO i RIPSO.

-rpafs=*pole_PAF* [**,** *pole_PAF*...]

Określa każde *pole_PAF*, które jest akceptowane podczas odbierania pakietów IPSO. Takich pól może być maksymalnie 256.

-epaf=*pole_PAF*

Określa *pole_PAF* dołączane do odpowiedzi na błędy, gdy pakiety błędów są wysyłane za pomocą IPSO w przesyłanych pakietach.

-tpaf=*pole_PAF*

Określa *pole_PAF* stosowane do pakietów wychodzących, gdy w przesyłanych pakietach używana jest opcja IPSO.

*pole_PAF***:NONE** | *PAF* [**+** *PAF*...]

pole_PAF jest kolekcją flag *PAF*. Jedno *pole_PAF* może zawierać pięć pojedynczych flag *PAF*. Są to: **GENSER**, **SIOP-ESI**, **SCI**, **NSA** i **DOE**. *pole_PAF* jest kombinacją tych wartości oddzielonych znakiem (**+**). Na przykład *pole_PAF* zawierające **GENSER** i **SCI** jest reprezentowane przez **GENSER+SCI**. Można użyć ustawienia *pole_PAF* **NONE**, które określa *pole_PAF* bez żadnej ustawionej flagi *PAF*.

-DOI=*domena_interpretacji*

Określa domenę interpretacji dla pakietów CIPSO. Przychodzące pakiety CIPSO muszą mieć tę domenę **DOI**, a wychodzące pakiety CIPSO zostaną oznaczone tą domeną **DOI**.

-tags=*znacznik*[**,***znacznik*...]

*tag***=1** | **2** | **5**

Określa zbiór znaczników, które są akceptowane i dostępne do przesłania przez opcje CIPSO. Jest to kombinacja wartości **1**, **2** i **5** oddzielonych przecinkami. Na przykład kombinacja **1,2** włączy znaczniki **1** i **2**.

Strategia bezpieczeństwa w systemie AIX Trusted Network
Należy określić minimalną, maksymalną i domyślną wartość etykiety SL.

Domyślna wartość SL jest stosowana wobec wszystkich pakietów, które nie zawierają w sobie żadnych informacji o etykiecie SL. Poziomy należy określać według następującej składni:

+*min* **+***maks* **+***domyślne*

Można użyć dowolnej etykiety poprawnej według zasad określonych w pliku kodowania etykiet. Etykiety zawierające spacje nie wymagają cudzysłowów.

Przykłady użycia komendy netrule
Poniżej przedstawiono przykłady zastosowania komendy **netrule**.

Następująca komenda konfiguruje **en0** w taki sposób, aby uniemożliwić przekazywanie opcji bezpieczeństwa i zezwolić na przepuszczanie wszystkich pakietów.

```
netrule i+ en0 +impl_lo +ts all +impl_lo
```

Poniższa komenda konfiguruje hosta **185.0.0.62** w taki sposób, aby akceptował tylko pakiety CIPSO w zakresie od **CONFIDENTIAL A** do **TOP SECRET ALL**:

```
netrule h+i 192.168.0.0 /24 185.0.0.62 -fc:c +confidential a +top secret all +confidential a
```

Poniższa komenda powoduje porzucanie wszystkich pakietów telnet z podsieci:

```
netrule h+i 192.168.0.0 /24 =tcp :telnet 192.0.0.5 -dr +impl_lo    +impl_lo +impl_lo
```

Więcej informacji oraz przykłady zawiera opis komendy **netrule**.

Zarządzanie kontami użytkowników
Informacje identyfikacyjne i uwierzytelniania o każdym użytkowniku są zabezpieczone. Używa się ich do jednoznacznego identyfikowania użytkowników i sprawdzania ich uprawnień dostępu w systemie.

Do informacji identyfikacyjnych użytkownika należą: nazwa użytkownika, nazwa tekstowa ID logowania, ID użytkownika, ID grupy, katalog osobisty, hasło, parametry starzenia się hasła, powłoka, zezwolenia, autoryzacje i maska kontroli. Większość informacji dotyczących użytkowników jest zapisana w następujących plikach:

/etc/passwd
Nazwy użytkowników, ID użytkowników, przypisania do grup podstawowych i katalogi osobiste.

/etc/group
Przypisania do grup dodatkowych i katalogi osobiste.

/etc/security/passwd
Hasła użytkowników w postaci zaszyfrowanej.

/etc/security/user
Ograniczenia logowania, parametry haseł, takie jak minimalna długość, umask.

Pliki `/etc/security/passwd` i `/etc/security/user` nie są dostępne do odczytu przez zwykłych użytkowników. Plik `/etc/security/passwd` jest zabezpieczony bez włączonych bitów dostępu indywidualnego i z etykietą SL SYSTEM_HIGH. Uniemożliwienie zwykłym użytkownikom odczytu zaszyfrowanego hasła eliminuje procedury szyfrowania/porównywania próbujące uzgodnić zaszyfrowane hasło.

Autoryzowani użytkownicy mogą bezpośrednio edytować te pliki, ale częściej do edycji parametrów użytkownika wygodniej jest użyć komendy **smit**. Komenda **smit** wywołuje program SMIT udostępniający menu z zadaniami zarządzania systemem, w tym zadaniami obsługi użytkowników.

ID użytkowników i grup
Istnieją dwie klasy ID użytkowników: ID systemowe i zwykłe ID użytkowników. Identyfikatory systemowe są zastrzeżone dla właścicieli podsystemów zabezpieczonych i specjalnych funkcji administrowania systemem. Identyfikatory zwykłych użytkowników są przypisywane osobom, które interaktywnie korzystają z systemu.

Każdy użytkownik ma unikalny ID użytkownika, identyfikujący go w systemie. Każdemu użytkownikowi można także przypisać jeden lub więcej identyfikatorów grup. Identyfikatory grup są współużytkowane przez użytkowników w tej samej grupie i nie muszą być koniecznie unikalne. Istnieją limity zakresów dotyczące wartości liczbowych używanych dla identyfikatorów. W poniższej tabeli zdefiniowano limity zakresów dla identyfikatorów. Zdefiniowano wartości umożliwiające określenie wystarczającej liczby identyfikatorów systemowych, identyfikatorów zwykłych użytkowników i grup.

Identyfikator użytkownika systemu
0 do 127

Identyfikator zwykłego użytkownika
128 do MAXUID

Identyfikator zwykłej grupy
0 do MAXUID-1

Wartość MAXUID jest zdefiniowana w pliku `/usr/include/sys/param.h`.

Należy zachować ostrożność podczas przypisywania wartości identyfikatorów nowym użytkownikom. Jeśli zwykłemu użytkownikowi zostanie nieumyślnie przypisany ID użytkownika o wartości mniejszej niż 128, użytkownik ten nie będzie mógł zalogować się w systemie.

Nie należy ponownie wykorzystywać ID użytkowników. Gdy użytkownik jest usuwany, zaleca się pozostawienie pozycji w plikach `/etc/passwd` i `/etc/security/passwd` i zablokowanie konta. Zadanie to można wykonać, używając komendy **smit**. Uniemożliwia to użytkownikowi zalogowanie się i zabezpiecza to przed ponownym wykorzystaniem identyfikatora. Dzięki temu, że identyfikator nie zostanie ponownie wykorzystany, nowy użytkownik nie będzie miał dostępu do plików należących do poprzedniego użytkownika, które nie zostały usunięte. Dzięki temu będzie można jednoznacznie odtworzyć zapis kontrolny.

Plikami `/etc/passwd`, `/etc/security/passwd` i `/etc/group` można zarządzać za pomocą komend **mkuser**, **chuser**, **rmuser**, **pwdadm** i **passwd**. Komendy te umożliwiają wymuszenie wszystkich powyższych środków ostrożności oraz obsługę innych zagadnień dotyczących bezpieczeństwa systemu. Komenda **mkuser** umożliwia dodatnie do systemu tylko zwykłych użytkowników.

Uwaga: Należy uważnie wymusić zastosowanie następujących standardów:

- nigdy nie należy ponownie przypisywać poprzedniego ID użytkownika nowemu użytkownikowi,
- nigdy nie należy przypisywać zduplikowanych ID użytkowników,
- nigdy nie należy przypisywać identyfikatora systemowego zwykłemu użytkownikowi,
- nigdy nie należy przypisywać MAXUID jako identyfikatora użytkownika lub grupy.

Hasła
Hasło jest łańcuchem znaków powiązanym z użytkownikiem i używanym do uwierzytelniania użytkownika na początku sesji.

Hasło jest zapisane w postaci zaszyfrowanej w pliku shadow. Hasło w postaci niezaszyfrowanej nie jest nigdzie zapisane w systemie.

Uwaga: Hasła związane z rolami użytkowników są bardzo ważne ze względu na bezpieczeństwo systemu i powinny być cały czas zabezpieczone.

Starzenie się haseł
Użytkownicy mogą zmieniać hasła pod warunkiem, że zostaną spełnione kryteria dotyczące starzenia się haseł.

Funkcja starzenia się haseł wymaga, aby użytkownik zmienił hasło, jeśli istnieje ono w systemie przez zdefiniowany czas. Funkcja ta określa wiek minimalny i maksymalny. Nie można zmienić hasła przed upływem wieku minimalnego. Zmiana hasła jest wymagana po upływie wieku maksymalnego.

Parametry starzenia się haseł można ustawić w pliku `/etc/security/user`. Z funkcją starzenia się haseł związane są następujące parametry:

maxage
Maksymalna liczba tygodni, w ciągu których hasło jest ważne.

maxexpired
Maksymalna liczba tygodni po upływie czasu określonego za pomocą parametru maxage, w ciągu których użytkownik może zmienić hasło.

minage
Minimalna liczba tygodni między zmianami hasła.

minlen
Minimalna długość hasła.

Istnieją także inne parametry, które można ustawić, aby określić znaki dozwolone w haśle. Pełną listę parametrów dotyczących haseł zawiera opis komendy **passwd**.

Powłoka
Podczas pracy w aplikacji, takiej jak edytor tekstu lub arkusz kalkulacyjny, użytkownicy zwykle nie potrzebują pracować interaktywnie z systemem operacyjnym, ponieważ robi to za nich aplikacja. Jednak

niektórzy użytkownicy potrzebują pracować interaktywnie z systemem operacyjnym bez korzystania z interfejsu innej aplikacji.

Gdy potrzebna jest bezpośrednia interakcja z systemem operacyjnym, użytkownicy muszą używać programu powłoki. Program powłoki umożliwia użytkownikom wprowadzanie komend systemu AIX i bezpośredni dostęp do plików oraz katalogów, a ponadto wykonywanie innych operacji. Każdy użytkownik musi mieć domyślny program powłoki podany w pliku `/etc/passwd`. Domyślny program powłoki użytkownika, taki jak `/bin/sh`, `/bin/csh` lub `/bin/ksh`, jest uruchamiany przez komendę **login** lub **xterm**, gdy użytkownik musi użyć powłoki.

Efektywne etykiety SL i TL logowania
Użytkownikom przypisuje się domyślne etykiety SL i TL podczas logowania. Po pomyślnym zalogowaniu domyślne etykiety SL i TL stają się efektywnymi SL i TL procesu użytkownika.

Jeśli użytkownik nie chce logować się przy użyciu domyślnej etykiety SL logowania, może wybrać inną etykietę SL, używając opcji **-e** w wywołaniu komendy **login**. Etykieta SL podana przez użytkownika musi być zdominowane przez poziom zezwolenia użytkownika i zawierać się w zakresie akredytacji użytkownika. Etykietę TL użytkownik może określić podczas logowania za pomocą opcji **-t** w wywołaniu komendy **login**.

Domyślne etykiety SL i TL logowania są zdefiniowane w pliku `/etc/security/user`, razem z nazwą użytkownika i zezwoleniem dla każdego użytkownika. Domyślna etykieta SL użytkownika musi znajdować się w zakresie SL urządzenia tty, określonym w pliku `/etc/security/login.cfg`. Efektywna etykieta SL użytkownika musi być zdominowana przez maksymalną SL urządzenia tty i dominować nad jego minimalną etykietą SL. Efektywna etykieta TL użytkownika musi być równa etykiecie TL urządzenia tty.

Zezwolenia
Podczas logowania do powłoki procesu użytkownika jest przypisywanych sześć etykiet.

Efektywna etykieta SL jest używana przez system w testach MAC. Minimalne zezwolenie SL i maksymalne zezwolenie SL ograniczają z dwóch stron efektywną etykietę SL: efektywna SL nie może dominować nad maksymalnym zezwoleniem SL oraz musi dominować nad minimalnym zezwoleniem SL. Efektywna etykieta TL jest używana przez system w testach MIC. Minimalne zezwolenie TL i maksymalne zezwolenie TL ograniczają z dwóch stron efektywną etykietę TL: efektywna TL nie może dominować nad maksymalnym zezwoleniem TL oraz musi dominować nad minimalnym zezwoleniem TL.

Użytkownik z uprawnieniem ISSO może modyfikować zezwolenie SL, TL, domyślną etykietę SL logowania oraz domyślną etykietę TL logowania dla dowolnego użytkownika. Wartości te są zdefiniowane w pliku `/etc/security/user`.

Podział odpowiedzialności za informacje o użytkownikach
Pojedynczy użytkownik nie może dodawać użytkowników do systemu. Dodawanie użytkowników wymaga współdziałania użytkowników mających uprawnienia SA i ISSO.

Użytkownik z uprawnieniem SA może dodawać informacje o użytkowniku niezwiązane z zabezpieczeniami, takie jak nazwisko, identyfikatory użytkownika i grupy, nazwa tekstowa identyfikatora logowania, powłoka i katalog osobisty. Użytkownik o uprawnieniach ISSO może definiować informacje związane z zabezpieczeniami, jak hasło użytkownika, zezwolenie, maska kontroli oraz role. Wymóg współdziałania dwóch osób zapobiega sytuacji, w której pojedynczy użytkownik z odpowiednim poziomem uprawnień mógłby nadać dowolnemu innemu użytkownikowi uprawnienia do całego systemu.

Rozszerzona kontrola
W systemie Trusted AIX podsystem kontroli został rozszerzony w celu uwzględniania dodatkowych informacji o zabezpieczeniach.

Nowe pola w rekordach kontroli
Następujące pola zostały dodane do wszystkich rekordów kontroli w systemie AIX Trusted AIX. Nowe pola mogą służyć jako kryteria selekcji przy użyciu komendy **auditselect**.

- role kontrolowanego procesu
- efektywna etykieta TL kontrolowanego procesu lub obiektu

- efektywna etykieta SL kontrolowanego procesu lub obiektu
- efektywne uprawnienia kontrolowanego procesu

System Trusted AIX w niektórych zapisach kontrolnych uwzględnia także następujące atrybuty bezpieczeństwa:

- etykieta TL kontrolowanego procesu lub obiektu
- etykieta SL kontrolowanego procesu lub obiektu
- opcje bezpieczeństwa związane z systemem Trusted AIX

Nowe atrybuty bezpieczeństwa można wyświetlać przy użyciu komendy **auditpr** -v.

Zakresy kontroli
System Trusted AIX jest wyposażony w mechanizm umożliwiający administratorom określenie zestawu zakresów kontroli w oparciu o etykiety TL i/lub SL kontrolowanych procesów lub obiektów. Wszystkie obiekty i podmioty, których etykiety TL lub SL znajdują się poza tak zdefiniowanym zakresem, będą podczas kontroli ignorowane.

Aby określić zakresy kontroli dla procesów i obiektów, należy użyć sekcji **war** w pliku `/etc/security/audit/config`:

```
war:
        obj_min_sl = "impl_lo a,b"
        obj_max_sl = "TS a,c"
        sub_min_sl = "impl_lo a,b"
        sub_max_sl = "TS a,c"
        obj_min_tl = impl_lo
        obj_max_tl = TS
        sub_min_tl = impl_lo
        sub_max_tl = TS
```

Wartości **obj_min_sl** i **obj_max_sl** definiują zakres kontroli etykiet SL dla obiektów. Wartości **sub_min_sl** i **sub_max_sl** definiują zakres kontroli etykiet SL dla podmiotów (procesów). Wartości **obj_min_tl** i **obj_max_tl** definiują zakres kontroli etykiet TL dla obiektów. Wartości **sub_min_tl** i **sub_max_tl** definiują zakres kontroli etykiet TL dla podmiotów (procesów).

Sekcja **war** jest odczytywana przez komendę **audit start** i ładowana do jądra przed uruchomieniem podsystemu kontroli. Jeśli sekcja **war** zostanie pominięta, bieżące zakresy kontroli w jądrze zostają usunięte. Jądro nie wykonuje żadnych testów zakresu kontroli etykiet TL ani SL, jeśli nie ma w nim odpowiednich zakresów kontroli.

Flaga jądra systemu Trusted AIX
Jeśli system w momencie instalacji zostanie skonfigurowany jako zaufany (Trusted AIX), spowoduje to uaktywnienie globalnej flagi jądra w zmiennej **_system_configuration**. W jądrze systemu znajduje się makro **__MLS_KERNEL()** pozwalające ustalić, czy system został skonfigurowany jako Trusted AIX. Makro to można wywoływać z poziomu aplikacji przestrzeni użytkowników lub z procedur jądra. Zwrócenie wartości **1** przez makro **__MLS_KERNEL()** wskazuje, że dany system skonfigurowano jako Trusted AIX. Dowolna inna wartość świadczy o tym, że system nie jest skonfigurowany jako Trusted AIX.

Aktualizowanie istniejących programów
Istniejące programy uprzywilejowane i zaufane na ogół działają poprawnie w systemie zaufanym i nie wymagają żadnych zmian.

Jednak wprowadzenie pewnych zmian pozwala zwiększyć poziom zaufania lub poprawić zgodność danego programu z nowszymi wersjami. Wiele zaleceń dotyczących tworzenia nowych programów w równym stopniu dotyczy aktualizowania programów istniejących. W szczególności zastosowanie mają następujące zalecenia:

- Programy testujące, czy są procesami uprzywilejowanymi (czyli czy efektywny identyfikator użytkownika jest równy 0), należy zmodyfikować zgodnie ze wskazówkami podanymi w temacie Bezpośrednie sprawdzanie uprawnień.
- Kod operujący na standardowych bitach uprawnień systemu UNIX (bity trybu) należy zmienić, aby uwzględnić w nim ewentualną obecność list kontroli dostępu.

- Kod uruchamiany z bitem setuid ustawionym na root należy przejrzeć pod kątem wykorzystania uprawnień i przypisać mu odpowiednie uprawnienia.

Tworzenie i odtwarzanie kopii zapasowej
Podczas importu i eksportu danych w systemach Trusted AIX używane są zaufane wersje komend **backup** i **restore**.

Komendy **backup** i **restore** zostały rozszerzone, aby zapewnić obsługę etykiet. Rozszerzenia te są przejrzyste dla użytkownika, a poza obsługą etykiet, komendy te działają identycznie, jak ich standardowe odpowiedniki z systemu AIX. Aby wyłączyć składowanie i odtwarzanie rozszerzonych informacji o zabezpieczeniach, można użyć opcji **-O**.

System importu i eksportu jest chroniony przez połączenie mechanizmów uprawnień i autoryzacji.

Ograniczenia dotyczące komendy cron
Komenda **cron** jest wyłączona i nie będzie wykonywać żadnych zadań w czasie, gdy system znajduje się w trybie konfiguracji. Gdy system działa w zwykłym trybie roboczym, komenda **cron** uruchamia zadania z etykietą czułości, z którą zadanie zostało wprowadzone, z użyciem domyślnej etykiety integralności użytkownika.

Obowiązują ograniczenia, takie jak minimalne i maksymalne poziomy zezwoleń użytkownika. Uwzględniane jest zawsze zezwolenie obowiązujące w czasie, gdy zadanie zostało wprowadzone lub w momencie ostatniego ponownego uruchomienia komendy **cron**, zależnie od tego, które z nich ma późniejszą datę. Komendą **cron** może administrować wyłącznie użytkownik z uprawnieniami SA.

Podłączanie i korzystanie z systemów plików
System Trusted AIX obsługuje stosowanie etykiet (SL i TL) w systemach plików JFS2 z EAv2. Użytkownik SA lub SO może w razie potrzeby podłączyć system plików, który nie obsługuje etykiet (CDFS lub HSFS). W takim przypadku pliki w podłączonym systemie plików nie mają indywidualnych etykiet SL, TL lub FSF, lecz dziedziczą atrybuty bezpieczeństwa punktu podłączenia.

Zarządzanie systemem Trusted AIX
Przestrzeganie zasad dotyczących prawidłowego zarządzania systemem Trusted AIX jest warunkiem utrzymania bezpieczeństwa systemu.

Zarządzanie systemem Trusted AIX należy do zadań określonej grupy użytkowników, których konta są skojarzone z rolami administracyjnymi. Użytkownicy ci to kierownik ds. bezpieczeństwa systemu (ISSO), administrator systemu (SA) i operator systemu (SO), a każdy z nich ma uprawnienia do wykonywania określonej grupy czynności administracyjnych. Użytkownicy ci są skojarzeni z predefiniowanymi rolami w systemie: odpowiednio `isso`, `sa` i `so`. Terminy ISSO, SA i SO są używane w odniesieniu do użytkowników mających odpowiednio role `isso`, `sa` i `so`. Niektóre czynności administracyjne mogą być wykonane tylko przy współudziale dwóch spośród trzech administratorów, ponieważ żaden z nich samodzielnie nie ma wystarczających do tego uprawnień. Na przykład podczas definiowania nowego użytkownika w systemie tylko użytkownik SA może dodać nowe konto użytkownika, a tylko użytkownik ISSO może ustanowić jego hasło, zezwolenie i maskę kontroli. Taki podział pracy jest nazywany regułą dwóch osób.

Uwaga: Skuteczność reguły dwóch osób zależy od faktycznych uprawnień przydzielonych do ról administracyjnych. Przydzielenie roli administracyjnej większej liczby uprawnień niż jest to konieczne naraża system na ataki od wewnątrz. Więcej informacji na temat kojarzenia uprawnień z rolami zawiera temat RBAC.

Zdefiniowane w systemie role `isso`, `sa` i `so` są domyślnie skojarzone z niżej wymienionymi uprawnieniami w systemie Trusted AIX. Podczas zmieniania tych powiązań należy zachować daleko idącą ostrożność, gdyż może to narazić system na ataki.

Tabela 41. Role i uprawnienia

isso	sa	so
		aix.mls.login
	aix.mls.printer	

Tabela 41. Role i uprawnienia (kontynuacja)		
isso	**sa**	**so**
aix.mls.network.config		
aix.mls.network.init		
aix.mls.network.config		
aix.mls.login		
aix.mls.pdir		
aix.mls.system.label		
aix.mls.tpath		
aix.mls.label		
aix.mls.system.config		
aix.mls.proc		
aix.mls.clear		
aix.mls.lef		
aix.mls.stat		
aix.mls.printer		

Zarządzanie systemem dla kierowników ds. bezpieczeństwa systemu (ISSO)
Zarządzaniem systemem Trusted AIX zajmują się łącznie użytkownicy mający role ISSO, SA i SO.

Podczas instalacji systemu Trusted AIX tworzone są trzy domyślne konta użytkowników **isso**, **sa** i **so** (jeśli te konta jeszcze istnieją, w przypadku migracji ze zwykłego systemu AIX do Trusted AIX). Użytkownicy ci są kojarzeni odpowiednio z rolami isso, sa i so.

Uwaga: Domyślne konta mają służyć tylko do zapewnienia początkowej konfiguracji systemu Trusted AIX. Zaleca się, by te role zostały przypisane do innych, zwykłych kont użytkowników. Po przypisaniu tych ról innym użytkownikom domyślne konta użytkowników można usunąć. Podręcznik *Instalowanie i przeprowadzanie migracji* zawiera więcej informacji na temat instalacji systemu Trusted AIX.

Zadania użytkownika ISSO

Zakres odpowiedzialności kierownika ds. bezpieczeństwa systemu (ISSO) obejmuje administrowanie systemem w zakresie jego funkcji bezpieczeństwa. Zadania te może wykonywać tylko użytkownik z uprawnieniami ISSO. Omawiane czynności to między innymi:

- planowanie, wdrażanie i egzekwowanie strategii bezpieczeństwa ośrodka;
- ustalanie ustawień domyślnych na poziomie systemu w zakresie zezwoleń, autoryzacji, uprawnień, kontroli logowania i parametrów haseł;
- konfigurowanie profili uwierzytelniania użytkowników, odzwierciedlających poziom zaufania dla danego użytkownika podczas tworzenia nowych kont przez administratora systemu;
- przypisywanie atrybutów bezpieczeństwa, etykiet SL i etykiet TL urządzeniom takim jak terminale, drukarki, dyski wymienne i napędy taśm magnetycznych;
- przypisywanie zestawów opcji bezpieczeństwa, etykiet, uprawnień i autoryzacji do plików;
- przywracanie systemu do stanu zaufanego w przypadku jego awarii.

Administrowanie systemem kontroli
Dostęp do komend systemu kontroli jest zarezerwowany dla użytkowników mających uprawnienie **AUDITSYS**. Więcej informacji zawierają opisy komend **audit**, **auditselect** i **auditpr**.

Przedstawiony przykład ilustruje wykonanie następujących operacji:

1. Tworzenie systemu plików, w którym będą przechowywane pliki z zapisami kontrolnymi.
2. Uruchamianie systemu kontroli.
3. Doprowadzenie do generowania wybranych rekordów.
4. Analizowanie zapisu kontrolnego w celu odczytania rekordów różnego typu.

Uruchom następujące komendy jako użytkownik z uprawnieniem **FSADMIN**:

```
/usr/sbin/crfs -v jfs -g rootvg -m /audit -a size=32M -A yes
```

```
mount /audit
```

Użyj komendy **/tbin/auctlmod -e** w celu dodania następującego wpisu do sekcji users pliku `/etc/security/audit/config`:

```
nazwa_użytkownika = ALL
```

Parametr *nazwa_użytkownika* zastąp faktyczną nazwą użytkownika umożliwiającą logowanie się w systemie.

Jako użytkownik ISSO utwórz plik o nazwie `/tmp/top_secret` i zmień etykietę SL tego pliku na **TS ALL**.

```
touch /tmp/top_secret
```

```
/usr/sbin/settxattr -f sl= "TS ALL" /tmp/top_secret
```

Uruchom następującą komendę jako użytkownik mający uprawnienie **AUDITSYS**:

```
/usr/sbin/audit start
```

System kontroli został teraz skonfigurowany i uruchomiony i będzie rejestrować działania użytkownika wskazanego przez parametr *nazwa_użytkownika*, gdy tylko zaloguje się on w systemie.

Zaloguj się w systemie, podając nazwę użytkownika podaną w miejsce parametru *nazwa_użytkownika* w pliku `/etc/security/audit/config` i wykonaj następujące komendy:

```
ls -l /tmp/top_secret
```

```
exit
```

Jako użytkownik mający uprawnienie **AUDITSYS** wykonaj następujące komendy:

```
audit shutdown
```

```
$ /usr/sbin/auditselect -e “mac_fail==WILDCARD” /audit/trail | \
/usr/sbin/auditpr -v -APSV > /tmp/audit_trail-mac_failure
```

Zapoznaj się z zapisem kontrolnym skierowanym do pliku `/tmp/audit_trail-mac_failure` i znajdź w nim pozycję **mac_fail**. Parametr auditselect został zmodyfikowany w taki sposób, by akceptować następujące opcje:

- **subj_sl**
- **obj_sl**
- **mac_fail**
- **mac_pass**
- **mic_fail**
- **mic_pass**
- **priv_fail**

- **priv_pass**
- **auth_pass**
- **fsf_fail**
- **fsf_pass**

Wszystkie te opcje jako dopasowywanej wartości używają słowa **WILDCARD**.

Zarządzanie etykietami obiektów i procesów
Z każdym obiektem systemu plików i procesem systemowym są skojarzone etykiety.

Wszystkie obiekty systemu plików z wyjątkiem zwykłych plików mają zakresy etykiet czułości i etykiet integralności. Procesy mają jednocześnie zakresy etykiet czułości i etykiet integralności. Oprócz zakresów, procesy mają także efektywne etykiety SL i TL. Etykiety te wskazują bieżące wartości SL lub TL, z użyciem których proces aktualnie działa. Do wyświetlania etykiet służy komenda **lstxattr**. Do ustawiania etykiet obiektów systemu plików i procesów służy komenda **settxattr**.

Zarządzanie bezpieczeństwem sieci
System AIX Trusted Network wymaga zdefiniowania kilku tabel przez użytkownika ISSO. Tabele te są przechowywane w katalogu /etc/security. Za pomocą komendy **tninit** tabele są następnie przekształcane do postaci binarnej i ładowane do jądra.

Sposób, w jaki system traktuje przychodzące i wychodzące pakiety sieciowe, definiują reguły hosta i interfejsu sieciowego. Reguły hosta dotyczą określonych hostów. Reguły interfejsu sieciowego dotyczą interfejsów, przez które hosty komunikują się z siecią. W razie wystąpienia konfliktów między regułą hosta i interfejsu pierwszeństwo ma zawsze reguła hosta.

Do dodawania, edycji i odczytywania reguł służy komenda **netrule**. Na ogół reguły dotyczą stosowanych protokołów, zakresów adresów (hostów i portów), dla których reguła ma być stosowana, oraz wyboru etykiet SL przypisywanych pakietom. Więcej informacji zawiera opis komendy **netrule**.

Komenda **tninit** służy do inicjowania podsystemu AIX Trusted Network, zapisywania reguł w formacie binarnym oraz wyświetlania reguł w formacie tekstowym.

Konfigurowalne opcje zabezpieczające
Ustawienia opcji konfigurowalnych są wyświetlane podczas sekwencji startowej.

Ustawienia konfigurowalne są zapisane w ODM. Ustawienia te można wyświetlić za pomocą komendy **getsecconf**, a użytkownik ISSO może je zmodyfikować za pomocą komendy **setsecconf**.

Zarządzanie etykietami
Użytkownik ISSO może dodawać, modyfikować lub usuwać metody kodowania etykiet, modyfikując zawartość pliku `/etc/security/enc/LabelEncodings`. Plik `/etc/security/enc/LabelEncodings` określa sposób, w jaki czytelne nazwy są odwzorowywane na binarną reprezentację etykiet czułości systemu.

Uwaga: Modyfikowanie pliku kodowania etykiet czułości w działającym systemie wymaga daleko posuniętej ostrożności, gdyż może doprowadzić do powstania nieprawidłowych etykiet. Ponieważ do obiektów można przypisywać etykiety za pomocą pojedynczych słów lub połączeń słów spełniających odpowiednie ograniczenia, nieuważne zmienianie, dodawanie lub usuwanie ograniczeń złożonych z kombinacji słów może spowodować utratę ważności etykiet.

Plik `/etc/security/enc/LabelEncodings` jest tłumaczony do postaci binarnej za pomocą procedury bibliotecznej **l_init** i przechowywany w postaci tabel. Tabele te są używane do przekształcania etykiet SL, banerów drukarek i zezwoleń między postacią czytelną i binarną.

Podstawą implementacji etykiet w systemie Trusted AIX jest oprogramowanie MITRE Compartmented Mode Workstation Labeling. Dokument Compartmented Mode Workstation Labeling: Encodings Format, DDS-2600-6216-93 (MTR 10649 revision 1), wrzesień 1993 opisuje standardowy format kodowania etykiet.

W standardowym formacie kodowania etykiet etykiety czułości i integralności są traktowane jednakowo, w sposób opisany w sekcji **Sensitivity Labels** pliku `/etc/security/enc/LabelEncodings`.

System Trusted AIX opcjonalnie obsługuje sekcję **Integrity Labels**, która umożliwia wprowadzenie rozróżnień między etykietami czułości i integralności.

Zarządzanie katalogami partycjonowanymi
Dla zwykłego procesu użytkownika katalog partycjonowany działa i jest widoczny tak samo, jak zwykły katalog. Jednak w przypadku katalogu partycjonowanego różne procesy o różnych etykietach SL widzą inną zawartość tego samego katalogu.

Na przykład, jeśli proces uruchomiony z etykietą bezpieczeństwa **SECRET** utworzy plik o nazwie **dom** w katalogu partycjonowanym, to drugi proces uruchomiony z etykietą bezpieczeństwa TOP SECRET nie widzi tego pliku **dom** w tym katalogu ani nie może uzyskać do niego dostępu. Co więcej, drugi proces może utworzyć własny plik **dom**, który nie będzie kolidował z pierwszym plikiem **dom**.

Takie działanie jest realizowane za pomocą ukrytych podkatalogów. Dla każdej unikalnej etykiety SL, za pomocą której proces uzyskuje dostęp do katalogu partycjonowanego, istnieje podkatalog partycjonowany. Gdy proces uzyskuje dostęp do katalogu partycjonowanego, system automatycznie przekierowuje ten proces do ukrytego podkatalogu. W przykładzie podanym powyżej dwa pliki **dom** w rzeczywistości znajdują się w różnych podkatalogach, mimo że dla użytkownika są one widoczne w tym samym katalogu.

Więcej informacji na temat katalogów partycjonowanych zawiera sekcja “Katalogi partycjonowane” na stronie 459.

Katalogi partycjonowane są obsługiwane w systemie plików JFS2 z EAv2.

Tworzenie katalogu partycjonowanego
Podczas tworzenia katalogu partycjonowanego domyślny zakres etykiet SL to System Low (minimalna SL) do System High (maksymalna SL). Podczas dostępu do katalogu partycjonowanego jądro automatycznie tworzy katalog potomny związany z daną etykietą (jeśli taki jeszcze nie istnieje) i kieruje użytkownika do tego katalogu.

Do tworzenia katalogu partycjonowanego służy komenda **pdmkdir**. Komenda **pdmkdir** wymaga autoryzacji **aix.mls.pdir.create**, aby przesłonić ograniczenia DAC, MAC i MIC. Do usunięcia pustego katalogu partycjonowanego służy komenda **pdrmdir**.

Partycjonowane podkatalogi i pod-podkatalogi

Katalogi potomne związane z poszczególnymi etykietami są partycjonowanymi podkatalogami. Kiedy proces utworzy katalog potomny w katalogu partycjonowanym, korzystając z komendy **mkdir**, nowy katalog staje się podkatalogiem partycjonowanym.

Po utworzeniu podkatalog partycjonowany dziedziczy atrybuty bezpieczeństwa nadrzędnego katalogu partycjonowanego, z wyjątkiem minimalnej i maksymalnej etykiety SL. Minimalne i maksymalne etykiety SL są konfigurowane zgodnie z domyślną etykietą SL procesu w trybie wirtualnym, który jako pierwszy odwołał się do podkatalogu partycjonowanego.

W systemie Trusted AIX rozróżniane są cztery różne typy katalogów:

- katalog zwykły (dir)
- katalog partycjonowany (pdir)
- podkatalog partycjonowany (psdir)
- pod-podkatalog partycjonowany (pssdir)

Tryb wirtualny i tryb rzeczywisty
Istnieją dwa różne tryby dostępu do katalogu partycjonowanego: tryb wirtualny i rzeczywisty.

W trybie wirtualnym proces uzyskujący dostęp do katalogu partycjonowanego widzi tylko zawartość jego zależnego od etykiety podkatalogu partycjonowanego. Katalog partycjonowany nigdy nie jest widoczny dla procesu działającego w trybie wirtualnym. Katalog partycjonowany jest widoczny dla procesu działającego w trybie rzeczywistym. Procesy uruchomione w trybie rzeczywistym widzą całą rzeczywistą zawartość

katalogów partycjonowanych i podkatalogów partycjonowanych. W przypadku procesów uruchomionych w trybie rzeczywistym system nie wykonuje przekierowania.

Domyślnie procesy są uruchamiane w trybie wirtualnym. Tryb rzeczywisty jest przeznaczony tylko do celów związanych z administrowaniem systemem. Aby uruchomić komendy w trybie innym niż tryb bieżącej powłoki procesów lub aby przełączyć się do powłoki w innym trybie, należy użyć komendy **pdmode**.

Chociaż procesy użytkowników w trybie rzeczywistym widzą katalogi oraz podkatalogi partycjonowane i mogą nimi manipulować, ten typ dostępu i manipulacji należy stosować, zachowując ostrożność. Na przykład, jeśli zwykły katalog jest tworzony lub przenoszony do katalogu partycjonowanego przez proces w trybie rzeczywistym, katalog ten nie będzie nigdy widoczny dla procesów uruchomionych w trybie wirtualnym.

Chociaż katalog partycjonowany jest widziany przez proces w trybie wirtualnym jak zwykły katalog, istnieją jednak pewne ograniczenia dotyczące katalogu partycjonowanego.

Hierarchia
Partycjonowane katalogi i podkatalogi są zorganizowane w hierarchię.

Hierarchią partycjonowanych katalogów i podkatalogów rządzą następujące reguły:

- Dopuszczalne są następujące cztery typy katalogów:
  - katalog zwykły,
  - katalog partycjonowany,
  - podkatalog partycjonowany,
  - pod-podkatalog partycjonowany.
- Katalog nie może jednocześnie należeć do więcej niż jednego typu.
- Katalogiem nadrzędnym partycjonowanego podkatalogu musi być partycjonowany katalog.
- Każdy potomny katalog partycjonowanego podkatalogu musi być partycjonowanym pod-podkatalogiem.
- Katalogiem nadrzędnym partycjonowanego pod-podkatalogu musi być partycjonowany podkatalog.

Każde naruszenie powyższych reguł powoduje zaburzenie struktury drzewa katalogów partycjonowanych, czego efektem jest niespójny system plików o nieprzewidywalnych właściwościach.

Podłączanie systemów plików
Katalog lub podkatalog partycjonowany może być punktem podłączenia, lecz nie może nim być partycjonowany pod-podkatalog. Podobnie katalog główny podłączanego systemu plików może być partycjonowanym katalogiem lub podkatalogiem, ale nie może być partycjonowanym pod-podkatalogiem.

Tworzenie i usuwanie katalogów
Kiedy proces uruchomiony w trybie wirtualnym znajduje się w partycjonowanym podkatalogu, komenda **mkdir** powoduje utworzenie zwykłego katalogu. Jeśli ten sam proces znajduje się w partycjonowanym podkatalogu, wywołanie komendy **mkdir** powoduje automatyczne utworzenie partycjonowanego pod-podkatalogu. Każdy pusty katalog może zostać usunięty z zachowaniem ograniczeń MAC, MIC i DAC.

Przenoszenie katalogów
Ograniczenia MAC, MIC i DAC obowiązują także przy przenoszeniu katalogów.

Zwykły katalog można przenieść w dowolne miejsce. Jeśli nowy katalog nadrzędny jest podkatalogiem partycjonowanym, przeniesiony katalog zwykły staje się partycjonowanym pod-podkatalogiem. W innych przypadkach pozostanie on zwykłym katalogiem. Jeśli nowy katalog nadrzędny jest partycjonowany, to w razie zaistnienia konfliktu nazw z potencjalnym partycjonowanym podkatalogiem wszelkie późniejsze przekierowania procesów trybu wirtualnego do tego potencjalnego podkatalogu zakończą się niepowodzeniem.

Katalog partycjonowany można przenieść do innego katalogu zwykłego, lecz nawet po przeniesieniu pozostanie on katalogiem partycjonowanym. System Trusted AIX nie zezwala na zagnieżdżanie katalogów partycjonowanych, ponieważ zabieg taki nie daje żadnych korzyści.

Partycjonowany podkatalog można przenieść tylko do katalogu partycjonowanego i po przeniesieniu pozostaje on podkatalogiem partycjonowanym. Niedozwolone jest przenoszenie podkatalogu partycjonowanego do katalogu zwykłego, do podkatalogu partycjonowanego lub do pod-podkatalogu partycjonowanego.

Partycjonowany pod-podkatalog można przenieść w dowolne miejsce. Jeśli jego nowym katalogiem nadrzędnym jest katalog zwykły, katalog partycjonowany lub pod-podkatalog partycjonowany, partycjonowany pod-podkatalog staje się zwykłym katalogiem. W przeciwnym razie pozostaje on partycjonowanym pod-podkatalogiem.

Tabela 42. Zestawienie informacji o przenoszeniu katalogów

Typ przenoszonego katalogu	**Do katalogu zwykłego**	**Do katalogu partycjonowanego**	**Do podkatalogu partycjonowanego**	**Do pod-podkatalogu partycjonowanego**
Zwykły	Dozwolone. Pozostaje katalogiem zwykłym.	Dozwolone[1]. Pozostaje katalogiem zwykłym.	Dozwolone[1]. Staje się partycjonowanym pod-podkatalogiem.	Dozwolone. Pozostaje katalogiem zwykłym.
Partycjonowany	Dozwolone. Pozostaje katalogiem partycjonowanym.	Dozwolone[1]. Pozostaje katalogiem partycjonowanym.	Niedozwolone.	Dozwolone. Pozostaje katalogiem partycjonowanym.
Podkatalog partycjonowany	Niedozwolone.	Dozwolone. Pozostaje podkatalogiem partycjonowanym.	Niedozwolone.	Niedozwolone.
Pod-podkatalog partycjonowany	Dozwolone. Staje się katalogiem zwykłym.	Dozwolone. Staje się katalogiem zwykłym.	Dozwolone. Pozostaje pod-podkatalogiem.	Dozwolone. Staje się katalogiem zwykłym.

[1] W razie konfliktu nazw z potencjalnym (jeszcze nieistniejącym) podkatalogiem partycjonowanym wszelkie późniejsze przekierowania procesów trybu wirtualnego do podkatalogu partycjonowanego zakończą się niepowodzeniem.

Zmiana typu katalogu
Za pomocą komendy **pdset** katalog zwykły można zmienić w katalog partycjonowany. Nie istnieje komenda pozwalająca zmienić katalog partycjonowany w zwykły.

Zastępowanie numerów i-węzłów
Podczas dostępu do partycjonowanego podkatalogu, gdy proces wymaga numeru i-węzła tego podkatalogu lub jego nadrzędnego katalogu partycjonowanego (..), zwracany jest odpowiednio numer i-węzła nadrzędnego katalogu partycjonowanego lub numer i-węzła katalogu nadrzędnego wobec nadrzędnego katalogu partycjonowanego. Podczas dostępu do partycjonowanego pod-podkatalogu, gdy proces wymaga numeru i-węzła jego katalogu nadrzędnego (..), zwracany jest numer i-węzła jego nad-nadrzędnego katalogu partycjonowanego.

Komendy do obsługi katalogów partycjonowanych
Opisane tu komendy dotyczą katalogów partycjonowanych.

pdmkdir
Tworzenie katalogów partycjonowanych.

pdrmdir
Usuwanie partycjonowanych katalogów i podkatalogów.

pdlink
Dowiązywanie plików między partycjonowanymi podkatalogami.

pdset
Konfigurowanie katalogu jako katalogu partycjonowanego.

pdmode
Zwrócenie bieżącego trybu dostępu do katalogu.

Uruchomienie komendy w określonym trybie dostępu do katalogu.

Katalog zwykły po przekształceniu w katalog partycjonowany, nie może już zostać przywrócony do stanu katalogu zwykłego.

Przegląd bezpieczeństwa systemu
Przeglądanie status bezpieczeństwa systemu należy do obowiązków użytkownika ISSO. Przeglądu bezpieczeństwa systemu należy dokonać natychmiast po instalacji i w każdej sytuacji, gdy integralność systemu mogła zostać naruszona. Ponadto przeglądy bezpieczeństwa systemu powinny być dokonywane okresowo.

Katalog bazy danych integralności systemu, zapisany w pliku `/etc/security/tsd/tsd.dat`, zawiera informacje dotyczące bezpieczeństwa o obiektach systemu plików, takich jak newralgiczne komendy i urządzenia systemowe. Tę bazę danych należy zaktualizować po dodaniu nowego urządzenia lub po modyfikacji informacji o bezpieczeństwie plików. Więcej informacji na ten temat zawiera opis komendy **trustchk**.

Komenda **trustchk** porównuje bieżące ustawienia bezpieczeństwa pliku, katalogu lub urządzenia z odpowiednią pozycją w bazie danych integralności systemu i naprawia niespójności atrybutów bezpieczeństwa. Komendę **trustchk** może uruchamiać tylko użytkownik z autoryzacją ISSO.

Zarządzanie urządzeniami TTY
Minimalna etykieta SL, maksymalna etykieta SL i etykieta TL dla urządzeń tty są zdefiniowane w bazie danych urządzeń tty w pliku `/etc/login.cfg`. Więcej informacji na ten temat zawiera opis komendy **chsec**.

Efektywna etykieta SL użytkownika logującego się za pomocą portu TTY powinna mieścić się w zakresie zdefiniowanym w tym pliku dla tego portu. Jeśli dla portu urządzenia TTY zostanie określona etykieta TL inna niż NOTL, to efektywna etykieta TL użytkownika musi być taka sama, jak podana etykieta TL.

Zarządzanie zezwoleniami użytkowników
Każdy użytkownik, w tym użytkownicy ISSO, SA i SO, muszą mieć etykiety, aby zalogować się w systemie. Zezwolenia użytkownika można określić w pliku `/etc/security/user` w sekcji dotyczącej użytkownika. Atrybuty **minsl**, **maxsl**, **defsl**, **mintl**, **maxtl** i **deftl** określają odpowiednio minimalną etykietę SL, maksymalną etykietę SL, domyślną etykietę SL, minimalną etykietę TL, maksymalną etykietę TL i domyślną etykietę TL danego użytkownika. Jeśli te atrybuty są określone w sekcji dotyczącej użytkownika, temu użytkownikowi przypisywane są wartości podane w sekcji wartości domyślnych pliku.

Bazę danych zezwoleń dostępu może modyfikować tylko użytkownik ISSO. Zezwolenia użytkownika można wyświetlić za pomocą komend **lsuser** i **lssec**, a zmodyfikować - za pomocą komend **chuser** i **chsec**.

Wartość domyślnej etykiety SL musi być zdominowana przez wartość maksymalnej etykiety SL i musi dominować nad minimalną etykietą SL. Analogicznie wartość domyślnej etykiety TL musi być zdominowana przez wartość maksymalnej etykiety TL i musi dominować nad minimalną etykietą TL.

Uwaga: Aby użytkownik mógł pomyślnie zalogować się w systemie, powyższa relacja musi być zawsze prawdziwa.

Zarządzanie systemem przez administratorów systemu
Administratorzy systemu (użytkownicy SA) są przede wszystkim odpowiedzialni za te aspekty administrowania systemem, które nie dotyczą bezpieczeństwa.

Użytkownicy SA są między innymi odpowiedzialni za:

- dodawanie, usuwanie i konserwację kont użytkowników,
- wykonywanie zadań wraz z użytkownikiem ISSO, które mają na celu zapewnienie wewnętrznej spójności oprogramowania systemowego i systemów plików.
- tworzenie i konserwację systemów plików; to zadanie obejmuje planowanie układu dysków, partycjonowanie dysków i zmianę wielkości partycji dysków, przydzielanie obszarów wymiany oraz obszarów na katalogi systemowe i użytkownika, monitorowanie wykorzystania systemów plików, wykrywanie i obsługę błędnych bloków dyskowych oraz zarządzanie obszarami systemów plików przez przenoszenie, usuwanie, archiwizowanie lub kompresowanie plików i systemów plików,
- rozpoznawanie i raportowanie problemów z systemem przez analizowanie danych o błędach i testowanie komponentów systemu, takich jak systemy plików, pamięć systemowa i urządzenia.

Zarządzanie kontami użytkowników
Za dodawanie nowych użytkowników do systemu odpowiada użytkownik SA. Za umożliwianie nowym użytkownikom zalogowania się i wykonywania komend w systemie odpowiada użytkownik ISSO.

Informacje na temat dodawania autoryzacji do kont użytkowników zawiera sekcja Zarządzanie systemem przez użytkowników ISSO.

Gdy użytkownik SA doda użytkownika do systemu, użytkownik ISSO musi być o tym poinformowany, aby ustawił początkowe hasło umożliwiające nowemu użytkownikowi dostęp do systemu.

Po stwierdzeniu, że dany użytkownik nie powinien mieć więcej dostępu do systemu, takiego użytkownika należy natychmiast usunąć. Usunięcie użytkownika może wykonać tylko użytkownik SA. Identyfikatora użytkownika usuniętego z systemu nie należy ponownie wykorzystywać, chyba że zostanie on przypisany pierwotnemu użytkownikowi tylko wtedy, gdy użytkownik ten ma być przywrócony w systemie.

Informacje na temat tworzenia i modyfikowania kont użytkowników zawierają opisy komend **mkuser**, **rmuser**, **chuser** i **pwadm**.

Zarządzanie drukarkami
Po poprawnym zainstalowaniu drukarki jest ona dodawana do systemu przez połączone działania użytkowników SA i SO. Użytkownik SO dodaje drukarkę do systemu, a użytkownik SA ustala zakres etykiety SL tej drukarki. Uprawnienia do wykonania obu tych zadań ma użytkownik ISSO.

Zakresu etykiety SL drukarki nie wolno ustawiać przed dodaniem drukarki do systemu. Do zarządzania drukarkami należy użyć komendy **smit**.

Uwaga: Oznaczone etykietami drukowanie PostScript i plików ASCII jest obsługiwane tylko przez drukarki typu PostScript.

Dostęp MAC do drukarki jest określony przez etykietę SL procesu drukującego plik. Ta etykieta SL znajduje się w banerze, nagłówku/stopce i na ostatniej stronie. Proces używający komendy **lp** musi mieć dostęp MAC, MIC i DAC do drukowanego pliku. W przeciwnym razie komenda **lp** nie wygeneruje żądania wydruku.

Gdy drukarka zostanie usunięta z systemu, należy natychmiast usunąć profil tej drukarki. Zadanie to może wykonać tylko użytkownik z autoryzacją SO.

Zarządzanie systemami plików
System plików składa się z katalogów, plików danych, plików wykonywalnych i plików specjalnych. System plików może znajdować się na różnych urządzeniach pamięci masowej, jak napędy dysków twardych lub dyskietki.

Systemy plików może tworzyć i modyfikować tylko użytkownik z uprawnieniami SA, jednak podłączanie i odłączanie systemów plików jest możliwe zarówno z poziomu kont SA, jak i SO.

Sprawdzanie systemów plików przy użyciu komendy fsck
Wewnętrzna integralność systemu plików powinna być okresowo sprawdzana przy użyciu komendy **fsck**. Komendę **fsck** należy uruchamiać dla niepodłączonych systemów plików. Uruchomienie komendy **fsck** jest możliwe tylko dla użytkownika SA.

Domyślnie komenda **fsck** działa w trybie interaktywnym, monitując użytkownika o wskazanie czynności do wykonania w razie znalezienia osieroconego pliku lub katalogu. Użytkownik ma do wyboru usunięcie pliku lub próbę jego odzyskania. Jeśli użytkownik zdecyduje się na odzyskanie pliku, komenda **fsck** podejmuje próbę zapisania pliku w katalogu `/lost+found`.

Po zakończeniu wykonywania komendy **fsck**, gdy odzyskane pliki znajdują się już w katalogu `/lost+found`, użytkownik ISSO powinien przejrzeć te pliki, aby ustalić ich poziom bezpieczeństwa. Zaleca się przydzielenie katalogowi `/lost+found` etykiety SL **SYSTEM_HIGH**, aby uniemożliwić dostęp do odzyskanych plików zwykłym użytkownikom.

Więcej informacji zawiera opis komendy **fsck**.

Zarządzanie systemem przez użytkowników SO
Użytkownicy SO są przede wszystkim odpowiedzialni za te aspekty administrowania systemem, które dotyczą bezpieczeństwa.

Zarządzanie systemami plików
Za zarządzanie systemami plików odpowiedzialni są użytkownicy SO.

Obsługiwane systemów plików
Trusted AIX obsługuje wszystkie dyskowe systemy plików.

Wszystkie systemy plików, oprócz JFS2, są obsługiwane w systemie Trusted AIX jako jednopoziomowe systemy plików. Systemy te można podłączać w systemie Trusted AIX. Automatycznie otrzymają one etykiety i inne atrybuty bezpieczeństwa, a ponadto będą podlegały mechanizmom bezpieczeństwa wymuszanym przez system Trusted AIX. Wszystkie obiekty plikowe w jednopoziomowym systemie plików mają te same atrybuty bezpieczeństwa. Atrybuty te są dziedziczone z punktu podłączenia.

JFS2 zaimplementowano w systemie Trusted AIX jako wielopoziomowy system plików. Każdy obiekt plikowy w wielopoziomowym systemie plików ma własne atrybuty bezpieczeństwa (etykiety bezpieczeństwa). Na przykład katalog JFS2 ma niezależne od siebie minimalne i maksymalne etykiety SL.

W jednopoziomowych systemach plików minimalne i maksymalne etykiety SL punktu podłączenia są równe, a ponadto wszystkie katalogi i pliki znajdujące się poniżej punktu podłączenia muszą także być równe tym etykietom SL.

Podłączanie i odłączanie systemów plików
System plików może podłączyć lub odłączyć użytkownik SO (z autoryzacją **aix.fs.manage.mount**). Komenda **mount** opcjonalnie korzysta z nazwy pliku specjalnego urządzenia i katalogu podłączania.

Podczas podłączania wielopoziomowych systemów plików JFS2 katalogowi podłączania przypisywana jest etykieta głównego systemu plików. W wielopoziomowym systemie plików każdy plik ma własną etykietę czułości i integralności. Modyfikacja pliku powoduje odpowiednią aktualizację jego etykiety.

Zarządzanie drukarkami
Użytkownik SO może używać komendy **lpadmin**, aby dodawać i usuwać drukarki, modyfikować je oraz wykonywać innego typu operacje sterowania podsystemem drukarek. Użytkownik SA może używać komendy **lpadmin**, aby dodawać lub usuwać etykiety SL dla drukarki, a także komend enable i disable, aby włączać i wyłączać drukarki.

Podsystem drukarek
Podsystem drukarek wykonuje wiele zadań powiązanych z działaniem drukarek.

Do zadań podsystemu drukarek należą:

- administrowanie drukarkami i ich atrybutami,
- odbieranie, zapisywanie i planowanie zadań drukowania użytkowników,
- planowanie zadań drukowania dla wielu drukarek,
- uruchamianie programów współdziałających z drukarkami,
- śledzenie statusu drukarek i zadań drukowania,

- zgłaszanie problemów, gdy pojawiają się,
- ograniczanie zadań drukowania użytkowników do tych, które mieszczą się w zakresie etykiety SL drukarki,
- ograniczanie dostępu do zadań drukowania użytkowników już wprowadzonych,
- ograniczanie dostępu do plików i katalogów obsługi drukarek,
- odpowiednie oznaczanie wydruków.

Opcje zabezpieczające drukarek
Podsystem drukarek został zmodyfikowany w systemie Trusted AIX dzięki czemu zawiera szereg opcji zabezpieczających.

Podsystem drukarek jest podsystemem zabezpieczonym, którego właścicielem jest identyfikator systemowy **lp**. Dzięki temu zwykli użytkownicy nie mają dostępu do plików i katalogów obsługi drukarek innych niż wprowadzane przez nich własne zadania drukowania ani do plików specjalnych drukarek.

Podsystem drukarek sprawdza, czy wprowadzone przez użytkownika zadanie drukowania mieści się w zakresie etykiety SL drukarki. Ta weryfikacja jest przeprowadzana, gdy użytkownik wprowadza zadanie drukowania za pomocą komendy **lp**, ale przed wydrukowaniem wprowadzonego zadania przez demon **lpsched**. Administrator powinien mieć świadomość sprawdzeń zabezpieczeń wykonywanych przez podsystem drukarek, jeśli zadanie drukowania użytkownika zostanie odrzucone.

Strony banera są drukowane dla wszystkich zadań drukowania. Strona banera zawiera czytelną etykietę SL zadania drukowania. Strona banera jest umieszczana na początku i na końcu wszystkich zadań drukowania. Każdy użytkownik może drukować bez stron banera, ale to działanie podlega kontroli. Zawsze należy sprawdzać, czy etykiety paginy górnej i paginy dolnej na każdej stronie są poprawne i czy są zdominowane przez etykiety na stronie banera.

Uwaga: Administrator drukarek wierszowych musi ustalić zakres etykiety dla każdej drukarki. Aby przypisać pojedynczą etykietę do drukarki, uruchom następującą komendę:

lpadmin -d *nazwa_drukarki* **-J***etykieta* **-L***etykieta*

Dzięki temu mamy pewność, że na tej drukarce można drukować tylko informacje z etykietą o nazwie *etykieta*.

Podsumowanie komend dotyczących drukarek
Niektóre komendy podsystemu drukarek mogą być uruchamiane przez każdego użytkownika. Jednak niektóre komendy podsystemu drukarek mogą być uruchamiane tylko przez użytkownika SO, SA lub ISSO.

W poniższej tabeli podano komendy podsystemu drukarek, które mogą być uruchamiane przez każdego użytkownika:

lp
Wysyła plik do drukarki.

lpstat
Udostępnia raport o statusie podsystemu drukarek.

Komendy administrowania podsystemem drukarek wymagają autoryzacji SO, tyle tylko, że użytkownik z autoryzacją SA lub ISSO może uruchomić komendę **lpadmin**, aby podać zakres etykiety drukarki, i komendę **lpstat**, aby wyświetlić etykiety SL drukarki i żądania zadania. W poniższej tabeli podano komendy administrowania podsystemem drukarek:

accept
Zezwala na zadania na drukarce.

cancel
Anuluje żądanie wydruku pliku.

disable
Dezaktywuje drukarkę.

enable
Aktywuje drukarkę.

lpadmin
Konfiguruje lub zmienia konfigurację drukarki.

lpfilter
Konfiguruje lub zmienia filtr drukarki.

lpforms
Konfiguruje lub zmienia formularz drukarki.

lpmove
Przenosi żądanie wydruku.

lpsched
Drukuje żądanie.

lpshut
Zatrzymuje usługę wydruku.

lpusers
Konfiguruje lub zmienia priorytet wydruku.

reject
Odrzuca zadania na drukarce.

Zarządzanie drukarką za pomocą wiersza komend
Do zarządzania drukarką z poziomu wiersza komend można użyć następujących komend **accept**, **enable**, **disable**, **lpstat** i **lp**.

Komenda **accept** służy do zezwalania na wysyłanie zadań do drukarki. Aby zezwolić drukarce *laser* na akceptowanie zadań drukowania, uruchom następującą komendę:

```
/usr/sbin/accept laser
```

Drukarka *laser* może teraz odbierać żądania zadań drukowania. Jednak zadania drukowania nie będą drukowane, o ile drukarka nie zostanie włączona. Aby włączyć drukarkę, uruchom komendę enable:

```
/usr/bin/enable laser
```

Komendy **enable** i **disable** są komendami administracyjnymi i mogą być uruchamiane tylko przez użytkownika z autoryzacją ISSO lub SA.

Aby potwierdzić, że drukarka została poprawnie skonfigurowana, uruchom komendę **lpstat**:

```
lpstat -p laser -l
```

Ta komenda wyświetla długi raport o statusie drukarki *laser*. Jeśli komenda **lpstat** zostanie uruchomiona bez opcji **-l**, zostanie wyświetlony krótszy raport o statusie. Jeśli użytkownik ma autoryzację SA lub ISSO i użyto opcji **-l**, raport będzie także zawierał informacje o zakresie etykiety SL.

Aby określić status żądania drukowania, uruchom następującą komendę **lpstat**:

```
lpstat -o
```

Ta komenda wyświetli wszystkie żądania drukowania **lp**. Jeśli użytkownik ma autoryzację SA lub ISSO, zostanie wyświetlona efektywna etykieta SL i zezwolenie każdego żądania.

Aby wydrukować nazwę pliku, uruchom następującą komendę **lp**:

```
lp -d laser nazwa_pliku
```

W przeciwnym razie podczas uruchamiania komendy **lp** należy podać miejsce docelowe zadania drukowania.

Jeśli administrator skonfigurował domyślną drukarkę docelową, podanie opcji **-d** *drukarka_docelowa* nie jest konieczne. Na przykład, aby wydrukować plik o nazwie nazwa_pliku na drukarce laser, wprowadź następującą komendę **lp**:

```
lp nazwa_pliku
```

Zarządzanie zamknięciem systemu
Użytkownik SO może zamknąć system, restartując go lub całkowicie go zatrzymując.

Poniżej podano komendy, które może uruchamiać użytkownik SO, aby restartować lub zatrzymać system albo zmienić jego stan początkowy:

reboot
Automatycznie restartuje system.

halt
Zatrzymuje wszystkie operacje systemowe.

shutdown
Zatrzymuje wszystkie operacje systemowe.

init
Zmienia stan początkowy systemu.

Tworzenie i odtwarzanie kopii zapasowych plików
Kopie zapasowe pomagają w ochronie przed utratą danych w przypadku awarii sprzętu lub przypadkowego usunięcia pliku. Kopie zapasowe należy tworzyć regularnie, pamiętając o tworzeniu przyrostowych kopii zapasowych między pełnymi kopiami zapasowymi.

Komendy **backup** i **restore** zawierają opcje umożliwiające podanie nazw kopii zapasowych plików, miejsc, typów i innych opcji. Użytkownik może użyć komendy **mksysb** do utworzenia obrazu instalacyjnego Trusted AIX głównej grupy woluminów w pliku lub na taśmie startowej. Komendy te można uruchamiać za pomocą komendy **smit**. Kopie zapasowe systemów plików należy oznaczyć odpowiednimi etykietami i przechowywać w bezpiecznym miejscu.

Programowanie w systemie Trusted AIX

Bezpieczeństwo systemu zależy od oprogramowania zaufanej bazy przetwarzania (baza TCB), sprzętu i oprogramowania wbudowanego. Obejmuje to całe jądro systemu operacyjnego, wszystkie sterowniki urządzeń i moduły STREAMS systemu System V, rozszerzenia jądra oraz wszystkie programy zaufane. Wszystkie pliku używane przez te programy w procesie podejmowania decyzji dotyczących bezpieczeństwa także stanowią część bazy TCB.

Tworzenie oprogramowania zaufanego wymaga gruntownego zrozumienia zasad i opcji podstawowego bezpieczeństwa systemu. Prawie wszystkie błędy dotyczące bezpieczeństwa w systemach UNIX wynikają z niskiej jakości utworzonego oprogramowania zaufanego. Jednak korzystając z funkcji sprawdzeń bezpieczeństwa jądra w systemie Trusted AIX, można tworzyć aplikacje używające rozszerzonych opcji zabezpieczających. Aplikacja napisana dla systemu Trusted AIX może być wrażliwa na pliki i procesy na różnych poziomach bezpieczeństwa i może zachowywać się odmiennie w zależności od poziomu procesu lub pliku używanego przez tę aplikację. Taką aplikację nazywa się aplikacją rozpoznającą wiele poziomów (MLS).

Programista systemu zaufanego musi bardzo dobrze znać się na opcjach zabezpieczających systemu Trusted AIX, a ponadto musi rozumieć wszystkie nowe wywołania systemowe, komendy i biblioteki systemu Trusted AIX dotyczące bezpieczeństwa. Podane informacje są przeznaczone dla programistów tworzących lub modyfikujących oprogramowanie zaufane. Udostępniono wytyczne, zasady i ostrzeżenia dotyczące modyfikacji i tworzenia oprogramowania zaufanego. Niniejsze informacje stanowią wprowadzenie do niektórych zasad i metod dotyczących bezpieczeństwa, zaleca się więc, aby programiści systemu zaufanego przeczytali inne materiały dotyczące bezpiecznych systemów.

Zasady dotyczące oprogramowania zaufanego

Istnieje szereg ważnych zasad dotyczących tworzenia i modyfikowania oprogramowania zaufanego, w tym potwierdzania i uprawnień, projektowania oprogramowania zaufanego, najmniejszego uprzywilejowania, konwencji programowania i ochrony bazy TCB.

Zaufanie i uprawnienie

Proces może obejść podstawowe ograniczenia bezpieczeństwa (MAC, MIC, DAC i inne operacje zastrzeżone) tylko wtedy, gdy ma on odpowiednie uprawnienia. Każdy proces uruchamiany z uprawnieniem lub uprawnieniami jest nazywany procesem uprawnionym, a program uruchamiany przez ten proces jest nazywany programem uprawnionym (zaufanym).

Termin uprawnienie odnosi się do pojedynczego atrybutu, który umożliwia procesowi wykonanie operacji dotyczącej bezpieczeństwa. Trusted AIX identyfikuje i grupuje niektóre operacje dotyczące bezpieczeństwa, a z każdą operacją wiąże odrębne uprawnienie. W ten sposób skutecznie usuwane jest uprawnienie administratora (lub użytkownika root) z systemu podstawowego. Uprawnienia są powiązane z procesami i plikami wykonywalnymi.

Programy muszą być zaufane w następujących okolicznościach:

- program jest skonfigurowany lub jest przeznaczony do uruchomienia jako proces uprawniony; dotyczy to każdego programu, który ma być uruchamiany przez proces uprawniony;
- program jest uzależniony od innego programu zaufanego, jeśli chodzi o podejmowanie decyzji dotyczących bezpieczeństwa; na przykład program zmieniający bazę danych objętą szczególną ochroną musi być zaufany, jeśli inne programy są uzależnione od danych znajdujących się w tej bazie danych, jeśli chodzi o podejmowanie decyzji dotyczących bezpieczeństwa;

Należy zadbać o to, aby programy niezaufane nigdy nie były uruchamiane jako procesy uprawnione. Istnieje kilka sposobów na to, aby uniemożliwić uruchamianie programów niezaufanych jako procesów uprawnionych:

- Zwykle nie należy zezwalać procesom uprawnionym na wykonywanie programów niezaufanych. Na przykład należy ostrzec użytkowników uruchamiających uprawnione programy powłoki, aby nie uruchamiali programów niezaufanych w uprawnionym programie powłoki.
- Nigdy nie należy zezwalać na rodzime, odziedziczone lub autoryzowane uprawnienia dla niezaufanych plików wykonywalnych.

Wszystkie części jądra systemu operacyjnego, w tym sterowniki urządzeń, moduły STREAMS i rozszerzenia jądra, muszą być zaufane. Obiekty danych, takie jak pliki i urządzenia fizyczne także uważane są za zaufane, jeśli zawierają informacje uzależnione od programu zaufanego, jeśli chodzi o podejmowanie decyzji dotyczących bezpieczeństwa.

Projektowanie oprogramowania zaufanego

Proces tworzenia oprogramowania zaufanego jest podobny do procesu tworzenia newralgicznego komponentu oprogramowania. Procesowi tworzenia oprogramowania zaufanego powinny towarzyszyć cykle kontrolne obejmujące dogłębne zrozumienie i udokumentowanie fazy specyfikowania, projektowania, implementowania, testowania i konfigurowania.

Najważniejszymi aspektami procesu projektowania oprogramowania zaufanego są określenie podmiotów i obiektów oraz zdefiniowanie precyzyjnych działań bezpieczeństwa na odpowiednim poziomie abstrakcji. Większość strategii bezpieczeństwa opiera się na podmiotach, obiektach i działaniach. Gdy podmioty żądają uprawnienia do odczytu, zmiany lub tworzenia obiektów, strategie bezpieczeństwa monitorują te żądania i zatwierdzają je lub odrzucają.

Podmioty

Podmiot jest zwykle reprezentowany przez ID użytkownika i ID grupy. Zwykle do tego celu używany jest efektywny ID użytkownika i/lub grupy procesu, chociaż w niektórych sytuacjach właściwym rozwiązaniem może być użycie rzeczywistego ID użytkownika i/lub grupy.

Obiekty

Obiekt jest kolekcją danych, do których dostęp powinien podlegać kontroli. W większości przypadków obiektami są pliki. Chociaż zwykle programy zaufane kontrolują dostęp do logicznie odrębnych obiektów w obrębie tego samego pliku, ogólnie lepszą procedurą jest zastosowanie odwzorowania obiektów na pliki typu jeden-do-jednego.

W niektórych sytuacjach podmiot można także traktować jak obiekt. Na przykład proces traktuje się jako podmiot. Jednak, gdy jeden proces próbuje wpłynąć na drugi proces, to ten drugi proces traktuje się jako obiekt w odniesieniu do tej operacji.

Żądania

Żądania są zbiorem działań, które moduł zaufany wykonuje w imieniu podmiotu. Każde żądanie musi być jasno określone pod kątem danych wejściowych, możliwych danych wyjściowych i wyników żądania, w tym wszystkich efektów ubocznych. Precyzyjne określenie wszystkich żądań jest ważnym wstępem do zdefiniowania strategii bezpieczeństwa.

Strategie bezpieczeństwa

Strategie bezpieczeństwa zawierają proste instrukcje wskazujące, kiedy żądania obejmujące określone obiekty zostaną wykonane w imieniu podanych podmiotów. Podmioty, obiekty i żądania należy zdefiniować starannie. Strategie bezpieczeństwa powinny być zwięzłe i proste. Na potrzeby kontroli należy określić tożsamość podmiotu żądającego i angażowanych obiektów.

Najniższy poziom uprawnień

Zasada najmniejszego uprzywilejowania mówi, że modułom oprogramowania należy przypisać minimalne możliwości wymagane do wykonania zamierzonych zadań.

Jedna z zasad najmniejszego uprzywilejowania mówi, że programy zaufane powinny dobrowolnie ograniczać własne możliwości objęte szczególną ochroną, aby były one używane w tak niewielu obszarach programu, jak to tylko możliwe. Najmniejsze uprzywilejowanie pomaga ograniczyć szkody wynikające z błędów w oprogramowaniu lub z nieoczekiwanych efektów ubocznych. Całe oprogramowanie zaufane powinno być zaprojektowane zgodnie z regułą najmniejszego uprzywilejowania.

Przypisywanie i odbieranie uprawnień

Jedna z technik realizacji zaufanego oprogramowania polega na tym, że program wykonuje wszystkie operacje wymagające specjalnych uprawnień na początku działania, a następnie zrzeka się tych uprawnień na całą resztę czasu wykonywania. Nazywa się to czasowym ograniczaniem uprawnień.

Podczas korzystania z uprawnień należy mieć na uwadze następujące kwestie:

- Każdy proces użytkownika w czasie wykonywania otrzymuje maksymalny zestaw uprawnień. Ten zestaw może zawsze zostać zawężony, nigdy zaś rozszerzony przez użytkownika bez uprawnień.
- Działający proces jest odpowiedzialny za podnoszenie i obniżanie poziomu uprawnień względem zbioru maksymalnego, tworząc zestaw optymalny pod kątem potrzeb aktualnie wykonywanych operacji wymagających tych uprawnień.
- Uprawnienia procesu są modyfikowane, gdy procesy uruchamiają pliki wykonywalne mające niepuste własne zestawy uprawnień. Więcej informacji zawiera opis komendy **exec**.
- Uruchamianym procesom mogą być także przypisywane ograniczające zestawy uprawnień. Mając odpowiednie uprawnienia, proces może podnieść poziom uprawnień w zestawie maksymalnym do poziomu wyznaczanego przez ograniczający zestaw uprawnień.

Krótkoterminowe zmiany etykiet MAC

Gdy proces musi zmienić swoją etykietę MAC z normalnej etykiety operacyjnej, okres tej zmiany powinien być maksymalnie krótki. Można to osiągnąć za pomocą procedur bibliotecznych.

Więcej informacji na temat procedur bibliotecznych zawiera sekcja “Wywołania systemowe w modelu Trusted AIX” na stronie 522.

Krótkoterminowe otwarcia plików objętych szczególną ochroną
Plik objęty szczególną ochroną, taki jak plik zaszyfrowanych haseł, zawiera informacje, których przejęcie może naruszyć bezpieczeństwo systemu. Pliki objęte szczególną ochroną powinny być otwierane do odczytu lub zapisu tylko na niezbędny okres.

Należy ustawić atrybut **close-on-exec** deskryptora pliku, używając wywołania systemowego **fcntl**. Uniemożliwia to nieautoryzowanym procesom dziedziczenie deskryptorów otwartych plików za pomocą wywołania systemowego **exec**.

Centralizowanie newralgicznych operacji
Operacja newralgiczna jest to czynność wymagająca określonych uprawnień. Wykonanie czynności newralgicznej przez nieuprawniony proces może naruszyć bezpieczeństwo systemu.

Wykonywanie operacji newralgicznych powinno być zastrzeżone dla wydzielonych modułów (podprocedur lub oddzielnych programów). Gdy duży program zostanie podzielony na odrębne podprogramy, niektóre z nich będą wymagały niższego lub nawet zerowego poziomu uprawnień. Pozwala to zmniejszyć ryzyko przypadkowego naruszenia bezpieczeństwa systemu.

Użycie efektywnych katalogów głównych
Program można ograniczyć do konkretnego drzewa katalogów, ustawiając efektywny katalog główny tego programu na podstawowy katalog drzewa (za pomocą wywołania systemowego **chroot**) i ustawiając katalog roboczy programu wewnątrz tego samego drzewa. W rzeczywistości jest to mechanizm najmniejszych uprawnień, ponieważ nawet dla procesu uprawnionego ogranicza dostęp do tych plików, które znajdują się w drzewie. Jest to szczególnie skuteczne, gdy zaufany proces nadrzędny w ten sposób ogranicza zaufane lub niezaufane procesy potomne.

Chociaż zmiana katalogów głównych zabezpiecza pliki poza nowym drzewem głównym, powstaje potencjalny problem dotyczący bezpieczeństwa. Zmiana katalogu głównego może być źródłem naruszenia bezpieczeństwa nowego drzewa głównego, jeśli nie zachowa się ostrożności. Dzieje się tak wtedy, gdy można podrobić wykonawczy program łączący i obiekty współużytkowane w nowym drzewie głównym. Tej procedury należy używać ostrożnie i sporadycznie.

Użycie podsystemów zabezpieczonych
Podsystemy zabezpieczone zapewniają zabezpieczenie integralności podsystemów specjalnych. Podsystem jest kolekcją programów i/lub plików danych, których właścicielem jest jeden ID użytkownika i/lub ID grupy i które są używane do zaimplementowania konkretnej funkcji w systemie.

Podsystem może zawierać programy setuid lub setgid. Podsystem zabezpieczony to taki, którego ID użytkownika jest ID użytkownika systemowego.

ID użytkownika systemowego to ID o wartości mniejszej lub równej 127. Użytkownicy nie mogą logować się, używając ID użytkowników systemowych. Użycie podsystemów zabezpieczonych może znacznie ograniczyć liczbę procesów uprawnionych.

Tryb dostępu minimalnego
Programy zaufane (w zasadzie wszystkie programy) powinny otwierać obiekty tylko w takim trybie odczytu lub zapisu, jaki jest bezwzględnie konieczny. Zasadniczo oznacza to, że obiekt nigdy nie powinien być otwierany do zapisu i odczytu, jeśli otwarcie go tylko do odczytu byłoby wystarczające. W szczególnie newralgicznych sytuacjach proces powinien otwierać obiekt tylko do zapisu w konkretnym miejscu, w którym zapis jest wymagany.

Opisywane techniki mają szczególne znaczenie w przypadku programów tworzących inne procesy, ponieważ przekazywanie uprawnień i innych możliwości (na przykład otwartych połączeń z ważnymi plikami) należy do zasadniczych aspektów projektowania oprogramowania zaufanego. Uprawnienia pozwalają ominąć wszelkie ograniczenia. Dlatego przy tworzeniu nowych komend dysponujących uprawnieniami niezbędne jest przemyślane projektowanie i daleko posunięta ostrożność.

Inne konwencje dotyczące programowania zaufanego
Trusted AIX korzysta z wielu innych konwencji programowania zaufanego.

Nadmiarowość
Nadmiarowość jest techniką przydatną dla systemów bezpieczeństwa. Zabezpieczenia są rzadko bezwzględne, ale prawie zawsze jest to kwestia umieszczenia wystarczającej liczby blokad na ścieżce osoby próbującej uzyskać niedozwolony dostęp do systemu.

Zaletą wynikającą z nadmiarowych sprawdzeń zabezpieczających jest to, że jeśli jedno sprawdzenie nie powiedzie się lub zostanie naruszone, inne sprawdzenia mogą zapewnić bezpieczeństwo. Ujemną stroną nadmiarowych sprawdzeń jest to, że sprawdzenia zabezpieczające są oddzielone lub rozproszone w systemie. Z tego względu, chociaż nadmiarowe sprawdzenia mogą być bardzo przydatne, należy je starannie zaprojektować, udokumentować i konserwować.

Sprawdzenia pod kątem duplikacji jądra
Rzadko zaleca się, aby proces wykonywał sprawdzenie, które może wykonać jądro. Na przykład proces nigdy nie powinien odczytywać etykiety MAC pliku i sam wykonywać obowiązkowego sprawdzenia dostępu. Gdy tylko jest to możliwe, sprawdzenie powinno być wykonywane przez jądro.

Istnieją dwa główne powody, aby sprawdzenia były wykonywane przez jądro.

- Operacje jądra są niepodzielne w odniesieniu do innych procesów, podczas gdy sprawdzenia wykonywane przez proces mogą być współbieżne z innymi procesami.
- Ważniejszym powodem jest to, że używane precyzyjne algorytmy mogą się zmieniać w nowszych wersjach jądra. Trudno śledzić takie zmiany w przypadku algorytmów będących częścią oprogramowania użytkownika końcowego.

Bezpośrednie sprawdzanie uprawnień
Programy nie powinny sprawdzać, czy zostały wywołane jako procesy uprzywilejowane (na przykład badając swój efektywny lub maksymalny wektor uprawnień). Zamiast tego programy powinny zakładać, że są uprzywilejowane tam, gdzie jest to wymagane.

Jeśli program nie jest procesem uprzywilejowanym, uprzywilejowane wywołania systemowe nie powiodą się, a program może podjąć odpowiednie działania. Zazwyczaj mechanizm, według którego program aktywnie odmawia wykonania pewnych operacji, jeśli samodzielnie ustali, że nie jest uprzywilejowany, nie jest zabezpieczeniem godnym polecenia. Jeśli program jest uprzywilejowany, wynik testu jest bez znaczenia. Jeśli program nie jest uprzywilejowany, jego działanie nie może przynieść więcej szkody niż działania innych nieuprzywilejowanych procesów.

Niemniej jednak, takie sprawdzenie może zabezpieczać przed przypadkowym niewłaściwym użyciem. Można w takim przypadku sformułować zrozumiały komunikat o błędzie informujący, że program w założeniu miał być uprzywilejowany, a nie jest.

Propagacja możliwości objętych szczególną ochroną
Możliwości objęte szczególną ochroną to te możliwości programu zaufanego, które mogą spowodować naruszenie bezpieczeństwa systemu, jeśli zostaną udostępnione programowi niezaufanemu.

Należy zachować ostrożność, gdy program uprzywilejowany propaguje swoje uprawnienia lub możliwości ogólne na inne programy za pomocą rodziny wywołań systemowych **fork** i **exec**. Wywołania systemowe **exec** są najważniejsze, ponieważ przekazują one uprawnienia między programami. Wywołanie systemowe **fork** tworzy nowy proces, ale uprawnienia tego nowego procesu są takie same, jak uprawnienia procesu nadrzędnego. Podstawowe niebezpieczeństwo polega na tym, plik programu wykonywalnego może nie być zaufany lub został zmieniony przez program niezaufany. Należy wziąć pod uwagę następujące ostrzeżenia:

- Należy pamiętać, aby programy zaufane nie przekazywały otwartych połączeń do obiektów (głównie plików) do procesu potomnego, chyba że można zaufać temu procesowi potomnemu i jego potomkom, że uzyskają właściwy dostęp do pliku w trybie, w którym został on otwarty. Najlepszym rozwiązaniem dla procesu może być przekazanie nowego połączenia do obiektu, którego tryby są bardziej zamknięte niż tryby, które by istniały w przeciwnym razie.
- Zaufany proces, który działa w efektywnym katalogu głównym innym niż absolutny katalog główny, musi być pewny, że jego procesy potomne nie pogubią się. Na przykład, gdy program potomny otwiera plik zaufany, taki jak plik haseł shadow, może on użyć absolutnej nazwy ścieżki, zakładając, że jego efektywnym katalogiem głównym jest absolutny katalog główny.

- Mogą istnieć sytuacje, w których program zaufany potrzebuje narzucić swoim programom potomnym bardziej ograniczające ustawienia umask.
- Procesy potomne dziedziczą wiele atrybutów procesu. Jeśli program zaufany wie, że proces potomny jest niezaufany i ma etykietę MAC niedominującą nad etykietą procesu zaufanego i te atrybuty zostały odziedziczone przez program zaufany z niezaufanego przodka, to mogą być one źródłem potencjalnych ukrytych kanałów.
- Należy mieć świadomość reguł propagacji uprawnień w wywołaniach systemowych **fork** i **exec**. Uprawnienia procesu macierzystego stają się uprawnieniami procesu potomnego, gdy pojawi się wywołanie systemowe **fork**. Uprawnienia są modyfikowane podczas wywołania systemowego **exec**.

W sytuacjach objętych szczególną ochroną program zaufany może sprawdzić prawa dostępu dla pliku zaufanego w celu zapewnienia, że plik jest odpowiednio zabezpieczony przed modyfikacją przez programy niezaufane. Na przykład może istnieć wymaganie, aby właścicielem pliku był użytkownik root i aby dla jego właściciela były określone maksymalnie uprawnienia do zapisu DAC.

Efektywny katalog główny
Programy zaufane często polegają na poprawności ścieżek bezwzględnych. Na przykład program **login** działa w oparciu o założenie, że plik `/etc/security/passwd` jest poprawnym plikiem zaszyfrowanych haseł.

Dotyczy to nie tylko plików danych, lecz także plików wykonywalnych dla programów zaufanych. Programy niezaufane nie mogą korzystać z wywołania systemowego **chroot** w celu bezpośredniej modyfikacji efektywnego katalogu głównego programu, mogą jednak zaistnieć sytuacje, w których TCB zezwala na działanie programów niezaufanych w środowisku efektywnego katalogu głównego. Możliwość uruchomienia przez program niezaufany programu zaufanego, który polega na ścieżkach bezwzględnych, stwarza potencjalne zagrożenia dla systemu bezpieczeństwa.

Uwierzytelnianie za pomocą rzeczywistych i efektywnych identyfikatorów
Programy zaufane mogą czasem korzystać z kilku identyfikatorów użytkowników i grup, które są skojarzone z procesem. Istotna jest umiejętność rozróżnienia między tymi identyfikatorami i odpowiednie korzystanie z nich.

Rzeczywiste identyfikatory użytkowników i grup

Rzeczywiste identyfikatory użytkowników i grup zazwyczaj odpowiadają tożsamości użytkownika dla sesji, w ramach której proces został utworzony. W niektórych przypadkach rzeczywiste identyfikatory (zwłaszcza użytkowników) mogą być wykorzystywane podczas podejmowania decyzji dotyczących bezpieczeństwa. Jednym z przykładów jest sprawdzanie autoryzacji. Rzeczywiste identyfikatory użytkowników są używane przez komendy jako podstawa podczas weryfikowania tożsamości. Może to być szczególnie użyteczne przy zapobieganiu użyciu bitów sterujących **setuid-on-exec** lub **setgid-on-exec** w złych zamiarach lub w sposób nieprzemyślany. Jednak sprawdzanie rzeczywistych identyfikatorów nie mieści się w standardach przyjętych w systemie UNIX i powinno być wykonywane tylko w razie konieczności. Zgodnie z ogólną zasadą obowiązującą w systemach UNIX do kontroli dostępu i innych testów związanych z bezpieczeństwem stosuje się identyfikatory efektywne. Odstępowanie od tej zasady nie powinno mieć miejsca bez dokładnego przemyślenia i udokumentowania.

Efektywne identyfikatory użytkowników i grup

Efektywne identyfikatory użytkowników i grup powinny być używane podczas podejmowania wszelkich decyzji związanych z kontrolą dostępu (DAC i MAC). Użytkownicy systemu mają wartości identyfikatorów z przedziału od 0 do 127. Identyfikatory zwykłych użytkowników zaczynają się od wartości 128 wzwyż.

Bezwzględne ścieżki dla komend zaufanych
Niektóre schematy obejścia zabezpieczeń polegają na stworzeniu fałszywego zaufanego programu, który zostaje umieszczony w ścieżce wyszukiwania programu pełniącego rolę powłoki używanej przez administratora lub nawet zwykłego użytkownika. Na przykład fałszywa kopia komendy **passwd** może posłużyć do przechwycenia hasła dla istniejącego lub nowego konta użytkownika.

Zalecaną praktyką w administracji jest usuwanie bieżącego katalogu roboczego ze ścieżki wyszukiwania, aby zabezpieczyć się przed takim posunięciem. Mogą jednak istnieć inne ścieżki wyszukiwania, nie zawsze objęte ścisłą ochroną, a szeregowy użytkownik musi mieć uprawnienia, by umieścić bieżący katalog roboczy we własnej ścieżce wyszukiwania. Skuteczną metodą przeciwdziałania temu zagrożeniu jest konsekwentne wywoływanie zaufanych programów z podaniem ścieżki bezwzględnej (na przykład `/usr/bin/passwd`). Program zaufany sprawdza swój pierwszy argument i nazwę wywołaną. W przypadku, gdy nie użyto poprawnej ścieżki bezwzględnej, program zaufany nie zostanie uruchomiony. Program zaufany powinien także sprawdzać, czy jego efektywny katalog główny nie różni się od bezwzględnego katalogu głównego.

Uwaga: Opisana metoda jest skuteczna tylko pod warunkiem, że użytkownicy są przyzwyczajeni do korzystania ze ścieżek bezwzględnych. Jeśli użytkownik nieumyślnie użyje ścieżki względnej, nastąpi wywołanie fałszywego programu i omawiany schemat obejścia zabezpieczeń okaże się nieskuteczny.

Struktura drzewa katalogów
Drzewa katalogów powinny mieć przemyślaną strukturę, aby zapewnić należytą ochronę newralgicznych plików. Podstawową zasadą jest nałożenie możliwie restrykcyjnych ograniczeń na dostęp do funkcji przeszukiwania katalogów (na przykład umieszczenie plików dostępnych publicznie w katalogach bliskich katalogowi głównemu systemu plików).

Zalecane jest też umieszczanie najbardziej newralgicznych katalogów jak najbliżej bezwzględnego katalogu głównego, ponieważ ogranicza to do minimum liczbę pośrednich katalogów, które należy objąć ścisłą ochroną.

Systemy plików tylko do odczytu
Być może najważniejszym zagadnieniem, jeśli chodzi o struktury drzew katalogów, jest miejsce, w którym umieszczane są rzadko zmieniane pliki zaufane we własnym systemie plików i podłączane jako pliki tylko do odczytu. Praktycznie zapewnia to, że ich treść nie może być zmieniona podczas normalnego działania systemu. Tej techniki często używa się dla dużych kolekcji plików wykonywalnych dla programów zaufanych.

Jeśli wymagana jest modyfikacja pliku, system plików można podłączyć ponownie jako system z możliwością zapisu w bardziej zabezpieczonym kontekście (na przykład w trybie pojedynczego użytkownika lub na oddzielnym, lepiej zabezpieczonym komputerze). Po takich aktualizacjach zaleca się użycie programów do skanowania systemu plików pod kątem poprawnej konfiguracji (na przykład, czy etykiety DAC, MIC i MAC są poprawne).

Ponadto informacji DAC, MIC i MAC nie można zmienić w systemie tylko do odczytu. Gdy system plików jest już odpowiednio skonfigurowany, powinno to zabezpieczyć przed schematami penetracji zabezpieczeń usiłującymi zmienić informacje DAC i/lub etykiety MIC i MAC.

Obsługa haseł
Ogólnie, nie jest dobrą praktyką wysyłanie zapytań do użytkownika o podanie hasła do zalogowania się przez programy inne niż standardowe programy narzędziowe. Hasła są informacjami objętymi szczególną ochroną i ich obsługa powinna być ściśle ograniczona do kilku istniejących i mających szczególne zaufanie systemowych programów narzędziowych.

W przypadku niektórych podsystemów zaufanych odpowiednim rozwiązaniem może być zaimplementowanie własnych haseł. Jednak poleganie na takich prywatnych schematach obsługi haseł może być niebezpieczne, ponieważ nie są one tak zabezpieczone jak mechanizmy wymuszane przez system.

Zabezpieczanie Zaufanej Bazy Przetwarzania (TCB)
Pliki zawierające elementy bazy TCB muszą być zabezpieczone przed modyfikacją, a w niektórych przypadkach przed ujawnieniem (odczytem) przez programy niezaufane.

Zabezpieczenie przed modyfikacją jest zadaniem krytycznym, a zabezpieczenie przed ujawnieniem może być zadaniem krytycznym. Należy zabezpieczyć następujące pliki:

- wszystkie pliki zawierające dane używane przez program zaufany podczas podejmowania decyzji dotyczącej bezpieczeństwa (na przykład plik zaszyfrowanych haseł),

- wszystkie pliki wykonywalne programu zaufanego,
- pseudopliki umożliwiające dostęp do części bazy TCB (na przykład `/dev/kmem`).

Uwaga: Należy zwłaszcza zabezpieczyć pliki inicjowania systemu (pliki rc) jako część bazy TCB.

Zabezpieczenie przed modyfikacją
Zabezpieczenie przed nieuprawnioną modyfikacją zasadniczo realizuje się przez ustawienie odpowiedniej wartości dla informacji DAC. Zwykle właścicielem tych plików jest ID użytkownika systemowego z dostępem do zapisu tylko dla właściciela pliku.

Etykietę MIC zaprojektowano z myślą o zabezpieczeniu przed modyfikacją. Zadanie to jest realizowane przez zabezpieczanie integralności obiektów. Określenie wysokiej etykiety MIC dla pliku powoduje, że procesy o niższych etykietach MIC nie mogą modyfikować, usuwać ani zmieniać nazwy tego pliku. Jest to idealna metoda zabezpieczania przed niepożądaną modyfikacją plików.

W niektórych sytuacjach do zabezpieczenia przed nieuprawnioną modyfikacją można użyć etykiety MAC. Jednak etykietę MAC zaprojektowano z myślą o zabezpieczeniu przed ujawnieniem (odczytem) i nie jest ona dobrze przystosowana do zabezpieczania przed modyfikacją. Podstawowa strategia MAC nie zabrania podmiotom modyfikowania obiektów z etykietą na wyższym poziomie. Chociaż nie jest to dozwolone dla bezpośrednich zapisów w pliku, niektóre podsystemy zaufane mogą zezwolić na to. Ponadto wiele zaufanych plików, takich jak wykonywalne pliki programów, musi mieć niski poziom etykiety MAC, aby były one ogólnie dostępne. Dlatego ustawienie dla pliku etykiety MAC na wysokim poziomie nie zawsze jest wykonalne.

Przed modyfikacją zabezpieczają także flagi zabezpieczeń plików. Niektóre flagi zabezpieczeń plików uniemożliwiają modyfikację obiektów nawet przez uprawnione podmioty. Jeśli dla pliku ustawiono flagę zabezpieczeń pliku **FSF_TLIB**, plik ten można zmienić tylko wtedy, gdy system jest w trybie konfigurowania, przy założeniu, że włączono flagę zabezpieczeń jądra **trustedlib_enabled**. Aby dla pliku ustawić flagę **FSF_TLIB**, proces musi mieć uprawnienie **PV_TCB** w swoim zbiorze EPS. Inną odpowiednią flagą zabezpieczeń plików jest **FSF_APPEND**, która uniemożliwia modyfikację uprzednio zapisanych danych. Do pliku z ustawioną flagą **FSF_APPEND** można tylko dodawać dane. Może to być przydatne wtedy, gdy aplikacja rejestruje rekordy w pliku.

Flagi te zwykle są ustawiane dla plików przez integratory, a nie w ramach sterowania programami. Programiści powinni mieć świadomość istnienia tych flag i funkcji, jakie one pełnią.

Zabezpieczenie przed ujawnieniem
Do ochrony plików bazy TCB przed dostępem do odczytu można użyć procedur DAC i MAC. Procedury MAC dla tych plików muszą dokładnie odzwierciedlać poziom wrażliwości informacji zawartych w tych plikach. Na przykład, jeśli klasyfikowany jest określony algorytm, etykieta MAC dla pliku wykonywalnego programu używającego tego algorytmu musi być odpowiednio ustawiona.

Akceptowalną praktyką jest ustawianie sztucznie zawyżonej etykiety MAC (tzn. na wyższym poziomie niż wynika z rzeczywistej klasyfikacji danych zawartych w tym pliku), aby zabezpieczyć dane przed ujawnieniem. Jednak z takich zawyżonych klasyfikacji należy korzystać oszczędnie.

W większości przypadków, aby plik był odpowiednio zabezpieczony, należy zabezpieczyć cały łańcuch katalogów, począwszy od absolutnego katalogu głównego. W przeciwnym razie złośliwy program może być w stanie odłączyć część łańcuchu katalogów i utworzyć nowe poddrzewo z fałszywą kopią pliku.

Załóżmy na przykład, że plik zaufany jest zapisany w ścieżce `/A/B/dom`. Chociaż plik **dom** jest zabezpieczony przed modyfikacją, katalog **B** nie jest przed nią zabezpieczony. Złośliwy program niezaufany mógłby usunąć dowiązanie w **B** do **dom** i utworzyć nowy plik **dom** zawierający fałszywą kopię starego pliku **dom**. Zaufane programy otwierające plik `/A/B/dom` otworzą fałszywy plik i mimowolnie będą korzystały z fałszywych danych.

Zaufane programy polegają na poprawnych nazwach ścieżek, aby uzyskać dostęp do plików bazy TCB. Dlatego pliki dowiązań symbolicznych używane w nazwach ścieżek dla plików bazy TCB powinny być tak mocno zabezpieczone jak same pliki.

W niektórych sytuacjach do zabezpieczenia przed nieuprawnionym ujawnieniem można użyć procedury MIC. Jednak procedura MIC jest głównie przeznaczona tylko do zabezpieczania przed modyfikacją (zapisaniem) i nie jest dobrze dostosowana do zabezpieczania przed ujawnieniem.

Operacje na etykietach czułości
Istnieją wytyczne dla programów zaufanych dla sytuacji obejmujących podmioty lub obiekty z różnymi etykietami czułości.

Użytkownik powinien znać formę etykiety czułości i relacje dominacji między etykietami. Określenie etykiety jako wyższej oznacza, że ta etykieta dominuje. Określenie etykiety jako niższej oznacza, że ta etykieta jest zdominowana. Podwyższenie etykiety oznacza podniesienie klasyfikacji danych do etykiety o wyższym poziomie, a jej obniżenie oznacza obniżenie poziomu klasyfikacji danych do etykiety o niższym poziomie.

Podstawowe ograniczenie MAC
Podstawowe, obowiązkowe ograniczenie w zakresie kontroli dostępu polega na tym, że niezaufany podmiot nie może zmienić etykiety czułości przypisanej do danych z A na B, jeśli B dominuje nad A.

Podstawowe ograniczenie MAC obejmuje wszystkie klasy danych. Podlegają mu ograniczenia dotyczące zarówno zmiany etykiet danych (czyli modyfikowania etykiety kontenera danych), jak i przenoszenia danych z etykietą między kontenerami.

Na różnych poziomach systemu (wywołanie systemowe, narzędzia usług systemowych itp.) to podstawowe ograniczenie jest realizowane za pomocą bardziej szczegółowych zestawów reguł, lecz zawsze z tym samym podstawowym założeniem, że poziom zabezpieczenia danych może być tylko podnoszony. Na przykład pierwszy poziom rozszerzenia mówi, że procesy mogą otwierać do odczytu dowolny z dużej klasy obiektów, jeśli etykieta procesu dominuje nad etykietą obiektu, a otwieranie do zapisu jest możliwe, jeśli etykieta obiektu dominuje nad etykietą procesu.

W przypadku zwykłych plików obowiązują jeszcze bardziej restrykcyjne ograniczenia co do operacji zapisu, wymagające, by plik miał taką samą etykietę jak proces. W przypadku katalogów i urządzeń operacje zapisu są dozwolone, jeśli etykieta SL podmiotu dominuje nad minimalną etykietą SL obiektu, a maksymalna etykieta SL obiektu dominuje nad etykietą SL podmiotu. W przypadku plików specjalnych FIFO (potoki nazwane) operacje odczytu są także ograniczone do plików specjalnych FIFO o takiej samej etykiecie, jak proces - w celu zabezpieczenia przed użyciem kanałów ukrytych.

Migracja danych na wyższy poziom czułości jest możliwa, ale nie jest to wymagane dla danego obiektu i sytuacji. Na przykład system operacyjny jako taki nie zezwala procesowi nieuprzywilejowanemu na otwieranie do zapisu pliku o wyższej etykiecie, mimo że podstawowe ograniczenie MAC dopuszcza taką sytuację. Decyzja, czy zezwolić na takie podnoszenie danych do podmiotów niezaufanych pozostaje kwestią projektu i przyjętych założeń. W niektórych przypadkach może to być przydatne, w innych - nie. Na przykład zapisy bezpośrednie w plikach o wyższej etykiecie rodzą taką trudność, że proces nie może później odczytywać tych plików, toteż użyteczność takich zapisów jest problematyczna. Niemniej jednak, proste, zaufane narzędzie, które podnosi etykietę pliku na żądanie niezaufanego podmiotu, może mieć sensowne i przydatne zastosowania.

Na poziomie wywołania systemowego ograniczenie dotyczy tylko procesów nieuprzywilejowanych. Oznacza to, że procesy uprzywilejowane nie podlegają ograniczeniu. Jednak praktycznie wszystkie usługi wykonywane przez system zaufany są przeznaczone dla użytkowników niezaufanych, dlatego od strony użytkownika ograniczenie obowiązuje.

Podstawowe ograniczenie MAC dotyczy wszystkich metod transmisji danych pozostających do dyspozycji programów niezaufanych. Jednak podstawowe ograniczenie MAC często jest dzielone na dwie składowe. Pierwsza z nich odnosi się tylko do funkcji systemu operacyjnego związanych z transmisją danych (lub przydzielaniem etykiet). Funkcje te obejmują na przykład odczytywanie i zapisywanie plików oraz przekazywanie danych między procesami. Druga składowa dotyczy metod komunikacji i jest osiągana za pomocą mechanizmów mających zasadniczo inne przeznaczenie. Metody te określa się nazwą kanałów ukrytych. Skuteczne egzekwowanie podstawowego ograniczenia MAC wobec kanałów ukrytych jest w praktyce niemożliwe. Z tego powodu zezwala się na istnienie kanałów ukrytych o niskiej przepustowości (np. 0,1 bita na sekundę), jednak tylko w przypadku, gdy jest to dostatecznie uzasadnione innymi względami.

Podstawowe ograniczenie MAC jest nieskomplikowane, a szczegółowych reguł dotyczących operacji na danych wielopoziomowych jest stosunkowo niewiele.

Operacje wielopoziomowe
Przez wywołanie systemowe **sec_setplab** proces uprzywilejowany może dowolnie zmieniać własną etykietę.

Ponieważ w przypadku wcześniej istniejących wywołań systemowych (czyli tych, które są zdefiniowane w podstawowym systemie operacyjnym) niemal wszystkie ograniczenia MAC i MIC dotyczące procesów nieuprzywilejowanych są również egzekwowane wobec procesów uprzywilejowanych, procesy uprzywilejowane wykonujące działania wielopoziomowe często korzystają z wywołania **sec_setplab**. Tymczasem użycie wywołania sec_setplab() przez programy zaufane powinno podlegać następującym regułom:

- W każdym przypadku użycie wywołania systemowego **sec_setplab** do wykonywania operacji wielopoziomowych (na przykład otwieranie plików z wysoką etykietą do odczytu) powinno się odbywać tylko za pośrednictwem procedur bibliotecznych, które odzwierciedlają semantykę wykonywanej rzeczywistej operacji wysokiego poziomu, ukrywając przy tym szczegóły użycia wywołania **sec_setplab**.
- Jedynym wyjątkiem są bardzo proste zmiany etykiet procesów, nie będące częścią większej operacji wielopoziomowej. W takich prostych operacjach dopuszczalne jest bezpośrednie użycie wywołania systemowego **sec_setplab**.

Powyższe wytyczne dotyczące wywołania **sec_setplab** są uzasadnione w dwójnasób. Po pierwsze, wrażliwa i potencjalnie niebezpieczna funkcja, jaką jest wywołanie systemowe **sec_setplab**, powinna być używana tylko w dobrze zaprojektowanym, modułowym otoczeniu. Po drugie, na skutek rozwoju standardów dotyczących systemów zaufanych, wywołania systemowe niskiego poziomu mogą obsługiwać rozmaite mechanizmy operacji wielopoziomowych.

Zawieranie operacji wysokiego poziomu w procedurach bibliotecznych zapewnia znakomitą zgodność z nowszymi wersjami oprogramowania i łatwość adaptacji do wymogów nowszych wersji systemu operacyjnego, ułatwiając jednocześnie przenośność między zaufanymi wersjami systemu UNIX.

System zaufany zawiera podstawowy zestaw takich procedur. Procedury te należy stosować wszędzie tam, gdzie jest to możliwe. Zestaw procedur powinien być sukcesywnie rozbudowywany z każdą nową wersją systemu operacyjnego. Programista systemów zaufanych może także tworzyć takie procedury biblioteczne stosownie do potrzeb.

Innym wyjątkiem od stosowania ograniczeń MAC i MIC jest używanie jednego lub większej liczby spośród dostępnych uprawnień MAC lub MIC, aby ominąć te ograniczenia. Dopuszczając stosowanie dowolnego z tych uprawnień, należy zachować daleko idącą ostrożność.

Komunikacja między procesami systemu System V
Mechanizmy komunikacji między procesami (IPC), takie jak kolejki komunikatów, semafory i pamięć współużytkowana, podlegają ograniczeniom DAC, MIC i MAC. Zwykle nie ma żadnych komend umożliwiających tworzenie i używanie obiektów komunikacji IPC systemu System V.

Wywołania systemowe AIX związane z komunikacją IPC zmodyfikowano, tak aby obsługiwały wielopoziomowość w systemie Trusted AIX. Do tych zmodyfikowanych wywołań systemowych należą:

- **msgget**
- **msgsnd**
- **msgrcv**
- **msgctl**
- **semget**
- **semop**
- **semctl**
- **shmget**
- **shmctl**
- **shmat**
- **shmdt**

Ponadto do systemu Trusted AIX dodano następujące wywołania systemowe zaprojektowane z myślą o manipulowaniu atrybutami MAC obiektów IPC:

sec_getmsgsec
Pobranie atrybutów bezpieczeństwa kolejek komunikatów.

sec_getsemsec
Pobranie atrybutów bezpieczeństwa semaforów.

sec_getshmsec
Pobranie atrybutów bezpieczeństwa segmentów pamięci współużytkowanej.

sec_setmsglab
Ustawienie atrybutów bezpieczeństwa kolejek komunikatów.

sec_setsemlab
Ustawienie atrybutów bezpieczeństwa semaforów.

sec_setshmlab
Ustawienie atrybutów bezpieczeństwa segmentów pamięci współużytkowanej.

Informacje dotyczące uprawnień wymaganych dla procesów, aby mogły manipulować obiektami IPC, zawiera sekcja Dostęp do obiektów IPC. Do manipulowania atrybutem IPC można użyć komendy **settxattr**.

Górne etykiety MIC i MAC implementacji i systemu
Niejednokrotnie proces zaufany musi ustalić etykietę MAC, która dominuje nad wszystkimi innymi etykietami w systemie. Można w tym celu użyć dwóch różnych etykiet MAC: górnej etykiety MAC implementacji i systemu.

Górna etykieta MAC implementacji jest najwyższą etykietą MAC obsługiwaną przez system Trusted AIX. Jest prawdopodobne, że ta etykieta ma klasyfikację hierarchiczną i zawiera kategorie, które nie są używane w danym ośrodku. Etykieta jest łatwa do wygenerowania, lecz należy z niej korzystać ostrożnie. Żaden proces nie powinien tworzyć obiektów z tą etykietą.

Górna etykieta MAC systemu jest najwyższą etykietą MAC używaną w danym ośrodku. Definiuje ją administrator w pliku **LabelEncodings**.

Korzystanie z górnej etykiety MAC systemu jest mniej efektywne, lecz jest zdecydowanie zalecane, ponieważ administrator może skutecznie ograniczać działania nawet procesów uprzywilejowanych, właściwie ustawiając odpowiedni parametr w pliku **LabelEncodings**.

Analogiczne górne etykiety implementacji i systemu można zdefiniować dla MIC.

Zakresy logowania dla użytkowników i systemu
Programy zaufane wykonujące usługi dla użytkowników mogą potrzebować ograniczać etykiety MIC i MAC obejmujące te operacje do wartości, za pomocą których użytkownik może zalogować się i/lub ograniczać je do etykiet logowania dozwolonych w systemie.

Zezwolenia przypisane do użytkowników w systemie znajdują się w pliku `/etc/security/user` bazy danych **user**, a dostęp do nich można uzyskać za pomocą procedur bibliotecznych **getuserattr** i **getuserattrs**.

Trusted AIX umożliwia użytkownikom działanie w systemie z użyciem dowolnej etykiety mieszczącej się w zakresie akredytacji systemu i zdominowanej przez maksymalne zezwolenia użytkownika i dominującej nad minimalnymi zezwoleniami użytkownika. Wszystkie programy umożliwiające użytkownikom działanie z użyciem różnych etykiet powinny zawsze zapewnić, aby nowa etykieta była poprawna dla danego użytkownika.

Na przykład przypuśćmy, że zdefiniowano program narzędziowy **upgrade** do podniesienia etykiety MAC dla pliku na żądanie użytkownika. Podstawowe ograniczenie MAC wymaga, aby program **upgrade** akceptował tylko te pliki, których etykieta MAC jest zdominowana przez etykietę użytkownika. Ponadto rozważnym (chociaż nie niezbędnym z punktu wiedzenia podstawowego ograniczenia MAC) rozwiązaniem jest zastosowanie nowej etykiety, która umożliwi zalogowanie się użytkownika obejmującej ograniczenia zakresu etykiety zarówno dla danego użytkownika, jak i w systemie. Do tego celu program narzędziowy **upgrade** użyje zarówno interfejsu **sl_cmp**, jak i interfejsu **accredrange**.

Struktura drzewa katalogów
Wywołania systemowe działają w ten sposób, że drzewa katalogów utworzone przez nieuprawnione procesy były zgodne ze strukturą niemalejących etykiet, w której etykieta pliku jest równa etykiecie jego katalogu nadrzędnego lub mieści się w zakresie katalogu partycjonowanego, a etykieta katalogu dominuje nad etykietą jego katalogu nadrzędnego (należy zauważyć, że dominacja obejmuje relację równości). Jest to naturalna struktura dla niezaufanych programów.

Jednak procesy z uprawnieniami nie są powiązane przez to ograniczenie i mogą tworzyć drzewa katalogów, w których relacje między etykietami MAC katalogów są dowolne. Takie konfiguracje są przydatne, ponieważ dostęp do wyszukiwania MAC jest ograniczany w miarę zbliżania się do katalogu głównego drzewa. Na przykład zabezpieczenie zagregowane, w którym etykieta MAC kolekcji obiektów danych jest wyższa niż jakakolwiek pojedyncza etykieta obiektu, można zaimplementować, ustawiając etykietę MAC katalogu na wyższą niż etykiety jej elementów. Procesy niezaufane muszą dominować nad etykietą katalogu, aby uzyskać dostęp do agregacji danych.

Należy zachować szczególną ostrożność podczas tworzenia drzew katalogów z malejącymi etykietami. Nieuprawniony proces nie może otworzyć pliku do zapisu, gdy plik ten nie dominuje nad etykietą jego katalogu nadrzędnego lub jest mu równy.

Implementacje katalogów partycjonowanych
Istnieje szereg wywołań systemowych, które zachowują się odmiennie dla różnych implementacji katalogów partycjonowanych.

Podane poniżej wywołania systemowe zachowują się odmiennie zależnie od implementacji katalogów partycjonowanych:

- getdirents
- link
- mkdir
- mount
- rename
- rmdir
- stat
- lstat
- fstat

Tryb procesu
Komenda **pdmode** wykonuje komendę w podanym trybie. Proces może użyć wywołania systemowego **setppdmode**, aby ustawić własny tryb na rzeczywisty lub wirtualny. Wywołanie systemowe **setppdmode** wymaga uprawnienia **PV_PROC_PDMODE**. Nie istnieje mechanizm, za pomocą którego proces mógłby zmienić tryb innego procesu.

Typ katalogu
Do zmiany zwykłego katalogu w katalog partycjonowany można użyć komendy **pdset**, ale nie istnieje komenda do zmiany katalogu partycjonowanego (lub podkatalogu partycjonowanego albo podkatalogu partycjonowanego) w zwykły katalog.

Do tworzenia katalogów partycjonowanych można także użyć wywołania systemowego **pdmkdir**. Wywołanie systemowe **pdmkdir** wymaga uprawnienia **PV_FS_PDMODE**.

Uwagi dotyczące etykiet MIC i MAC
Wszystkie programy do określenia relacji między etykietami MIC i MAC powinny używać tylko funkcji **sl_cmp** i **tl_cmp**.

Jest to szczególnie ważne dlatego, że wewnętrzny format etykiety może zostać zmieniony w nowszej wersji, a te procedury biblioteczne śledzą zmianę formatów. Analogicznie istnieje wiele innych procedur bibliotecznych manipulujących etykietami MIC i MAC, których należy używać, gdy tylko jest to możliwe.

Wywołania systemowe **setea**, **lsetea** i **fsetea** zmieniają etykietę MIC lub MAC pliku. Wywołanie systemowe **fsetea** akceptuje deskryptor pliku.

Sterowniki urządzeń
Podczas tworzenia sterowników urządzeń dla systemu Trusted AIX należy przestrzegać określonych zasad i wytycznych. Należy mieć wystarczającą wiedzę w zakresie mechanizmów tworzenia sterowników urządzeń dla podstawowego systemu operacyjnego oraz zasad dotyczących korzystania z tych mechanizmów.

Podsystem zarządzania urządzeniami
Urządzenie w systemie AIX jest tworem abstrakcyjnym, służącym do organizowania obiektów danych, do których dostęp odbywa się przez odwołania do plików specjalnych urządzeń. W niektórych przypadkach obiekty danych reprezentują rzeczywiste urządzenia fizyczne, w innych całkiem inne twory, na przykład urządzenie `/dev/null`, które nie jest obiektem do przechowywania danych. Urządzenia z tej drugiej klasy często są nazywane pseudourządzeniami.

W systemach Trusted AIX działają urządzenia dwóch typów: urządzenia jednoetykietowe i urządzenia wielopoziomowe. Urządzenie wielopoziomowe ma status zaufany, który umożliwia przetwarzanie danych na więcej niż jednym poziomie czułości jednocześnie. Urządzenie jednoetykietowe zazwyczaj ma status niezaufany. Etykiety danych są zwykle powiązane z informacjami, które urządzenie wielopoziomowe obsługuje w taki sposób, aby zagwarantować prawidłowe przypisania etykiet danym. Urządzenie jednoetykietowe natomiast zwykle nie kwestionuje etykiet nadanych zewnętrznie.

Dysk twardy jest przykładem urządzenia wielopoziomowego. Wszystkie dane umieszczone na twardym dysku mają odpowiednie etykiety czułości. Drukarka, fizycznie znajdująca się w otoczeniu, do którego wstęp wymaga określonych uprawnień, jest przykładem urządzenia jednoetykietowego. Drukarka będzie przyjmować zadania wydruku tylko w przypadku danych wysłanych z użyciem takich właśnie uprawnień.

Przestrogi dla programistów sterowników urządzeń
Sterowniki urządzeń wchodzą w skład jądra systemu operacyjnego, toteż ich działanie nie podlega ograniczeniom. Tworzenie i modyfikowanie sterowników urządzeń jest zabiegiem równie newralgicznym, jak modyfikowanie samego jądra. Niestety, konieczność tworzenia lub modyfikowania sterowników urządzeń często występuje po stronie użytkownika. Należy przy tym bezwzględnie zachować najwyższą ostrożność.

Nie da się tu zebrać wszystkich uwag i ostrzeżeń, o jakich powinien pamiętać programista sterowników urządzeń, ponieważ sterowniki mogą (czasem zupełnie nieumyślnie) naruszać bezpieczeństwo systemu na wiele różnych sposobów. Dlatego bezpieczeństwo sterowników urządzeń zależy przede wszystkim od rozsądku i doświadczenia projektanta.

Sterowniki urządzeń nie powinny wykonywać żadnych innych operacji, tylko proste zarządzanie funkcjami urządzenia. Sterowniki urządzeń są tworzone głównie w celu dodania nowych wywołań systemowych, w tym sterowników pseudourządzeń, na przykład sterowniki znajdując się w `/dev/kmem`, należy traktować jako nowe wywołania systemowe i stosować podczas ich projektowania odpowiednie do tego zasady. Wskazówki zawarte w tej sekcji dotyczą przede wszystkim sterowników rzeczywistych urządzeń.

Przed rozpoczęciem tworzenia nowych sterowników urządzeń programista powinien dokładnie zapoznać się z budową sterowników już istniejących. Najważniejsze czynności sterowników urządzeń wpływające na bezpieczeństwo mają związek z obsługą wywołań systemowych **open** i **ioctl**.

Otwieranie urządzeń
Podobnie jak w przypadku większości obiektów systemowych, większość testów zabezpieczeń związanych z dostępem do urządzeń ma miejsce podczas otwierania urządzenia przez wywołanie systemowe **open**.

Jądro najpierw wykonuje zestaw podstawowych operacji, a następnie przekazuje przetwarzanie żądania otwarcia do sterownika urządzenia. Przed przekazaniem sterowania do sterownika urządzenia jądro przeprowadza następujące testy zabezpieczeń:

- Jeśli proces nie ma dostępu MAC do pliku specjalnego urządzenia, wywołanie open kończy się niepowodzeniem.

- Jeśli proces nie ma dostępu MIC do pliku specjalnego urządzenia, wywołanie open kończy się niepowodzeniem.
- Jeśli proces nie ma dostępu DAC do pliku specjalnego urządzenia, wywołanie open kończy się niepowodzeniem.

W przypadku wielu urządzeń odczyt z urządzenia (przy użyciu wywołania systemowego **read**) zmienia stan urządzenia w sposób możliwy do wykrycia przez inny proces, którego etykieta MAC nie dominuje nad etykietą procesu odczytującego. Stwarza to możliwość powstania kanału ukrytego. Problem ten dotyczy przede wszystkim urządzeń typu FIFO. W takich przypadkach typową praktyką jest ograniczanie uprawnień do odczytu do procesów mających taką samą etykietę MAC, jak urządzenie. Osiąga się to, przeprowadzając odpowiedni test w sterowniku urządzenia.

Nie istnieje wiele reguł ani wytycznych dotyczących projektowania urządzeń nieregularnych. Należy rozumieć i stosować podstawowe zasady obowiązkowej i indywidualnej kontroli dostępu. Na szczęście większość sterowników urządzeń można skonfigurować jako urządzenia regularne, toteż nietypowe działanie sterowników urządzeń nieregularnych nie jest częstym źródłem problemów.

Przykłady obsługi wywołania open przez sterowniki urządzeń
Poniżej przedstawiono przykłady obsługi urządzeń nieregularnych, pochodzące ze standardowych sterowników urządzeń systemowych. Ilustrują one możliwą różnorodność tego typu sterowników.

/dev/null

`/dev/null` jest to pseudourządzenie pozbawione kontenera na dane. Dane zapisywane w urządzeniu `/dev/null` są odrzucane, a w odpowiedzi na żądanie odczytu zawsze zwracany jest znak końca pliku (EOF). Dlatego wywołanie open nie podlega żadnym ograniczeniom MAC. Ze względu na wymogi zgodności wymagany jest dostęp DAC do pliku `/dev/null`, mimo że nie jest to w rzeczywistości konieczne.

/dev/tty

Kiedy proces wysyła żądanie otwarcia urządzenia `/dev/tty`, sterownik urządzenia w istocie próbuje otworzyć terminal sterujący związany z tym procesem. Dlatego uprawnienia MIC, MAC i DAC muszą zostać sprawdzone dla procesu terminalu związanego z procesem wysyłającym żądanie, a nie dla pliku `/dev/tty`. Ze względu na wymogi zgodności wymagany jest dostęp DAC do pliku `/dev/tty`, mimo że nie jest to w rzeczywistości konieczne.

Ograniczenia dotyczące interfejsu ioctl
Wszystkie funkcje interfejsu sterownika urządzeń muszą być zaufane, jednak interfejs **ioctl** zazwyczaj wymaga szczególnej uwagi.

Z reguły tylko procesy z prawem do zapisu mogą zmieniać atrybuty pliku w taki sposób, aby zmiany te mogły wykryć inne procesy pozbawione prawa do zapisu. Prawo do zapisu oznacza, że dany proces otworzył plik do zapisu albo że etykieta MAC procesu jest równa etykiecie urządzenia. Ograniczenie to wywodzi się z podstawowego ograniczenia MAC, które mówi, że żaden proces nie może wykonywać czynności, które mogą zostać wykryte przez procesy mające niższe etykiety MAC.

Jeśli celem działania jest operacja odczytu/zapisu danych użytkownika, ograniczenie to musi być egzekwowane dosłownie. Sytuacje, w których ograniczenie to nie jest egzekwowane w pełni, prowadzą do powstawania kanałów ukrytych, które powinny podlegać ograniczaniu przepustowości i być objęte kontrolą.

Niektóre czynności związane ze sterowaniem urządzeniem mogą wymagać zastrzeżenia tylko dla procesów uprzywilejowanych, nawet jeśli urządzenie to nie jest skonfigurowane jako zaufane.

Inne ograniczenia
Jest stosunkowo niewiele innych sytuacji, w których sterownik urządzenia może wymagać wymuszania specjalnych testów zabezpieczeń.

Jako przykład można podać odczyt z urządzenia powodujący zmianę jego stanu w sposób możliwy do wykrycia przez proces, którego etykieta MAC nie jest dominowana przez etykietę procesu odczytującego.

Stwarza to potencjalny kanał ukryty, wymagający ograniczania lub kontrolowania przez sam sterownik urządzenia.

Podsumowanie zasad programowania sterowników urządzeń
Podczas implementacji sterowników urządzeń należy przestrzegać następujących wytycznych.

Uwaga: Dodano nowe wywołania systemowe obsługujące rozszerzone funkcje bezpieczeństwa dla operacji odczytu i zapisu w strumieniach i urządzeniach FIFO. Do obsługi tego rozszerzonego atrybutu bezpieczeństwa służą nowe biblioteczne funkcje API, eread() i ewrite(). W przypadku jądra MLS Kernel dla urządzenia zostaje ustawiona opcja bezpieczeństwa DEV_SEC_ERDWR. Podobnie, dla urządzeń FIFO ustawiana jest opcja GNF_SEC_ERDWR. Opcje te umożliwiają dodatkowe testy bezpieczeństwa dla każdej operacji odczytu i zapisu.

Ogólne techniki projektowania

Wszystkie testy bezpieczeństwa wykonywane w sterowniku urządzenia powinny mieć postać modułową i być łatwe do identyfikacji.

Testy wykonywane w przez sterowniki urządzeń

W każdej sytuacji zalecane jest wyprowadzanie testów MIC, MAC i DAC poza sterownik urządzenia. Sterowniki urządzeń pozbawione takich testów mogą być łatwo przenoszone do lub z systemów niezaufanych lub systemów zaufanych innych typów.

W implementacji regularnego sterownika urządzenia jądro wykonuje testy MIC, MAC i DAC, a sterownik realizuje wszelkie dodatkowe wymagane testy uprawnień. W nieregularnej implementacji sterownika urządzenia wszystkie testy (MIC, MAC, DAC i testy uprawnień) wykonuje sam sterownik. Wybór między implementacją regularnego i nieregularnego sterownika urządzenia pozostaje kwestią oceny projektanta.

DAC

Zasady DAC są wymuszane dla każdego pliku specjalnego urządzenia w oparciu o punkt wejścia w systemie plików używany przy dostępie do urządzenia.

Sprawdzanie poprawności instalacji

Każdy sterownik urządzenia wykonujący testy MAC powinien bezpiecznie obsługiwać (w rozsądnych granicach) ewentualność nieprawidłowej definicji urządzenia.

Dostęp uprzywilejowany

Niekiedy jest zalecane, by sterownik urządzenia rezerwował pewne operacje na urządzeniu dla procesów uprzywilejowanych. W sytuacjach takich obowiązuje jednak kilka szczególnych zaleceń.

Posiadanie wymaganych uprawnień można sprawdzić za pomocą funkcji jądra **refmon**.

Najniższy poziom uprawnień
W systemie Trusted AIX wprowadzono koncepcję najniższego poziomu uprawnień. Najniższy poziom uprawnień umożliwia zastąpienie powszechnego wcześniej, wszechpotężnego administratora (root) mechanizmem uprawnień o większej subtelności. Wprowadzony zostaje podział uprawnień, dzięki któremu ewentualny błąd programowania lub inny defekt w oprogramowaniu zaufanym spowoduje minimalne szkody z punktu widzenia bezpieczeństwa systemu.

Operacje na uprawnieniach
Z każdym procesem powiązane są cztery wektory uprawnień: efektywne, maksymalne, odziedziczone i ograniczające.

Wektor uprawnień maksymalnych definiuje górny limit uprawnień, które mogą być aktywne dla każdego procesu. Wektor uprawnień efektywnych definiuje uprawnienia, które są sprawdzane w celu podjęcia decyzji o uprawnieniach. Należy zauważyć, że zbiór uprawnień efektywnych jest podzbiorem zbioru uprawnień maksymalnych, który z kolei jest zawsze podzbiorem ograniczającego zbioru uprawnień.

Ograniczający zbiór uprawnień definiuje uprawnienia, które może mieć proces w swoich zbiorach uprawnień maksymalnych, odziedziczonych i efektywnych. Zbiór uprawnień odziedziczonych reprezentuje zbiór uprawnień, które są dziedziczone przez proces potomny w wywołaniach fork i exec.

Gdy wykonywany jest obraz nowego kodu programu, następuje eskalacja uprawnień w oparciu o podany poniżej algorytm. Do wspomnianych uprawnień specjalnych należą: **PV_ROOT**, **PV_SU_**, **PV_SU_EMUL**, **PV_SU_ROOT**, **PV_AZ_ROOT** i **PV_SU_UID**.

Poniższy algorytm demonstruje dwie ważne koncepcje dotyczące podsystemu najmniejszego uprzywilejowania. Pierwsza koncepcja mówi, że uprawnienia specjalne (**PV_ROOT**, **PV_SU_**, **PV_SU_EMUL**, **PV_SU_ROOT**, **PV_AZ_ROOT** i **PV_SU_UID**) są jedynymi uprawnieniami, które mogą być bezwarunkowo propagowane podczas wykonywania obrazu nowego procesu. Druga koncepcja mówi, że wektor uprawnień efektywnych procesów jest wyczyszczony z wszystkich uprawnień, chyba że dla pliku ustawiono **FSF_EPS**. Dzięki temu zapewniona jest kompatybilność wsteczna z aplikacjami, które muszą być uruchamiane w systemie zaufanym bez zaliczania do systemu najmniejszych uprzywilejowań.

```
new_max_privs = old_inheritable_privs
new_max_privs = new_max_privs | file_innate_privs
IF (użytkownikowi przypisano niektóre autoryzacje w pliku PAS)
new_max_privs = new_max_privs | file_authorized_privs
new_max_privs = new_max_privs & old_limiting_privs
IF (old_max_privs zawiera jedno lub więcej uprawnień specjalnych)
new_max_privs += ten sam zbiór uprawnień specjalnych
IF (FSF_EPS jest zbiorem dla kodu wykonywalnego)
new_eff_privs = new_max_privs
ELSE
new_eff_privs = old_inheritable_privs
IF (old_eff_privs zawiera jedno lub więcej uprawnień specjalnych)
new_eff_privs += ten sam zbiór uprawnień specjalnych
new_limiting_privs = old_limiting_privs
```

Przypisywanie i odbieranie uprawnień
Następujące standardowe procedury z bibliotek systemowych ilustrują operowanie na uprawnieniach w systemie. Procedury te są użyteczne tylko dla uprawnionych programów w systemie.

priv_raise
Zmienia wektor efektywnych uprawnień procesu, dodając (lub podnosząc) podaną listę uprawnień. Lista uprawnień musi zawierać się w wektorze maksymalnych uprawnień procesu, w przeciwnym razie zwracany jest komunikat o błędzie.

priv_remove
Zmienia wektor uprawnień efektywnych i maksymalnych procesu, odbierając podaną listę uprawnień. Jeśli proces nie może usunąć uprawnień efektywnych lub maksymalnych, zwracany jest komunikat o błędzie.

priv_lower
Zmienia wektor efektywnych uprawnień procesu, odbierając (lub obniżając) podaną listę uprawnień. Jeśli proces nie może obniżyć uprawnień efektywnych, zwracany jest komunikat o błędzie.

Każda z tych procedur przyjmuje jako parametr listę uprawnień rozdzielonych przecinkami, zakończoną przez **-1** (minus jeden, niepoprawny numer uprawnienia). Technika podnoszenia i obniżania uprawnień wokół najmniejszego fragmentu kodu, który może tych uprawnień wymagać, jest nazywana ograniczaniem czasowym uprawnień. Wszystkie zaufane aplikacje powinny korzystać z techniki ograniczania uprawnień, aby ograniczyć ryzyko naruszenia zabezpieczeń przez źle zaprojektowane lub zrealizowane oprogramowanie.

setppriv
Zmienia dla procesu wektor uprawnień efektywnych, maksymalnych, dziedziczonych i ograniczających, ustawiając odpowiednio zestawy uprawnień. Jeśli przekazane zestawy uprawnień są niepoprawne lub nie są dozwolone, zwracany jest komunikat o błędzie.

Autoryzacje
Autoryzacje są to zestawy służące do grupowania uprawnień przyznawanych użytkownikom.

Zazwyczaj komenda lub program narzędziowy sprawdza autoryzację na początku wykonywania i odpowiednio do niej określa własne uprawnienia. Dlatego użytkownicy z określoną autoryzacją uzyskują odmienne zestawy uprawnień w przypadku różnych wykonywanych komend, zależnie od sposobu zaprogramowania danej komendy.

Aby uniknąć nieporęcznej metody definiowania uprawnień bezpośrednio w kodzie programu, w systemie AIX można korzystać z zestawów autoryzacji i zestawów uprawnień określanych poza plikami binarnymi. Jeśli są stosowane zestawy PAS (Privileged Authorization Set) i APS (Authorized Privilege Set), system przejmuje od komendy zadanie ustawiania uprawnień w oparciu o autoryzację.

checkauths
Porównuje przekazaną listę autoryzacji z autoryzacjami skojarzonymi z bieżącym procesem.

Więcej informacji na temat sprawdzania autoryzacji zawiera sekcja “Autoryzacje RBAC” na stronie 88.

Kontrola
System Trusted AIX został wyposażony w zestaw komend do zarządzania zawartością i procesem generowania zapisów kontrolnych. Jest mało prawdopodobne, że programista systemu zaufanego będzie widział konieczność modyfikowania lub rozbudowy tych programów.

audit
Steruje demonem kontroli.

auditbin
Steruje obsługą plików z zapisami kontrolnymi.

auditselect
Scala i wybiera rekordy kontroli z plików z zapisami kontrolnymi.

auditpr
Wyświetla wybrane zdarzenia kontrolowane w postaci czytelnej.

Najważniejszym aspektem systemu kontroli, który ma znaczenie dla programisty systemu zaufanego, są zdarzenia kontrolowane generowane przez programy zaufane. Większość programów zaufanych musi kierować komunikaty do systemowego zapisu kontroli.

Sytuacje poddawane kontroli
Niewiele jest szczegółowych wytycznych odnośnie ustalania, które sytuacje powinny być wykrywane i kontrolowane przez program zaufany. Jest to przede wszystkim kwestia indywidualnego osądu i strategii kontroli. System podstawowy dzieli pełne spektrum sytuacji na powodzenia, błędy, dostęp do obiektów i potencjalne użycie kanałów ukrytych.

Powodzenia
Operacje zakończone powodzeniem należy uwzględnić w zakresie kontroli, tak aby powstał podstawowy zapis historii operacji.

Na przykład program przydzielający urządzenie powinien rejestrować, kiedy określony użytkownik przydziela i zwalnia urządzenie. Dzięki temu program może śledzić przepływ informacji przez system i ustalać odpowiedzialność użytkowników, gdy później wyjdzie na jaw, że urządzenie zostało użyte w niedozwolony sposób. Z drugiej strony, według niektórych koncepcji kontroli operacje wykonane pomyślnie niosą niewiele informacji, ponieważ zostały uznane za uprawnione i prawidłowe przez zaufane oprogramowanie.

Nieudane operacje
Kontrolowanie nieudanych operacji może być użyteczne przy wykrywaniu użytkowników usiłujących uzyskać nieuprawniony dostęp do usług lub danych. Duża częstotliwość nieudanych operacji może wskazywać na obecność w personelu osób mających złe zamiary (choć nie odznaczających się szczególną bystrością).

System podstawowy dzieli nieudane operacje na pięć kategorii:

- błąd uprawnień (podjęta przez proces nieuprzywilejowany próba wykonania czynności zastrzeżonej dla procesów uprzywilejowanych);
- błąd MAC (niepowodzenie czynności z powodu naruszenia ograniczeń MAC);

- błąd MIC (niepowodzenie czynności z powodu naruszenia ograniczeń MIC);
- błąd DAC (niepowodzenie czynności z powodu naruszenia ograniczeń DAC);
- inny błąd (na przykład próba logowania z użyciem niepoprawnego hasła).

Dostęp do obiektów
Monitorowanie dostępu do obiektów jest konieczne, aby kontrolować użytkowników odwołujących się do danego obiektu (na przykład pliku zaszyfrowanych haseł).

Potencjalne kanały ukryte
Kontrolowanie potencjalnych kanałów ukrytych ma duże znaczenie, ponieważ kanały ukryte mogą być wykorzystywane do przekazywania informacji między procesami mającymi różne etykiety MAC. Potencjalne kanały ukryte nie zawsze są używane do tego celu, jednak taka możliwość stale występuje.

Każdy zapis tworzony przez system kontrolny zawiera przyczynę utworzenia wpisu (powodzenie, błąd MAC, błąd MIC, błąd DAC, błąd uprawnień, inny błąd, dostęp do obiektów lub potencjalny kanał ukryty). Dotyczy to zarówno rekordów kontroli zapisanych przez system, jak i przez programy użytkownika.

Użyteczne może być ustalenie, czy użytkownik był zaufany (tzn., czy był administratorem), jednak nie istnieje metoda pewnego ustalenia, czy dany użytkownik zaufany lub niezaufany wymaga bardziej zaawansowanej kontroli. Na przykład chociaż administratorzy z definicji są zaufani i z tego powodu mogą wymagać słabszej kontroli, wykonywane przez nich czynności mają bardzo dalekosiężne skutki, dlatego rejestrowanie działań podejmowanych przez nieuprawnionego administratora może być użyteczne. Zwykli użytkownicy są w stanie wyrządzić mniejsze szkody, dlatego mogą wymagać mniej intensywnej kontroli, chociaż z drugiej strony ich konta są w mniejszym stopniu zaufane i powinny być kontrolowane mocniej. Administratorzy systemu często nakładają na swoje działania zaostrzone rygory kontroli, aby można było dowieść swojej niewinności w przypadku naruszenia bezpieczeństwa systemu.

Następujące zdarzenia powinny podlegać kontroli:

- operacje wykonane pomyślnie, zwłaszcza operacje związane z przekazywaniem informacji lub zmianą parametrów kontroli dostępu;
- operacje udaremnione przez system bezpieczeństwa;
- operacje wykonywane przez administratorów, zarówno udane, jak i nieudane;
- potencjalne użycie kanałów ukrytych;
- operacje wymagające dostępu do określonego obiektu;
- działania mające wpływ na przyszłą zawartość zapisu kontrolnego.

Poziomy szczegółowości zapisu kontrolnego
Zapis kontrolny o wyższym poziomie szczegółowości zawiera więcej użytecznych informacji. Programy zaufane mają dostęp do szczegółowych informacji o przebiegu różnych operacji i dzięki temu mogą generować komunikaty kontrolne wysokiej jakości.

Zapis mówiący tylko o tym, że administrator otworzył chroniony plik do zapisu, jest znacznie mniej użyteczny od szczegółowego zapisu operacji wykonanej na pliku (na przykład utworzenie przez administratora nowego wpisu w pliku, wraz z podstawowymi elementami treści tego wpisu). Zalecane jest, by zapisy kontrolne były prowadzone na jak najwyższym poziomie szczegółowości.

Lepiej jest, gdy pojedynczy zapis zawiera informacje o jednym zdarzeniu, a nie zbiorcze o kilku zdarzeniach. Głównym powodem przemawiającym za dzieleniem jednego wystąpienia kontroli na więcej niż jedno zdarzenie jest możliwość selektywnego włączania oddzielnych wystąpień.

Klasy i zdarzenia związane z kontrolą
Każdy program zaufany musi ustalić klasę kontroli, typ zdarzenia kontroli oraz przyczynę, której będzie używał podczas wysyłania komunikatów kontroli przy użyciu wywołania systemowego **auditlog**.

Każde zdarzenie kontroli należy do klasy kontroli. Przypisując zdarzenia do klas, można skuteczniej obsługiwać dużą liczbę zdarzeń. Definicje klas kontroli znajdują się w pliku `/etc/security/audit/config`.

Klasa kontroli służy do włączania i wyłączania rejestracji zdarzeń. Jeśli dwa zdarzenia powinny być włączone oddzielnie, nie powinny się znajdować w jednej klasie kontroli. Niemniej jednak, na ogół grupowanie zdarzeń w klasy przynosi korzyści. Zazwyczaj każdy zaufany program lub zestaw zaufanych programów rezerwuje jedną nazwę klasy kontroli (lub, w rzadkich przypadkach, kilka nazw klas kontroli) do indywidualnego użytku.

Podlegające kontroli czynności systemu są definiowane jako zdarzenia kontroli w pliku `/etc/security/audit/events`.

Ukryte kanały
Oprogramowanie zaufane nie powinno korzystać z ukrytych kanałów. Ponadto oprogramowanie takie powinno być konstrukcyjnie zabezpieczone przed wykorzystaniem go przez niezaufane oprogramowanie do wykorzystania kanałów ukrytych. W tej sekcji zdefiniowano pojęcie ukrytych kanałów i podano wytyczne w kwestii ich wykrywania i ograniczania skuteczności.

Definicja ukrytych kanałów
Żaden proces o etykiecie A nie będzie mógł wykonać czynności, która może być wykryta przez inny proces o etykiecie B z wyjątkiem sytuacji, gdy etykieta B dominuje nad etykietą A.

Definicję tę można rozpatrywać w kontekście dwóch różnych sytuacji: bezpośrednie operowanie na danych i operacje incydentalne. Bezpośrednie operowanie na danych to dla użytkowników bezpośrednia metoda przechowywania lub przesyłania danych użytkownika, na przykład odczyt i zapis w plikach. W operacjach tych musi być ściśle przestrzegane podstawowe ograniczenie MAC. Wszystkie inne operacje to operacje incydentalne. Użycie operacji incydentalnej w celu przekazania danych wbrew podstawowemu ograniczeniu MAC nosi nazwę kanału ukrytego.

Wykorzystanie kanału ukrytego wymaga użycia dwóch niezaufanych procesów, które będą tu nazywane nadawcą (etykieta X) i odbiorcą (etykieta Y). Ponadto czynimy założenie, że etykieta MAC odbiorcy nie dominuje nad etykietą nadawcy (gdyby tak było, przepływ danych od nadawcy do odbiorcy byłby uprawnionym podniesieniem poziomu bezpieczeństwa danych). Aby wykorzystać ten kanał, nadawca i odbiorca stosują pewne konwencje dotyczące użycia uzgodnionych zasobów w celu przekazania danych wbrew ograniczeniu MAC.

Jedyne kryterium decydujące o tym, że wykorzystano ukryty kanał, to warunek, by nadawca i odbiorca były procesami niezaufanymi oraz by etykieta odbiorcy nie dominowała nad etykietą nadawcy. Nadawca i odbiorca zazwyczaj są uruchomione na w imieniu tego samego użytkownika. Zakłada się, że TCB samoistnie podtrzymuje podstawowe ograniczenie MAC i że nie istnieje w nim kod naruszający to ograniczenie przez wykorzystanie kanałów ukrytych w złych zamiarach. (W istocie procesy uprzywilejowane dysponują znacznie większym arsenałem środków pozwalających naruszyć ograniczenie MAC, bez potrzeby odwoływania się do kanałów ukrytych). Prawdziwym problemem jest tu możliwość wykorzystania ukrytych kanałów przez procesy niezaufane, posługujące się w tym celu programem zaufanym.

Według ogólnej zasady kanały ukryte należy eliminować z systemu. Jednak są pewne przypadki, w których nieobecność kanałów ukrytych nakłada na system trudne do przyjęcia ograniczenia pod względem wydajności, niezawodności lub zgodności.

Wskazówki dotyczące przepustowości
System podstawowy korzysta z następujących wytycznych dla ukrytych kanałów bazujących na przepustowości:

Ponad 100 bit/s
Takie kanały nie mogą istnieć.

0,1 do 100 bit/s
Kanały w tym zakresie mogą istnieć, gdy jest to absolutnie konieczne, ale ich wykorzystanie jest wykrywane i kontrolowane przy każdej okazji.

Poniżej 0,1 bit/s
Kanały w tym zakresie mogą istnieć, ilekroć jest to konieczne, przy czym nie ma szczególnej potrzeby wykrywania ich użycia.

Zdecydowanie zaleca się, by wszystkie dodatkowe programy TCB przestrzegały tych samych wytycznych. Należy również wziąć pod uwagę, że nawet stosunkowo wolne kanały o przepustowości 10 bitów na sekundę pozwalają przesłać 4500 bajtów na godzinę, co daje znaczące ilości danych podlegające nieuprawnionemu obniżeniu poziomu bezpieczeństwa. Dlatego należy stosować wszelkie środki, by ograniczać przepustowość kanałów ukrytych do jak najmniejszych wartości.

Przepustowość większości kanałów ukrytych jest zwykle obniżana przez działania procesów innych niż te procesy, które mogą wykorzystywać kanał. Jednak zaleca się, by ograniczanie przepustowości kanałów ukrytych nie było uzależnione wyłącznie od tego efektu, ponieważ w każdym systemie zdarzają się okresy obniżonej aktywności.

Wykrywanie kanałów ukrytych
Wykrywanie kanałów ukrytych jest w dużej mierze kwestią uważnej analizy i projektowania. Jednak podczas wykrywania ukrytych kanałów warto skorzystać z kilku wskazówek.

Termin moduł odnosi się do wydzielonego fragmentu kodu TCB, który służy do wykrywania lub ograniczania użycia ukrytych kanałów w ramach jądra lub procesu. Wykrywanie kanałów ukrytych polega przeważnie na ustalaniu, czy niezaufany proces (nadawca) na poziomie A może wykorzystać moduł do wykonania czynności wykrywalnej przez inny proces (odbiorcę) na poziomie B, w sytuacji, gdy poziom B nie dominuje nad poziomem A.

Na przykład typowym kanałem ukrytym jest zapis danych w pliku przez proces zaufany w imieniu użytkownika niezaufanego, kiedy etykieta MAC pliku nie dominuje nad etykietą MAC użytkownika.

Arsenał metod opracowanych w celu wykrywania kanałów ukrytych jest stosunkowo ubogi. Najbardziej znamienną z nich jest macierz SRM (Shared Resource Matrix). Opis tej techniki można znaleźć w następujących pozycjach:

- • Kemmerer, R.A. "Shared Resource Matrix Methodology: An Approach to Identifying Storage and Timing Channels," ACM Transactions on Computing Systems 1(3) 1983, 256-277.
- • Tsai, CR. "A Formal Method for the Identification of Covert Storage Channels in Source Code", materiały z 1987 IEEE Symposium on Security and Privacy, 74-87.

Wykrywanie kanałów ukrytych przez kontrolę
Możliwość kontrolowania potencjalnego użycia kanałów ukrytych może być skutecznym sposobem zapobiegającym temu zagrożeniu. Jednak by kontrola spełniała swoje zadanie, zdarzenie kontroli musi występować dosyć rzadko. Kontrola jest mało użyteczna, jeśli stosunek liczby rzeczywistych przypadków wykorzystania kanału ukrytego do liczby wystąpień zdarzenia inicjującego kontrolę jest bardzo mały.

Ograniczanie efektywności kanałów ukrytych
Najlepszym sposobem ograniczenia efektywności kanałów ukrytych jest ich usunięcie.

Jeśli nie jest to możliwe, kanały te należy ograniczać w sposób opisany w temacie Wskazówki dotyczące przepustowości. Dodatkowo, gdy jest to możliwe i zasadne, potencjalne użycie kanałów należy objąć kontrolą.

Na ogół kod jądra i sterowników urządzeń ma trudności z ograniczaniem dostępu do kanałów ukrytych, ponieważ kod jądra i sterowników urządzeń jest optymalizowany pod kątem efektywności i używane przez nie kanały mają wyższą przepustowość. Ograniczanie efektywności kanałów ukrytych jest łatwiejsze z poziomu procesów zaufanych.

Uwaga: Nie ma uzasadnienia dla ograniczania dostępności kanałów ukrytych wobec procesów o tej samej etykiecie lub w sytuacjach, gdy proces odbierający dominuje nad procesem wysyłającym. Dlatego większość modułów TCB może zwiększyć wydajność systemu, nie nakładając żadnych ograniczeń w takich przypadkach.

Limity określane dla etykiet
Wiele kanałów ukrytych działa w oparciu o pulę zasobów współużytkowaną przez procesy o różnych etykietach MAC. Ich efektywność można skutecznie ograniczyć, tworząc oddzielne pule zasobów o stałym rozmiarze dla każdej etykiety MAC, dzięki czemu każdy proces może modulować użycie zasobów tylko należących do puli odpowiadającej jego etykiecie MAC.

Z czasem nieużywane zasoby mogą być przenoszone między pulami odpowiednio do dynamiki zapotrzebowania. Taka migracja zasobów sama w sobie stanowi kanał ukryty, jednak mający bardzo niską i łatwo ograniczaną przepustowość.

Opóźnienia
Jedną z technik ograniczania efektywności kanałów ukrytych jest takie skonfigurowanie TCB, aby przed wykonaniem usługi zawierającej kanały ukryte musiał zawsze upłynąć określony czas. Najprostszy sposób realizacji tego celu to nakazanie wprowadzania modułu w stan uśpienia na czas obliczany zależnie od ilości przekazywanych informacji.

Jednak opóźnienia wywoływane w niewprawny sposób mogą nie stanowić przeszkody dla programów wykorzystujących kanał ukryty. Na przykład procesy korzystające z kanału mogą tworzyć wiele zestawów procesów nadających i odbierających. Baza TCB może łatwo ograniczyć przepustowość dostępną dla każdego zestawu metodą opóźnień, jednak faktyczną przepustowość kanału będzie stanowić suma przepustowości dostępnych dla wszystkich zestawów.

Lepiej jest, gdy określona usługa TCB powoduje nakładanie w pewien sposób opóźnień na wszystkie procesy, które mogą korzystać z tej usługi.

Opóźnienia stanowią pewną barierę ochronną, jednak należy je stosować w dobrze przemyślany sposób, ponieważ mogą być stosunkowo łatwo ominięte przez programy napisane w złych zamiarach.

Ograniczenia dotyczące danych
Przepustowość kanału ukrytego można obniżać nie tylko przez wydłużanie czasu, lecz także przez zmniejszanie ilości zwracanych informacji. Programy zwracające dane w postaci serii operacji mogą często po prostu zwracać mniejsze pakiety informacji lub mniejszą ich liczbę w ciągu tego samego czasu.

Przybliżony czas
Wiele spośród technik wykorzystywania ukrytych kanałów wymaga, by czyniący to proces dysponował precyzyjną metodą pomiaru czasu względnego lub bezwzględnego. Dlatego efektywność takich kanałów można czasem ograniczyć, nie dopuszczając, by proces dokładnie ustalał czas.

Jakkolwiek stosunkowo łatwo można sprawić, że usługi TCB odpowiedzialne za odczyty czasu podawały go jako wartość przybliżoną, proces czasami dysponuje innymi metodami pomiaru upływu czasu, na przykład przez liczenie własnych czasów wykonywania instrukcji. Tego rodzaju techniki ograniczania efektywności kanałów należy stosować z ostrożnością.

Procesy zakłócające
Przepustowość większości kanałów ukrytych jest zazwyczaj obniżana, czasem bardzo radykalnie, przez działające procesy inne niż procesy korzystające z kanału. Istnieje możliwość, aczkolwiek nie jest to zalecane, tworzenia programów zaufanych, których celem jest nieprzerwane zapewnianie określonego poziomu aktywności. Są one czasem określane mianem procesów zakłócających.

Jakkolwiek użycie procesów zakłócających może wydawać się atrakcyjnym pomysłem, z reguły procesy te mają trudności z ustaleniem, kiedy powinny generować zakłócenia, a kiedy nie. Dlatego technika ta nie jest zalecanym sposobem ograniczania efektywności kanałów ukrytych.

Łańcuchy U-T-U
Możliwe są sytuacje, w których proces niezaufany **U1** wywołuje uprzywilejowany i zaufany proces **T**, który następnie wywołuje następny proces niezaufany **U2**, mający inną etykietę niż **U1**. **U1** i **U2** to niezaufane procesy o różnych etykietach MAC i mające szczególny potencjał tworzenia kanału ukrytego z uwagi na to, że jeden z nich jest potomkiem drugiego. (W istocie T i U mogą być całymi sekwencjami procesów zaufanych i niezaufanych). Sytuację taką nazywa się łańcuchem U-T-U.

Procesy zaufane muszą zapewniać mechanizmy zabezpieczające przed przepływem informacji między dwoma procesami niezaufanymi wbrew podstawowej zasadzie MAC. Obejmuje to zarówno wykluczanie niedozwolonych bezpośrednich operacji na danych, jak i eliminowanie użycia kanałów ukrytych. Należy przy tym uwzględnić następujące okoliczności:

- Deskryptory plików nie mogą pozostawać otwarte, jeśli proces **U2** nie mógł otworzyć danego pliku w obecnym trybie odczytu/zapisu.
- Należy wyzerować zmienne środowiskowe, jeśli etykieta **U2** nie dominuje nad etykietą U1.

- Katalog roboczy przekazywany z **U1** do **U2** może stanowić kanał ukryty (najpewniej o niewielkiej przepustowości), jeśli etykieta **U2** nie dominuje nad etykietą **U1**. Podobnie, wiele spośród parametrów automatycznie dziedziczonych przez proces potomny może udostępniać kanał ukryty.

Istnieje możliwość bezpiecznego zarządzania łańcuchami U-T-U (czyli odpowiedniego ograniczenia efektywności kanałów ukrytych). Jednak nie jest to zadanie łatwe, dlatego na ogół należy unikać powstawania łańcuchów U-T-U. Trzeba jednak podkreślić, że warunkiem zagrożenia jest to, by proces U2 był niezaufany. Może on natomiast z powodzeniem być zaufany, chociaż nieuprzywilejowany.

Przykłady ukrytych kanałów
Poniżej podano przykłady ukrytych kanałów, które mogą istnieć w modułach tworzonych przez programistę systemowego.

Przykład kanału ukrytego dla usługi wydruku
W tej sekcji przedstawiono przykład kanału ukrytego związanego z usługą wydruku.

Zaufana usługa drukarki wierszowej prawidłowo znakuje każde otrzymane zadanie etykietą MAC procesu zlecającego i utrwala tę etykietę razem z kolejkowanymi zadaniami aż do momentu wydruku. Dozwolone są stosunkowo długie nazwy zadań.

Program odczytujący status zadań umożliwia użytkownikowi przeglądanie wszystkich umieszczonych w kolejce zadań pochodzących od danego użytkownika, wraz z przypisywaną przez użytkownika nazwą, bez względu na etykietę zadania. Funkcjonalność ta może posłużyć jako kanał ukryty, ponieważ proces wysyłający może tworzyć zadania o nazwach zawierających dane przeznaczone do bezprawnego przekazania procesom odbierającym, które działają w imieniu tego samego użytkownika.

Uwaga: Jedyne kryterium decydujące o tym, że wykorzystano ukryty kanał, to warunek, by nadawca i odbiorca były procesami niezaufanymi oraz by etykieta odbiorcy nie dominowała nad etykietą nadawcy. Procesy nadawcy i odbiorcy zazwyczaj działają na koncie tego samego użytkownika.

Kanał ten można zamknąć, zezwalając użytkownikowi na przeglądanie tylko tych zadań, których etykieta jest dominowana przez bieżącą etykietę MAC użytkownika. Takie ograniczenie wymusza sytuację, w której etykieta MAC odbiorcy dominuje nad etykietą MAC nadawcy, skutkiem czego kanał można wykorzystać tylko do uprawnionego podniesienia poziomu zabezpieczeń danych. Dla wygody użytkownika program odczytujący status może go informować o istnieniu innych zadań, o etykietach niedominowanych. Stwarza to kanał o znacznie skromniejszych możliwościach i mający dobre uzasadnienie funkcjonalne.

Uwaga: Kontrolowanie i wykrywanie zadań wyższego poziomu może być użyteczne, ponieważ w normalnym działaniu zadania takie powinny występować rzadko.

Jest to typowy przykład kanału ukrytego, w którym nazwane obiekty danych o różnych poziomach (w tym przypadku: kolejkowane zadania wydruku) są dostępne dla procesów o innych etykietach MAC. Kanał można skutecznie wyeliminować, wymuszając rygory związane z etykietą MAC także wobec nazwy obiektu. Do nieuprawnionego przekazywania informacji mogą służyć także inne atrybuty niż nazwa, na przykład rozmiar.

Przykład z pulą zasobów
Kiedy program zaufany wykonuje usługę na rzecz niezaufanego klienta, program zaufany przydziela zasoby określonego typu (na przykład bufor) z puli zasobów współużytkowanej przez procesy z różnymi etykietami MAC.

Jednym ze sposobów wykorzystania tej techniki jako kanału ukrytego jest doprowadzenie przez procesy nadawcy i odbiorcy do sytuacji, w której przydzielone zostaną wszystkie zasoby oprócz jednego, na przykład innym programom działającym z użyciem innych etykiet MAC lub innych identyfikatorów użytkownika. Następnie nadawca doprowadza do przydzielenia lub nieprzydzielenia pojedynczego pozostałego zasobu, a odbiorca wykrywa ten fakt, również próbując przydzielić zasób.

Jest to typowy przykład kanału ze wspólnym zasobem. Jego efektywność można ograniczyć, przydzielając pule zasobów pod rygorem etykiety w sposób opisany powyżej. Kanał daje się także wykryć w wyniku kontroli.

Przykład z bazą danych
System zaufanej bazy danych pozwala programom użytkownika umieszczać dane w wielopoziomowej bazie danych. Dostęp bezpośredni jest odpowiednio kontrolowany za pośrednictwem podstawowych ograniczeń MAC.

Przy tym czas konieczny na umieszczenie wpisu w bazie danych w dużym stopniu zależy od jej bieżącej całkowitej wielkości. Dlatego nadawca może wprowadzać lub usuwać wpisy, aby wpłynąć na wielkość bazy danych, a odbiorca może po prostu mierzyć czas potrzebny do dokonania wpisu, aby tę wielkość ustalić. Ten kanał najczęściej ma stosunkowo niską przepustowość, chyba że dostęp do bazy danych jest realizowany z wysoką wydajnością.

Aby ograniczyć efektywność kanału, można nałożyć gwarantowany minimalny czas dostępu. Wielkość opóźnienia może być każdorazowo określana jako liczba pseudolosowa, aby zmniejszyć średnią długość czasu bezproduktywnego. Niemniej jednak, opisywana metoda wprowadza pewne opóźnienia i dlatego należy ją stosować z rozwagą.

Prosta kontrola wszystkich operacji dostępu może nie okazać się skuteczna, ponieważ przypadki wykorzystywania kanału ukrytego będą bardzo trudne do wykrycia wśród ogromnej liczby uprawnionych operacji na bazie danych.

Przykłady oprogramowania
W niniejszej sekcji przedstawiono kilka przykładów oprogramowania spełniającego kryteria programów zaufanych.

Przykład sprawdzania uprawnień przez program zaufany
Przedstawiono tu modułową procedurę, za pomocą której program zaufany może sprawdzić, czy proces wywołujący ma określone uprawnienie.

```
#include <sys/priv.h>
#include <sys/secattr.h>

int
priv_check (int priv)
{
  /* atrybuty zabezpieczeń procesu */
  secattr_t secattr;

/* odczytanie atrybutów zabezpieczeń procesu wywołującego */
  if ( sec_getpsec(-1, &secattr;) != 0 )
  {
    return (-1);
/* błąd podczas odczytu struktury cred procesu */
  }

  /*
   * wynik mówiący, czy określone uprawnienie należy
   * do maksymalnego zestawu uprawnień procesu wywołującego
   */
  return privbit_test(secattr.sc_maxpriv, priv);
}
```

Przykład zmiany etykiety czułości efektywnej (SL)
Ten program zmienia etykietę czułości efektywnej (SL) bieżącego procesu na wysoki systemowy.

Następujące uprawnienia są wymagane we własnym zestawie uprawnień programu:

- **PV_LAB_LEF**
- **PV_LAB_SLUG**
- **PV_LAB_SL_SELF**

```
#include <stdio.h>
#include <mls/mls.h>
#include <unistd.h>
#include <sys/secattr.h>
#include <userpriv.h>
#include <sys/mac.h>
#include <sys/secconf.h>

#define SUCCESS    0
```

```
#define ERROR    1

int
main()
{
    sl_t sl_syshi;    /* górna systemowa etykieta SL */
    secattr_t attr;
    char *clBuffer = NULL;

    /*
     * Odczyt górnych i dolnych systemowych etykiet SL.
     */
    if ((sec_getsyslab(NULL, &sl_syshi, NULL, NULL)) != 0 ) {
        fprintf (stderr, "Wywołanie sec_getsyslab nie powiodło się.\n");
        exit(ERROR);
    }

    /*
     * Inicjowanie procesu funkcją initlabeldb(), aby odczytać
     * domyślną systemową bazę danych etykiet.
     */
    priv_raise(PV_LAB_LEF , -1);
    if (initlabeldb(NULL) != 0) {
        fprintf(stderr, "Nie można odczytać bazy danych kodowania etykiet.\n");
        exit(ERROR);
    }
    priv_remove(PV_LAB_LEF, -1);

    /*
     * Odczytanie zakresu zezwoleń procesu i efektywnej etykiety SL.
     */
    priv_raise(PV_LAB_SLUG, PV_LAB_SL_SELF, -1);
    if (sec_getpsec(-1, &attr) != 0) {
        fprintf (stderr, "Problem przy odczytaniu atrybutów zabezpieczeń programu w systemie
Trusted AIX.\n");
        exit(ERROR);
    }

    /* malloc dla maksymalnej długości etykiety SL możliwej do utworzenia dla procesu */
    if((clBuffer = (char *) malloc(maxlen_cl())) == NULL) {
        perror("malloc");
        exit(ERROR);
    }
    /* Przekształcenie binarnej efektywnej SL do formy czytelnej */
    if (clbtohr(clBuffer, &attr.sc_sl, HR_LONG) != 0) {
        fprintf(stderr, "Nie można przekształcić etykiety SL do postaci czytelnej.\n");
        exit(ERROR);
    }
    printf("Początkowa efektywna etykieta SL programu = %s.\n",clBuffer);

    /*
     * Ustawienie efektywnej etykiety SL procesu na poziom górnej systemowej.
     * Maksymalna etykieta SL procesu może być inna niż górna systemowa,
     * więc także należy ją zmienić na górną systemową.
     */
    attr.sc_sl = sl_syshi;
    attr.sc_sl_cl_max = sl_syshi;

    if (sec_setplab(-1, &attr.sc_sl, NULL, &attr.sc_sl_cl_max,
            NULL, NULL, NULL) != 0) {
        fprintf (stderr, "Problem przy ustawianiu efektywnej etykiety SL programu.\n");
        exit(ERROR);
    }

    priv_lower(PV_LAB_SLUG, PV_LAB_SL_SELF, -1);

    if (sec_getpsec(-1, &attr) != 0) {
        fprintf (stderr, "Problem przy odczytaniu atrybutów zabezpieczeń programu w systemie
Trusted AIX.\n");
        exit(ERROR);
    }

    /* Przekształcenie binarnej efektywnej SL do formy czytelnej */
    if (clbtohr(clBuffer, &attr.sc_sl, HR_LONG) != 0) {
        fprintf(stderr, "Nie można przekształcić etykiety SL do postaci czytelnej.\n");
        exit(ERROR);
    }
    printf("Programowo zmieniona efektywna etykieta SL = %s.\n",clBuffer);
    return(SUCCESS);
}
```

Przykłady ustawiania klasyfikacji etykiet czułości i porównywania etykiet czułości
Przedstawiany przykład dotyczy ustawiania klasyfikacji etykiet czułości i wykorzystania procedur bibliotecznych do ich porównywania.

Uprawnienie **PV_LAB_LEF** jest wymagane w zestawie uprawnień delegowanych programu oraz w maksymalnym zestawie uprawnień procesu wywołującego.

```
#include <stdio.h>
#include <mls/mls.h>
#include <userpriv.h>
#include <errno.h>

#define SUCCESS    0
#define ERROR    1
int
main (int argc, char **argv)
{
/* Etykiety czułości  */
sl_t sl1, sl2;

/* łańcuchy do przechowywania nazw etykiet */
char *slBuffer1 = NULL;
char *slBuffer2 = NULL;

if (argc != 3) {
fprintf(stderr, "Składnia: compare etykieta1 etykieta2\n");
exit(ERROR);
}
/*
* Inicjowanie procesu funkcją initlabeldb(), aby odczytać
* domyślną systemową bazę danych etykiet.
*/
priv_raise(PV_LAB_LEF , -1);
if (initlabeldb(NULL) != 0) {
fprintf(stderr, "Nie można odczytać bazy danych kodowania etykiet.\n");
exit(ERROR);
}
priv_remove(PV_LAB_LEF, -1);

/* Konwersja przekazanej SL do formatu binarnego */
if (slhrtob(&sl1, argv[1]) != 0) {
fprintf(stderr, "Nie można przekształcić %s do formatu binarnego.\n", argv[1]);
exit(ERROR);
}
if (slhrtob(&sl2, argv[2]) != 0) {
fprintf(stderr, "Nie można przekształcić %s do formatu binarnego.\n", argv[2]);
exit(ERROR);
}

/* malloc dla maksymalnej długości etykiety SL możliwej do utworzenia */
slBuffer1 = (char *) malloc(maxlen_sl());
slBuffer2 = (char *) malloc(maxlen_sl());

if ((slBuffer1 == NULL) || (slBuffer2 == NULL)) {
perror("malloc");
exit(ERROR);
}

/*
* Tłumaczenie etykiety z powrotem do formatu czytelnego.
* Ten krok nie jest konieczny. Umieszczono go tu jako przykład
* użycia funkcji slbtohr().
*/
if (slbtohr(slBuffer1, &sl1, HR_LONG) != 0) {
fprintf(stderr, "Nie można przekształcić etykiety z postaci binarnej do czytelnej.\n");
exit(ERROR);
}

if (slbtohr(slBuffer2, &sl2, HR_LONG) != 0) {
fprintf(stderr, "Nie można przekształcić etykiety z postaci binarnej do czytelnej.\n");
exit(ERROR);
}

/*
* Użycie sl_cmp() do porównania dominacji obu etykiet.
*/
if (sl_cmp(&sl1, &sl2) == LAB_SAME) {
printf("etykieta (%s) jest równa etykiecie (%s).\n",
slBuffer1, slBuffer2);
```

```
    }
    else if (sl_cmp(&sl1, &sl2) == LAB_DOM) {
    printf("etykieta (%s) dominuje nad etykietą (%s).\n",
    slBuffer1, slBuffer2);
    }
    else if (sl_cmp(&sl2, &sl1) == LAB_DOM) {
    printf("etykieta (%s) dominuje nad etykietą (%s).\n",
    slBuffer2, slBuffer1);
    }
    else {
    printf("Obie etykiety są rozłączne.\n");
    }

    return (SUCCESS);
    }
```

Przykład z ustawianiem zapisów kontrolnych
Przedstawiony program odczytuje i ustawia zapisy kontrolne.

Następujące uprawnienia są wymagane we własnym zestawie uprawnień programu:

- **PV_AU_ADMIN**
- **PV_DAC_GID**

```
#include <sys/types.h>
#include <sys/priv.h>
#include <sys/audit.h>

char buf[1024];
int main(int argc, char *argv[])
{
    int rc, len, p;
    /* *Odczyt maski preselekcji kontroli procesu */
    priv_raise(PV_AU_ADMIN, -1);
    rc = auditproc(0, AUDIT_QEVENTS, buf, sizeof (buf));
    priv_lower(PV_AU_ADMIN, -1);
    if (rc)
        fprintf(stderr, "Nie powiodło się odczytanie danych kontroli\n");
           /* *Dodanie klasy kontroli jądra do maski preselekcji */
    p = 0;
    while ((len = strlen(&buf;[p])) > 0)
        p += len +1;
           strncat(&buf;[p], "jądro", (sizeof(buf)-p-1));
    p += strlen("jądro") + 2;
    buf[p] = 0;
    priv_raise(PV_AU_ADMIN, -1);
    rc = auditproc(0, AUDIT_EVENTS, buf, p);

    priv_lower(PV_AU_ADMIN, -1);
    if (rc)
        fprintf(stderr, "Nie powiodło się ustawienie danych kontroli\n");
    /* *Ustawienie GID procesu w celu wygenerowania zapisu kontroli */
    priv_raise(PV_DAC_GID, -1);
    rc = setgid(129);
    priv_lower(PV_DAC_GID, -1);
    if (rc)
        fprintf(stderr, "Nie powiodło się wywołanie setgid\n");
    exit(0);
}
```

Przykład klienta
Ten program przesyła na serwer dwa komunikaty: jeden przy użyciu standardowej procedury **write**, a drugi przy użyciu procedury **ewrite**.

Zabezpieczony komunikat jest przesyłany jako SECRET. Należy zauważyć, że niezabezpieczony komunikat wysyłany za pośrednictwem wywołania **write** otrzymuje domyślny zestaw atrybutów zabezpieczeń, które można konfigurować przy użyciu komendy netrule.

Następujące uprawnienia są wymagane we własnym zestawie uprawnień programu:

- **PV_LAB_LEF**
- **PV_MAC_CL**

- **PV_LAB_SLUG_STR**

```
#include  <sys/mac.h>
#include  <sys/socket.h>
#include  <netinet/in.h>
#include  <sys/priv.h>
#include  <sys/secattr.h>
#include  <errno.h>
#include  <stdio.h>
#define SECURE 1
int
main(int  argc,  char  *argv[])

{
    int  sockfd;
    int  uid,  gid;
    char  buf[BUFSIZ];

    struct  sockaddr_in  serv_addr;

#ifdef  SECURE
    int  l_init_result  =  0;

    int  ewrite_result  =  0;

    sec_labels_t  seclab;

#endif  /*SECURE*/


    uid  =  getuid();

    gid  =  getgid();


    if  (  argc  !=  3  )

    {
        fprintf(stderr,  "Składnia:%s:  ADDR  PORT\n",  argv[0]);

        exit(1);
    }
#ifdef  SECURE
    /*
     * *  Dostęp do bazy danych kodowania etykiet
     *
     *     */


    priv_raise(PV_LAB_LEF,-1);
    l_init_result  =  initlabeldb(NULL);
    if  (  priv_remove(PV_LAB_LEF,  -1)  !=  0  )
    {
        fprintf(stderr,  "Niepowodzenie podczas obsługi uprawnień\n");
        exit(1);
    }
    if  (  l_init_result  !=  0  )
    {
        fprintf(stderr,  "Nie można odczytać bazy danych kodowania etykiet\n");
        exit(0);
    }
#endif  /*SECURE*/
        /*
         * *  Wypełnij strukturę "serv_addr", podając
         * adres
         * *  serwera, z którym ma nastąpić połączenie.
         * */
    memset  ((char  *)  &serv_addr;,  '\0',  sizeof(serv_addr));
    serv_addr.sin_family  =  AF_INET;
    serv_addr.sin_addr.s_addr  =  inet_addr(argv[1]);
    serv_addr.sin_port  =  htons(atoi(argv[2]));
    /*  Otwarcie gniazda TCP  (gniazdo strumienia internetowego).  */
    if  (  (sockfd  =  socket(AF_INET,  SOCK_STREAM,  0))  <  0)
    {
        perror("tcpclient:  ");
        fprintf(stderr,  "klient:  Nie można otworzyć gniazda strumienia\n");
        exit(0);
    }
    if  (  connect(sockfd,  (struct  sockaddr  *)  &serv_addr;,
                sizeof(serv_addr))  <  0  )
    {
```

```
        perror("tcpclient:  ");
        fprintf(stderr,  "klient:  Nie można połączyć się z serwerem\n");
        exit(0);
    }
    /*
     * *  Wysłanie na serwer normalnego komunikatu write, który otrzyma
     * *  domyślne atrybuty zabezpieczeń
     * */
    strcpy(buf,  "Komunikat z domyślnymi atrybutami zabezpieczeń.\n");
    if  (  write(sockfd,  buf,  strlen(buf)+1)  ==  -1  )
    {
        perror("tcpclient:  ");
        fprintf(stderr,  "błąd zapisu\n");
    }
#ifdef  SECURE
        strcpy(buf,  "Ten komunikat ma status SECRET\n");
    /*  Konfiguracja SL i CL  */
    slhrtob(&seclab.sl;, "SECRET");
    slhrtob(&seclab.sl_cl_min;,  "SECRET");
    slhrtob(&seclab.sl_cl_max;,  "SECRET  A  B");
    seclab.sl.sl_format  =  STDSL_FORMAT;
    seclab.sl_cl_min.sl_format  =  STDSL_FORMAT;
    seclab.sl_cl_max.sl_format  =  STDSL_FORMAT;
    /*  To wywołanie ewrite  wymaga PV_MAC_CL  i PV_LAB_SLUG_STR  */
    priv_raise(PV_MAC_CL,PV_LAB_SLUG_STR,-1);
    ewrite_result  =  ewrite(sockfd,  buf,strlen(buf)+1,  &seclab;);
    priv_lower(PV_MAC_CL,PV_LAB_SLUG_STR,-1);

    if  (ewrite_result  ==  -1)
    {
        perror("wywołanie tcpclient");
        fprintf(stderr,  "błąd ewrite\n");
    }
    fflush(stderr);
#endif  /*SECURE*/
    fprintf(stderr,  "koniec   .....  \n");
    sleep(3);
    close(sockfd);
    exit(0);
}
```

Przykład z serwerem
Przedstawiony tu program działa jako serwer i korzysta z procedury **eread** do odbierania komunikatów wysyłanych do jego portu. Po pomyślnym odebraniu komunikatu program wyprowadza jego atrybuty zabezpieczeń.

Następujące uprawnienia są wymagane we własnym zestawie uprawnień programu (bez przypisywania opcji zabezpieczeń FSF_EPS):

- **PV_LAB_LEF**
- **PV_MAC_CL**
- **PV_MAC_R_STR**

```
#include  <sys/mac.h>
#include  <sys/socket.h>
#include  <sys/priv.h>
#include  <sys/secattr.h>
#include  <sys/stropts.h>
#include  <netinet/in.h>
#include  <errno.h>
#include  <stropts.h>
#include  <unistd.h>
#include  <stdio.h>
#include  <mls/mls.h>
#define  MAX_HR_LABEL_LEN 2048
#define  SECURE 1
int
main(int  argc,  char  *argv[])
{
    pid_t  childpid;
    uint  clilen;
    int  sockfd,  newsockfd;
    struct  sockaddr_in  cli_addr,  serv_addr;


#ifdef  SECURE
```

```
    int  l_init_result;
    char  label_str[MAX_HR_LABEL_LEN];
    sec_labels_t  seclab;
#endif  /*  SECURE  */
    if  (  argc  !=  2  )
    {
        fprintf(stderr,  "Składnia:%s  PORT\n",  argv[0]);
        exit(1);
    }
#ifdef  SECURE
    priv_raise(PV_LAB_LEF,  -1);
    l_init_result  =  initlabeldb(NULL);
    if  (priv_remove(PV_LAB_LEF,  -1)  !=  0)
    {
        fprintf(stderr,  "Niepowodzenie podczas obsługi uprawnień\n");
        exit(1);
    }

    if  (l_init_result  !=  0)
    {
        fprintf(stderr,  "Nie można odczytać bazy danych kodowania etykiet\n");
        exit(1);
    }
#endif  /*  SECURE  */
    /*  Otwarcie gniazda TCP  (gniazdo strumienia internetowego).  */
    if  (  (sockfd  =  socket(AF_INET,  SOCK_STREAM,  0))  <  0)
    {
        perror("tcpserver:  ");
        fprintf(stderr,  "serwer:  Nie można otworzyć gniazda strumienia\n");
        exit(1);
    }
    /*Powiązanie naszego lokalnego adresu, aby klient mógł do nas wysyłać*/
    memset((char  *)  &serv_addr;,  '\0',  sizeof(serv_addr));
    serv_addr.sin_family  =  AF_INET;
    serv_addr.sin_addr.s_addr  =  htonl(INADDR_ANY);
    serv_addr.sin_port  =  htons(atoi(argv[1]));
    if  (  bind(sockfd,  (struct  sockaddr  *)  &  serv_addr,
                sizeof(serv_addr))  <  0  )
    {
        perror("tcpserver:  ");
        fprintf(stderr,  "serwer:  Nie można powiązać lokalnego adresu\n");
        exit(0);
    }
    listen(sockfd,  5);
    for  (;;)
    {
        /*
         * *  Czekanie na połączenie z procesu klienta.
         * */
        fprintf(stdout,  "Oczekiwanie na połączenie z klienta\n");
        clilen  =  sizeof(cli_addr);
        newsockfd  =  eaccept(sockfd,  (struct  sockaddr  *)  &      cli_addr,
                &clilen;,  &seclab;);
        if  (  newsockfd  <  0  )
        {
            perror("tcpserver:  ");
            fprintf(stderr,  "serwer:  błąd akceptacji\n");
        }
        /*  Wydruk etykiety SL  */
        if  (  slbtohr(label_str,  &seclab.sl;,  HR_SHORT)  !=  0  )
        {
            fprintf(stderr,"problem podczas przekształcania etykiety SL w łańcuch\n");
        }
        else
        {
            fprintf(stdout,  "sl  =  %s.\n",label_str);
        }
        /*  Wydruk MIN  CLEARANCE  */
        if  (  slbtohr(label_str,  &seclab.sl_cl_min;,  HR_SHORT)  !=  0  )
        {
            fprintf(stderr,"problem podczas przekształcania zezwolenia min. w łańcuch\n");
        }
        else
        {
            fprintf(stdout,  "sl_cl_min  =  %s.\n",label_str);
        }

        /*  Wydruk MAX  CLEARANCE  */
        if  (  slbtohr(label_str,  &seclab.sl_cl_max;,  HR_SHORT)  !=  0  )
        {
            fprintf(stderr,"problem podczas przekształcania zezwolenia max. w łańcuch\n");
        }
```

```
        else
        {
            fprintf(stdout,  "sl_cl_max  =  %s.\n",label_str);
        }
        if  (  (childpid  =  fork())  <  0  )
        {
            perror("tcpserver:  ");
            fprintf(stderr,  "serwer: błąd rozwidlenia\n");
            exit(0);
        }
        else  if  (  childpid  ==  0  )  /*  proces potomny  */
        {
            int  i,  j;
            char  buf[BUFSIZ];
#ifdef  SECURE
        sec_labels_t  e_seclab;
#endif  /*  SECURE  */
        close(sockfd);
        for  (;;)
        {
            int  ret,  flag;
            struct  strbuf  ctstr,  dtstr;
            char  ctbuf[2048],  dtbuf[2048];
            ctstr.maxlen=2048;
            ctstr.buf  =  ctbuf;
            dtstr.maxlen=2048;
            dtstr.buf  =  dtbuf;
#ifdef  SECURE
            fprintf(stdout,  "Wywoływanie eread\n");
            priv_raise(PV_MAC_CL,PV_MAC_R_STR,-1);
            ret  =  eread(newsockfd,  buf,  sizeof(buf),&e_seclab;);
            priv_lower(PV_MAC_CL,PV_MAC_R_STR,-1);
            if  (  ret  <  1  )
           {
               if  (  ret  ==  -1  )
            fprintf(stderr,  "błąd eread\n");
               else
            fprintf(stderr,  "brak danych dla eread \n");
            close(newsockfd);
            exit(ret);
            }
            fprintf(stdout,  "\n%s",  buf);
            fprintf(stdout,  "\n");
            /*  Wydruk etykiety SL  */
            if  (  slbtohr(label_str,  &e_seclab.sl;,  HR_SHORT)  !=  0  )
            {
            fprintf(stderr,"problem podczas przekształcania etykiety SL w łańcuch\n");
             }
            else
            {
            fprintf(stdout,  "sl  =  %s.\n",label_str);
             }
             /*  Wydruk MIN  CLEARANCE  */
             if  (  slbtohr(label_str,&e_seclab.sl_cl_min;,HR_SHORT)!=  0)
            {
            fprintf(stderr,"problem podczas przekształcania min etykiety CL w łańcuch\n");
             }
            else
            {
            fprintf(stdout,  "sl_cl_min  =  %s.\n",label_str);
             }
             /*  Wydruk MAX  CLEARANCE  */
            if  (  slbtohr(label_str,&e_seclab.sl_cl_max;,HR_SHORT)  !=0)
            {
            fprintf(stderr,"problem podczas przekształcania max etykiety CL w łańcuch\n");
             }
             else
                    {
            fprintf(stdout,  "sl_cl_max  =  %s.\n",label_str);
              }
              fflush(stdout);
#else  /*  NOT  SECURE  */
              fprintf(stdout,  "Wywoływanie read\n");
              if  (read(newsockfd,  buf,  sizeof(buf))  <  1)
             {
            if  (ret  ==  -1)
               fprintf(stderr,  "błąd odczytu\n");
            else
               fprintf(stderr,  "brak danych do odczytu\n");
            close(newsockfd);
            exit(ret);
              }
```

```
              fprintf(stdout,  "%s\n",  buf);
              fflush(stdout);
#endif  /*  NOT  SECURE  */
                  }
    }
    /*  proces nadrzędny  */
    close(newsockfd);
        }
}
```

Atrybuty bezpieczeństwa użytkowników i portów w systemie Trusted AIX
Atrybuty bezpieczeństwa użytkowników i portów służą do odczytywania atrybutów zezwoleń użytkowników i portów i do porównywania atrybutów zezwolenia dla użytkownika z analogicznymi atrybutami portu.

Następujące atrybuty dodatkowe są zdefiniowane w pliku **usersec.h** w systemie Trusted AIX.

S_MINSL
Etykieta minimalnej czułości zezwolenia dla użytkownika. Typ: SEC_CHAR

S_MAXSL
Etykieta maksymalnej czułości zezwolenia dla użytkownika. Typ: SEC_CHAR

S_DEFSL
Etykieta domyślnej czułości dla użytkownika. Typ: SEC_CHAR

S_MINTL
Etykieta minimalnej integralności zezwolenia dla użytkownika. Typ: SEC_CHAR.

S_MAXTL
Etykieta maksymalnej integralności zezwolenia dla użytkownika. Typ: SEC_CHAR.

S_DEFTL
Etykieta domyślnej integralności dla użytkownika. Typ: SEC_CHAR

Następujące atrybuty mogą być używane w odniesieniu do portów.

S_MINSL
Etykieta minimalnej czułości do portu. Typ: SEC_CHAR.

S_MAXSL
Etykieta maksymalnej czułości przypisana do portu. Typ: SEC_CHAR

S_TL
Etykieta integralności przypisana do portu. Typ: SEC_CHAR

Następujący przykład pozwala ustalić, czy użytkownik może zalogować się na podanym porcie.

```
#include <mls/mls.h>
#include <usersec.h>
#include <stdio.h>
#include <errno.h>

   struct userlabels {
       sl_t minsl;
       sl_t maxsl;
       sl_t defsl;
       tl_t mintl;
       tl_t maxtl;
       tl_t deftl;
   };

   struct portlabels {
       sl_t minsl;
       sl_t maxsl;
       tl_t tl;
   };

   void getuserlabels(char * username, struct userlabels *usrlab);
   void getportlabels (char * portname, struct portlabels *portlab);
   void displayuseraccess (char * username, struct userlabels *usrlab,
                       struct portlabels *portlab);

   int
   main (int argc, char **argv)
```

```
{

    struct userlabels usrlab;
    struct portlabels portlab;
    char *username = NULL;
    char *portname = NULL;


    if (argc != 3 ) {
        fprintf (stderr, "Składnia: %s <nazwa_użytkownika> <nazwa_portu>\n", argv[0]);
        exit(1);
    }
    username = argv[1];
    portname = argv[2];

    initlabeldb(NULL);
    getuserlabels(username, &usrlab;);
    getportlabels(portname, &portlab;);
    displayuseraccess(username , &usrlab;, &portlab;);
    endlabeldb();
}

void getuserlabels(char *username,  struct userlabels *userlab)
{

    dbattr_t attributes[6];
    memset (attributes, 0, sizeof(attributes));

    attributes[0].attr_name = S_MINSL;
    attributes[0].attr_type = SEC_CHAR;

    attributes[1].attr_name = S_MAXSL;
    attributes[1].attr_type = SEC_CHAR;

    attributes[2].attr_name = S_DEFSL;
    attributes[2].attr_type = SEC_CHAR;

    attributes[3].attr_name = S_MINTL;
    attributes[3].attr_type = SEC_CHAR;

    attributes[4].attr_name = S_MAXTL;
    attributes[4].attr_type = SEC_CHAR;

    attributes[5].attr_name = S_DEFTL;
    attributes[5].attr_type = SEC_CHAR;

    if (getuserattrs(username, attributes, 6)) {
        fprintf(stderr,
                "Błąd podczas odczytu atrybutów dla użytkownika %s\n", username);
        exit (1);
    }

    if (clhrtob (&(userlab->minsl), attributes[0].attr_char)) {
        fprintf(stderr, "błąd konwersji minsl\n");
        exit (1);
    }

    if (clhrtob(&(userlab->maxsl), attributes[1].attr_char)) {
        fprintf(stderr, "błąd konwersji maxsl\n");
        exit (1);
    }

    if (clhrtob(&(userlab->defsl), attributes[2].attr_char)) {
        fprintf(stderr, "błąd konwersji defsl\n");
        exit (1);
    }

    if (tlhrtob(&(userlab->mintl), attributes[3].attr_char)) {
        fprintf(stderr, "błąd konwersji mintl\n");
        exit (1);
    }

    if (tlhrtob(&(userlab->maxtl), attributes[4].attr_char)) {
        fprintf(stderr, "błąd konwersji maxtl\n");
        exit (1);
    }

    if (tlhrtob(&(userlab->deftl), attributes[5].attr_char)) {
        fprintf(stderr, "błąd konwersji deftl\n");
        exit (1);
    }
```

```
        printf("Użytkownik %s ma następujące wartości zezwoleń\n", username);
        printf("minsl:%s\n", attributes[0].attr_char);
        printf("maxsl:%s\n", attributes[1].attr_char);
        printf("defsl:%s\n", attributes[2].attr_char);
        printf("mintl:%s\n", attributes[3].attr_char);
        printf("maxtl:%s\n", attributes[4].attr_char);
        printf("deftl:%s\n", attributes[5].attr_char);

        return;
    }

    void getportlabels(char *portname, struct portlabels *portlab)
    {
        int rc =0;
        char *val = NULL;
        if ( (rc = getportattr(portname,S_MINSL,(char*)&val;, SEC_CHAR)) != 0 ) {
            perror ("Błąd odczytu atrybutów portu");
            exit(1);
        }

        if (slhrtob(&(portlab->minsl), val)) {
            fprintf(stderr, "błąd konwersji minsl portu\n");
            exit (1);
        }

        if ( (rc = getportattr(portname,S_MAXSL, (char*)&val;, SEC_CHAR)) != 0 ) {
            perror ("Błąd odczytu atrybutów portu");
            exit(1);
        }

        if (slhrtob(&(portlab->maxsl), val)) {
            fprintf(stderr, "błąd odczytu maxsl portu\n");
            exit (1);
        }

        if ( (rc = getportattr(portname,S_TL, (char*)&val;, SEC_CHAR)) != 0 ) {
            perror ("Błąd odczytu atrybutów portu");
        }

        if (tlhrtob(&(portlab->tl), val)) {
            fprintf(stderr, "błąd konwersji tl portu\n");
            exit (1);
        }

        return;
    }

    void displayuseraccess (char *username, struct userlabels *usrlab, struct portlabels
*portlab)
    {
        CMP_RES_T cmpres;
        cmpres = sl_cmp(&(usrlab->defsl), &(portlab->minsl));
        if (cmpres != LAB_DOM && cmpres != LAB_SAME) {
            printf("Domyślna etykieta SL użytkownika nie dominuje nad minimalną etykietę SL tty
\n");
            exit(1);
        }

        cmpres = sl_cmp(&(portlab->maxsl), &(usrlab->defsl));
        if (cmpres != LAB_DOM && cmpres != LAB_SAME) {
            printf("Domyślna etykieta SL użytkownika nie jest dominowana przez maksymalną
etykietę SL tty\n");
            exit(1);
        }

        cmpres = tl_cmp(&(portlab->tl), &(usrlab->deftl));
        if (cmpres != LAB_SAME) {
            printf("Domyślna TL użytkownika nie jest identyczna z etykietą TL tty \n");
            exit(1);
        }

        printf("Użytkownik może logować się na podanym porcie\n");
        return;

}
```

Wywołania systemowe w modelu Trusted AIX

Wywołania systemowe są przeznaczone do operowania na dodatkowych funkcjach systemu Trusted AIX.

eaccept
Akceptuje połączenie na danym gnieździe.

ebind
Tworzy rozszerzone powiązanie w celu obsługi atrybutów bezpieczeństwa.

econnect
Inicjuje połączenie rozszerzone dla gniazda w celu obsługi atrybutów bezpieczeństwa.

eread
Odczytuje atrybuty bezpieczeństwa komunikatu ze strumienia.

ereadv
Odczytuje atrybuty bezpieczeństwa komunikatu ze strumienia.

erecv
Wykonuje rozszerzone operacje recv, recvfrom, recvmsg w celu obsługi atrybutów bezpieczeństwa.

erecvfrom
Wykonuje rozszerzone operacje recv, recvfrom, recvmsg w celu obsługi atrybutów bezpieczeństwa.

erecvmsg
Wykonuje rozszerzone operacje recv, recvfrom, recvmsg w celu obsługi atrybutów bezpieczeństwa.

esend
Wykonuje rozszerzone operacje send, sendto, sendmsg w celu obsługi atrybutów bezpieczeństwa.

esendmsg
Wykonuje rozszerzone operacje send, sendto, sendmsg w celu obsługi atrybutów bezpieczeństwa.

esendto
Wykonuje rozszerzone operacje send, sendto, sendmsg w celu obsługi atrybutów bezpieczeństwa.

ewrite
Wykonuje zapis w strumieniu i ustawia atrybuty bezpieczeństwa komunikatów.

ewritev
Wykonuje zapis w strumieniu i ustawia atrybuty bezpieczeństwa komunikatów.

sec_getmsgsec
Odczytuje atrybuty bezpieczeństwa kolejek komunikatów.

sec_getpsec
Odczytuje informacje zabezpieczeń skojarzone z procesem.

sec_getrunmode
Odczytuje tryb działania jądra.

sec_getsecconf
Zwraca bieżące opcje konfiguracji zabezpieczeń.

sec_getsemsec
Odczytuje atrybuty bezpieczeństwa semaforów.

sec_getshmsec
Odczytuje atrybuty bezpieczeństwa segmentów pamięci współużytkowanej.

sec_getsyslab
Odczytuje etykiety domyślnej czułości systemu.

sec_gettlibbufsize
Odczytuje wpisy ścieżek bibliotek w jądrze.

sec_gettlibpath
Odczytuje wpisy ścieżek bibliotek w jądrze.

pdmkdir
Tworzy/ustawia/usuwa katalog lub podkatalog partycjonowany.

sec_setauditrange
Ustawia zakres globalnej etykiety kontroli w systemie.

sec_setplab
Ustawia etykietę czułości efektywnej, etykietę czułości minimalnej zezwolenia, etykietę czułości maksymalnej zezwolenia oraz etykietę integralności podanego procesu.

setppdmode
Ustawia tryb katalogu partycjonowanego (rzeczywisty lub wirtualny) dla procesu.

setppriv
Ustawia zestaw uprawnień skojarzony z procesem.

sec_setptlibmode
Ustawia tryb TLIB procesu.

sec_setrunmode
Ustawia tryb działania jądra.

sec_setsecconf
Ustawia opcje konfiguracji zabezpieczeń jądra.

sec_setsemlab
Ustawia atrybuty bezpieczeństwa semaforów.

sec_setshmlab
Ustawia atrybuty bezpieczeństwa segmentów pamięci współużytkowanej.

sec_setsyslab
Ustawia domyślne etykiety czułości, informacji i integralności systemu.

Funkcje bibliotek C systemu AIX
Do obsługi dodatkowych funkcji systemu Trusted AIX przewidziano specjalne podprogramy i makra.

accredrange
Ustala, czy etykieta czułości znajduje się w zakresie akredytacji.

clbtohr
Przekształca podaną binarną etykietę zezwolenia do formatu czytelnego.

clhrtob
Przekształca podaną etykietę zezwolenia z formatu czytelnego do formatu binarnego.

getfsfbitindex, getfsfbitstring
Procedury pozwalające odczytać łańcuchy i indeksy opcji zabezpieczeń plików.

getmax_sl, getmax_tl
Odczytują etykiety maksymalnej czułości i integralności z pliku kodowania etykiet.

getmin_sl, getmin_tl
Odczytują etykiety minimalnej czułości i integralności z pliku kodowania etykiet.

getsecconfig, setsecconfig
Procedury odczytujące i ustawiające flagi konfiguracyjne bezpieczeństwa jądra dla poziomów pracy.

initlabeldb, endlabeldb
Procedury inicjowania i zakończenia bazy danych etykiet.

maxlen_sl, maxlen_cl, maxlen_tl
Odczytują maksymalną długość etykiet w formacie czytelnym z zainicjowanego pliku kodowania etykiet.

priv_isnull
Ustala, czy w danym zestawie uprawnień są ustawione pewne uprawnienia.

priv_lower
Operacje ustawiania uprawnień.

priv_raise
Operacje ustawiania uprawnień.

priv_remove
Operacje ustawiania uprawnień.

priv_subset
Operacje ustawiania uprawnień.

privbit_clr
Usuwa określone uprawnienie we wskazanym zestawie uprawnień.

priv_clrall
Usuwa wszystkie uprawnienia we wskazanym zestawie uprawnień.

priv_comb
Łączy dwa pierwsze wskazane zestawy uprawnień i umieszcza wynik w trzecim ze wskazanych zestawów uprawnień.

priv_copy
Kopiuje pierwszy ze wskazanych zestawów uprawnień do drugiego zestawu uprawnień.

priv_isnull
Ustala, czy w danym zestawie uprawnień nie są ustawione żadne uprawnienia.

priv_mask
Oblicza część wspólną dwóch pierwszych wskazanych zestawów uprawnień i umieszcza wynik w trzecim ze wskazanych zestawów uprawnień.

priv_rem
Usuwa uprawnienia zawarte w drugim z podanych zestawów uprawnień z pierwszego zestawu uprawnień, a wynik umieszcza w trzecim z podanych zestawów.

privbit_set
Ustawia podane uprawnienie we wskazanym zestawie uprawnień.

priv_setall
Ustawia wszystkie uprawnienia w podanym zestawie uprawnień.

priv_subset
Ustala, czy pierwszy z podanych zestawów uprawnień jest podzbiorem drugiego z podanych zestawów.

privbit_test
Sprawdza, czy podane uprawnienie jest ustawione w podanym zestawie uprawnień.

slbtohr, clbtohr, tlbtohr
Procedury konwersji etykiet binarnych do formatu czytelnego.

slhrtob, clhrtob, tlhrtob
Procedury konwersji etykiet z formatu czytelnego do binarnego.

sl_clr, tl_clr
Procedury resetowania etykiet

sl_cmp, tl_cmp
Procedury porównywania etykiet

tl_cmp
Porównanie etykiet integralności

Uprawnienia w systemie Trusted AIX
Poniżej podano uprawnienia dostępne w systemie Trusted AIX. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

Uprawnienia kontroli
Trusted AIX udostępnia podane poniżej uprawnienia kontroli. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_AU_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień **PV_AU_**.

PV_AU_ADD
Umożliwia procesowi zarejestrowanie lub dodanie rekordu kontroli.

PV_AU_ADMIN
Umożliwia procesowi skonfigurowanie systemu kontroli i wysyłanie do niego zapytań.

PV_AU_PROC
Umożliwia procesowi uzyskanie i ustawienie stanu kontroli procesu.

PV_AU_READ
Umożliwia procesowi odczytanie pliku oznaczonego jako plik kontroli.

PV_AU_WRITE
Umożliwia procesowi zapisanie lub usunięcie pliku oznaczonego jako plik kontroli albo oznaczenie pliku jako plik kontroli.

Uprawnienia autoryzacji
Trusted AIX udostępnia podane poniżej uprawnienia autoryzacji. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_AZ_ADMIN
Umożliwia procesowi modyfikowanie tabel zabezpieczeń jądra.

PV_AZ_READ
Umożliwia procesowi odtwarzanie tabel zabezpieczeń jądra.

PV_AZ_ROOT
Powoduje, że proces przechodzi sprawdzenia autoryzacji podczas wywołania systemowego **exec**.

PV_AZ_CHECK
Umożliwia procesowi przejście wszystkich sprawdzeń autoryzacji.

Uprawnienia DAC
Trusted AIX udostępnia podane poniżej uprawnienia DAC. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_DAC_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień PV_DAC_.

PV_DAC_O
Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących praw własności.

PV_DAC_R
Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących odczytu.

PV_DAC_W
Umożliwia procesowi przesłonięcie ograniczeń DAC dotyczących zapisu.

PV_DAC_X
Umożliwia procesowi przesłonięcie ograniczenia DAC dotyczącego wykonywania.

PV_DAC_UID
Umożliwia procesowi ustawienie lub zmianę jego identyfikatora użytkownika (UID).

PV_DAC_GID
Umożliwia procesowi ustawienie lub zmianę jego identyfikatora grupy (GID).

PV_DAC_RID
Umożliwia procesowi ustawienie lub zmianę jego identyfikatora roli (RID).

Uprawnienia systemu plików
Trusted AIX udostępnia podane poniżej uprawnienia systemu plików. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_FS_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień **PV_FS_**.

PV_FS_MKNOD
Umożliwia procesowi wykonanie wywołania systemowego **mknod** w celu utworzenia pliku dowolnego typu.

PV_FS_MOUNT
Umożliwia procesowi podłączanie i odłączanie systemu plików.

PV_FS_CHOWN
Umożliwia procesowi zmianę właściciela pliku.

PV_FS_QUOTA
Umożliwia procesowi zarządzanie informacjami powiązanymi z limitami pamięci dyskowej.

PV_FS_LINKDIR
Umożliwia procesowi utworzenie dowiązania stałego do katalogu.

PV_FS_RESIZE
Umożliwia procesowi wykonanie operacji rozszerzenia i zmniejszenia na systemie plików.

PV_FS_CNTL
Umożliwia procesowi wykonanie różnych operacji sterujących na systemach plików, oprócz operacji rozszerzenia i zmniejszenia.

PV_FS_CHROOT
Umożliwia procesowi zmianę własnego katalogu głównego.

PV_FS_PDMODE
Umożliwia procesowi utworzenie lub ustawienie katalogu partycjonowanego.

Uprawnienia procesu
Trusted AIX udostępnia podane poniżej uprawnienia procesu. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_PROC_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień **PV_PROC_**.

PV_PROC_PRIO
Umożliwia procesowi lub wątkowi zmianę priorytetu, strategii oraz innych parametrów planowania.

PV_PROC_CORE
Umożliwia procesowi wykonanie zrzutu pamięci.

PV_PROC_RAC
Umożliwia procesowi tworzenie większej liczby procesów, niż dopuszcza limit na użytkownika.

PV_PROC_RSET
Umożliwia dołączanie zestawu zasobów (**rset**) do procesu lub wątku.

PV_PROC_ENV
Umożliwia procesowi ustawienie informacji o użytkowniku w strukturze użytkowników.

PV_PROC_CKPT
Umożliwia procesowi wykonanie operacji checkpoint lub restartowania innego procesu.

PV_PROC_CRED
Umożliwia procesowi ustawienie uprawnienia procesu.

PV_PROC_SIG
Umożliwia procesowi wysyłanie sygnału do niepowiązanego procesu.

PV_PROC_PRIV
Umożliwia procesowi modyfikowanie lub wyświetlanie zestawów uprawnień powiązanych z procesem.

PV_PROC_TIMER
Umożliwia procesowi zgłaszanie i używanie liczników czasu o małej granulacji.

PV_PROC_RTCLK
Umożliwia procesowi dostęp do zegara procesora.

PV_PROC_VARS
Umożliwia procesowi pobieranie i aktualizowanie parametrów strojonych procesu.

PV_PROC_PDMODE
Umożliwia procesowi zmianę trybu REAL katalogu partycjonowanego.

Uprawnienia jądra
Trusted AIX udostępnia podane poniżej uprawnienia jądra. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_KER_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień **PV_KER_**.

PV_KER_ACCT
Umożliwia procesowi wykonanie ograniczonych operacji dotyczących podsystemu rozliczeniowego.

PV_KER_DR
Umożliwia procesowi wywoływanie dynamicznej rekonfiguracji.

PV_KER_TIME
Umożliwia procesowi zmodyfikowanie zegara i czasu systemowego.

PV_KER_RAC
Umożliwia procesowi użycie dużych (niestronicowanych) stron dla segmentów pamięci współużytkowanej.

PV_KER_WLM
Umożliwia procesowi zainicjowanie i zmodyfikowanie konfiguracji WLM.

PV_KER_EWLM
Umożliwia procesowi inicjowanie i wysyłanie zapytań do środowiska eWLM.

PV_KER_VARS
Umożliwia procesowi sprawdzenie lub ustawienie wykonawczych parametrów strojonych jądra.

PV_KER_REBOOT
Umożliwia procesowi zamknięcie systemu.

PV_KER_RAS
Umożliwia procesowi skonfigurowanie lub zapisanie rekordów RAS, rejestrowania błędów, śledzenia i funkcji zrzutu.

PV_KER_LVM
Umożliwia procesowi skonfigurowanie podsystemu LVM.

PV_KER_NFS
Umożliwia procesowi skonfigurowanie podsystemu NFS.

PV_KER_VMM
Umożliwia procesowi zmodyfikowanie parametrów stronicowania i innych parametrów strojonych VMM w jądrze.

PV_KER_WPAR
Umożliwia procesowi skonfigurowanie partycji zarządzania obciążeniem.

PV_KER_CONF
Umożliwia procesowi wykonanie różnych operacji konfigurowania systemu.

PV_KER_EXTCONF
Umożliwia procesowi wykonanie różnych zadań konfigurowania w rozszerzeniach jądra.

PV_KER_IPC
Umożliwia procesowi zwiększenie wartości buforu kolejki komunikatów IPC i przyłączenie wywołań systemowych **shmget** z zakresami.

PV_KER_IPC_R
Umożliwia procesowi odczytanie kolejki komunikatów IPC, zestawu semafora lub segmentu pamięci współużytkowanej.

PV_KER_IPC_W
Umożliwia procesowi zapisanie kolejki komunikatów IPC, zestawu semafora lub segmentu pamięci współużytkowanej.

PV_KER_IPC_O
Umożliwia procesowi odczytanie przesłonięcia prawa własności DAC we wszystkich obiektach IPC.

PV_KER_SECCONFIG
Umożliwia procesowi ustawianie opcji zabezpieczeń jądra.

PV_KER_PATCH
Umożliwia procesowi wprowadzenie poprawek do rozszerzeń jądra.

Uprawnienia etykiet
Trusted AIX udostępnia podane poniżej uprawnienia etykiet. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_LAB_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień etykiet (**PV_LAB_***).

PV_LAB_CL
Umożliwia procesowi modyfikowanie etykiet SCL podmiotu zgodnie z zezwoleniem procesu.

PV_LAB_CLTL
Umożliwia procesowi modyfikowanie etykiet SCL podmiotu zgodnie z zezwoleniem procesu.

PV_LAB_LEF
Umożliwia procesowi odczytanie bazy danych etykiet.

PV_LAB_SLDG
Umożliwia procesowi obniżanie etykiet SL zgodnie z zezwoleniem procesu.

PV_LAB_SLDG_STR
Umożliwia procesowi obniżanie etykiet SL pakietu zgodnie z zezwoleniem procesu.

PV_LAB_SL_FILE
Umożliwia procesowi zmianę etykiet SL obiektu zgodnie z zezwoleniem procesu.

PV_LAB_SL_PROC
Umożliwia procesowi zmianę etykiety SL podmiotu zgodnie z zezwoleniem procesu.

PV_LAB_SL_SELF
Umożliwia procesowi zmianę własnej etykiety SL zgodnie z zezwoleniem procesu.

PV_LAB_SLUG
Umożliwia procesowi podwyższanie etykiet SL zgodnie z zezwoleniem procesu.

PV_LAB_SLUG_STR
Umożliwia procesowi podwyższanie etykiety SL pakietu zgodnie z zezwoleniem procesu.

PV_LAB_TL
Umożliwia procesowi modyfikowanie etykiet TL podmiotu i obiektu.

Uprawnienia MAC
Trusted AIX udostępnia podane poniżej uprawnienia MAC. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_MAC_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień MAC (**PV_MAC_***).

PV_MAC_CL
Umożliwia procesowi ominięcie ograniczeń dotyczących kontroli czułości.

PV_MAC_R_PROC
Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC podczas odczytywania informacji o procesie, jeśli etykieta procesu docelowego jest w zakresie zezwoleń działającego procesu.

PV_MAC_W_PROC
Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC podczas wysyłania sygnału do procesu, jeśli etykieta procesu docelowego jest w zakresie zezwoleń działającego procesu.

PV_MAC_R
Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC.

PV_MAC_R_CL
Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC, gdy etykieta obiektu jest w zakresie zezwoleń procesu.

PV_MAC_R_STR
Umożliwia procesowi ominięcie ograniczeń dotyczących odczytu MAC podczas odczytu komunikatu ze strumienia, jeśli etykieta komunikatu jest w zakresie zezwoleń procesu.

PV_MAC_W
Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC.

PV_MAC_W_CL
Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, gdy etykieta obiektu jest w zakresie zezwoleń procesu.

PV_MAC_W_DN
Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, gdy etykieta procesu dominuje nad etykietą obiektu, a etykieta obiektu jest w zakresie zezwoleń procesu.

PV_MAC_W_UP
Umożliwia procesowi ominięcie ograniczeń dotyczących zapisu MAC, kiedy etykieta procesu jest zdominowana przez etykietę obiektu, a etykieta obiektu jest w zakresie zezwoleń procesu.

PV_MAC_OVRRD
Ominięcie ograniczeń dotyczących MAC w przypadku plików oznakowanych jako wyłączone z MAC.

Uprawnienia MIC
Trusted AIX udostępnia podane poniżej uprawnienia MIC. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_MIC
Umożliwia procesowi ominięcie ograniczeń dotyczących integralności.

PV_MIC_CL
Umożliwia procesowi ominięcie ograniczeń dotyczących kontroli integralności.

Uprawnienia dotyczące sieci
Trusted AIX udostępnia podane poniżej uprawnienia dotyczące sieci. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_NET_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień dotyczących sieci (**PV_NET_***).

PV_NET_CNTL
Umożliwia procesowi modyfikowanie tabel sieciowych.

PV_NET_PORT
Umożliwia procesowi przypisanie zastrzeżonego portu.

PV_NET_RAWSOCK
Umożliwia procesowi bezpośredni dostęp do warstwy sieciowej.

PV_NET_CONFIG
Umożliwia procesowi konfigurowanie parametrów sieciowych.

Uprawnienia administratora
Trusted AIX udostępnia podane poniżej uprawnienia administratora. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_SU_
Odpowiednik wszystkich pozostałych razem wziętych uprawnień administratora (**PV_SU_***).

PV_SU_ROOT
Nadaje procesowi odpowiednik wszystkich uprawnień powiązanych ze standardowym administratorem.

PV_SU_EMUL
Nadaje procesowi odpowiednik wszystkich uprawnień powiązanych ze standardowym administratorem, gdy numer UID procesu ma wartość 0.

PV_SU_UID
Powoduje, że wywołanie systemowe **getuid** zwraca wartość 0.

Inne uprawnienia
Trusted AIX udostępnia podane poniżej inne uprawnienia. Udostępniono streszczenie i opis każdego uprawnienia oraz sposób jego użycia. Niektóre uprawnienia tworzą hierarchię, w której jedno uprawnienie może nadać wszystkie prawa powiązane z innym uprawnieniem.

Sprawdzając uprawnienia, system najpierw określa, czy proces ma najniższe wymagane uprawnienie, a następnie przechodzi na wyższe poziomy hierarchii, sprawdzając istnienie silniejszych uprawnień. Na przykład proces z uprawnieniem **PV_AU_** ma automatycznie uprawnienia **PV_AU_ADMIN**, **PV_AU_ADD**, **PV_AU_PROC**, **PV_AU_READ** i **PV_AU_WRITE**, a proces z uprawnieniem **PV_ROOT** ma automatycznie wszystkie uprawnienia podane poniżej, oprócz uprawnienia **PV_SU_**.

PV_ROOT
Nadaje procesowi uprawnienia będące odpowiednikiem wszystkich pozostałych uprawnień, oprócz **PV_SU_** (i uprawnień zdominowanych przez **PV_SU_**).

PV_TCB
Umożliwia procesowi modyfikację ścieżek biblioteki zaufanej jądra.

PV_TP
Wskazuje, że proces jest procesem zaufanej ścieżki i umożliwia wykonywanie działań zastrzeżonych dla procesów zaufanej ścieżki.

PV_TP_SET
Umożliwia procesowi ustawianie i usuwanie opcji ścieżki zaufanej dla jądra.

PV_WPAR_CKPT
Umożliwia procesowi wykonanie operacji na punkcie kontrolnym i restartowania w partycjach zarządzania obciążeniem.

PV_DEV_CONFIG
Umożliwia procesowi konfigurowanie systemowych rozszerzeń jądra i urządzeń.

PV_DEV_LOAD
Umożliwia procesowi ładowanie i usuwanie z pamięci rozszerzeń jądra i urządzeń w systemie.

PV_DEV_QUERY
Umożliwia procesowi wysyłanie zapytań do modułów jądra.

Rozwiązywanie problemów dotyczących systemu Trusted AIX

Zamieszczone odpowiedzi na często zadawane pytania mogą pomóc podczas rozwiązywania problemów dotyczących systemu Trusted AIX.

Jak zalogować się w systemie Trusted AIX?

System Trusted AIX podczas instalacji tworzy trzech użytkowników administracyjnych z odpowiednimi rolami podanymi poniżej.

Hasła dla tych kont należy ustawić podczas pierwszego startu systemu Trusted AIX po zainstalowaniu. Jeśli system został zainstalowany z sieci w trybie bez zapytań, należy użyć haseł do tych kont domyślnych, które podano poniżej.

Użytkownik	**Hasło**
isso	isso
sa	sa
so	so

Jak wykonać komendę su, aby przełączyć się na użytkownika `root`?

Podczas instalacji systemu Trusted AIX atrybut **su** użytkownika `root` jest ustawiany na wartość **false**, przez co nikt nie może uzyskać dostępu do tego konta. Aby uzyskać dostęp do tego konta, użytkownicy administracyjni isso i sa będą musieli zmienić ten atrybut konta użytkownika root na wartość **true**, używając komendy **chuser**.

Jeśli dla komendy **su** włączono obsługę użytkownika root i hasło konta root nie jest ustawione, to każdy użytkownik w systemie może uzyskać dostęp do tego konta użytkownika root. Aby tego uniknąć, zaleca się, aby hasło konta użytkownika root zostało ustawione przed zresetowaniem atrybutu **su**.

Czy mam utworzyć własnych użytkowników administracyjnych, czy też użyć domyślnych?

Domyślni użytkownicy administracyjni są przeznaczeni wyłącznie do konfigurowania systemu podczas dostosowywania. Zdecydowanie zaleca się, chociaż nie jest to niezbędne, aby te konta były używane wyłącznie podczas dostosowywania systemu.

Utwórz tych trzech własnych użytkowników administracyjnych z odpowiednimi rolami isso, sa i so, a następnie usuń lub wyłącz tych trzech użytkowników domyślnych.

Dlaczego nie mogę zalogować się w systemie?

Podczas próby zalogowania się jako użytkownik root (konto o numerze UID równym 0) lub jako inny użytkownik, którego numer UID konta jest mniejszy niż 128, nastąpi odmowa dostępu. Te konta są nazywane kontami systemowymi. Aby uzyskać dostęp do kont systemowych, należy zalogować się jako użytkownik konta niesystemowego i wykonać operację **su** dla żądanego konta.

Czy podczas logowania wyświetlane są jakiekolwiek błędy dotyczące pliku kodowania etykiet?

Jeśli plik kodowania etykiet jest uszkodzony, należy przejść do trybu pojedynczego użytkownika jako użytkownik root. Konto użytkownika root jest dostępne tylko w trybie pojedynczego użytkownika.

Sprawdź, czy plik kodowania etykiet (`/etc/security/enc/LabelEncodings`) jest właściwy, używając komendy **labck**. Jeśli ten plik jest niewłaściwy, zmodyfikuj go i dokonaj ponownego sprawdzenia za pomocą komendy **labck** przed wyjściem z trybu pojedynczego użytkownika.

Uruchom komendę **trustchk** w trybie interaktywnym (**trustchk -t ALL**), aby sprawdzić poprawność stanu systemu.

Dlaczego nie mogę skompilować żadnego programu w systemie Trusted AIX używającego bibliotecznych funkcji API systemu Trusted AIX?

Pakiet narzędzi programisty nie jest instalowany domyślnie. Należy zainstalować zestaw plików `bos.mls.adt` z nośnika instalacyjnego.

Jak poprawić zmiany wprowadzone w uprawnieniach komend, które spowodowały, że te komendy przestały poprawnie działać?

Aby poprawić uprawnienia, dla tych komend uruchom komendę **trustchk** w trybie interaktywnym (**trustchk -t**).

Dlaczego nie mam dostępu do katalogu `/etc/security/enc`?

Aby uzyskać dostęp do katalogu `/etc/security/enc`, powłoka musi mieć uprawnienia PV_LAB_LEF i PV_MAC_R. Przypisz te uprawnienia do swojej powłoki.

Jak wyłączyć uruchamianie komendy `trustchk` podczas startu.
Usuń lub przekształć w komentarz wiersz z komendą `trustchk` znajdujący się w skrypcie `/etc/rc.mls`.

Jak skonfigurować system, aby nie wyświetlał zachęty do uwierzytelniania podczas każdego startu?
Dla systemu włączono uwierzytelnianie podczas startu. Można je wyłączyć, używając menu SMIT z podmenu systemu Trusted AIX.

Dlaczego wprowadzona zmiana nie odnosi skutku, gdy próbuję zmienić etykietę SL obiektu systemu plików?
Istnieje kilka możliwości:

Czy komenda `/usr/sbin/settxattr` zwróciła jakieś komunikaty o błędach?
Jeśli tak, przeczytaj je, aby uzyskać więcej informacji. Na przykład:

Czy masz uprawnienia do wykonania komendy `/usr/sbin/settxattr`?
Jeśli nie, sprawdź uprawnienia i autoryzacje.

Czy składnia była poprawna?
Aby sprawdzić składnię, skorzystaj ze strony podręcznika komendy **settxattr**.

Czy istnieje żądana etykieta SL lub jej skrót?
Zażądanie `"con a b"` będzie działało w systemie z domyślnym plikiem kodowania etykiet (`/etc/security/enc/LabelEncodings`), ale zażądanie `"conf a b"` nie będzie działało, chociaż wydaje się, że oba ustawienia są logicznymi skrótami tekstu "confidential compartment A compartment B".

Czy trzeba używać cudzysłowu dla etykiety zawierającej wiele słów?
Wykonanie komendy `settxattr -f sl=con <nazwa_pliku>` zadziała. Wykonanie komendy `settxattr -f -a sl="con a b" <nazwa_pliku>` też zadziała, ale wykonanie komendy `settxattr -a sl=con a b <nazwa_pliku>` nie zadziała.

Czy komenda `settxattr` zwróciła komunikaty o błędach?
Jeśli nie zostały zwrócone żadne komunikaty o błędach, obiekt systemu plików może być dowiązaniem symbolicznym. Jeśli obiekt, który próbowano zmienić, jest dowiązaniem symbolicznym, najpierw określ, czy chcesz zmienić etykietę SL dowiązania, czy też obiektu wskazywanego przez to dowiązanie. Komenda **settxattr** nie śledzi dowiązań, ale ustawia etykiety samego dowiązania.

Jak zainstalować aplikację innej firmy, aby działała poprawnie w systemie?
Jeśli zainstalowano aplikację innej firmy i nie działa ona poprawnie, być może próbuje ona uzyskać dostęp do zastrzeżonych plików lub katalogów, które wymagają dodatkowych uprawnień. Po oszacowaniu konieczności uzyskania dostępu do tych zastrzeżonych obiektów przez aplikację należy określić potrzebne uprawnienia zgodnie z następującymi wskazówkami:

- przypisz PV_ROOT do używanej powłoki,
- uruchom komendę `tracepriv -f -e <komenda_innej_firmy>`.

Zostaną wyświetlone uprawnienia wymagane przez tę aplikację. Dodaj je do bazy danych uprawnionych komend za pomocą komendy **setsecattr**.

Dlaczego nie mogę wykonać niektórych komend?
Ponieważ większość komend jest zabezpieczona za pomocą autoryzacji, wykonanie niektórych uprawnionych komend będzie dozwolone tylko wtedy, gdy użytkownik wywołujący ma odpowiednie autoryzacje. Można to sprawdzić, określając, czy autoryzacja wymagana do wykonania komendy istnieje w jednej z ról aktywowanych dla bieżącej sesji.

Posiadane autoryzacje aktywne można sprawdzić za pomocą komendy `rolelist -ae`, a autoryzacje wymagane przez komendę można sprawdzić za pomocą komendy `lssecattr -c <komenda>`.

Dlaczego niektóre komendy nie wyświetlają etykiet poprawnie?
Większość tych komend bazuje na pliku `/etc/security/enc/LabelEncodings` podczas konwersji etykiet do formatu czytelnego i odwrotnie. Jeśli ten plik jest uszkodzony lub został zmodyfikowany, te komendy mogą nie działać zgodnie z zamierzeniem.

Opcje bezpieczeństwa pliku

Opcje bezpieczeństwa pliku decydują o sposobach dostępu do plików. Opcje te są przechowywane jako część atrybutów rozszerzonych samego pliku. Miejscem definicji opcji bezpieczeństwa pliku jest nagłówek pliku.

FSF_APPEND
Do pliku można tylko dopisywać dane, nie można go modyfikować w trybie wykonawczym.

FSF_AUDIT
Plik jest oznaczony jako element podsystemu kontroli. Odczyt lub zapis do pliku wymaga od procesu odpowiednio uprawnień **PV_AU_READ** lub **PV_AU_WRITE**.

FSF_MAC_EXMPT
EPS z uprawnieniem **PV_MAC_OVRRD** ignoruje ograniczenia MAC podczas prób dostępu do obiektu.

FSF_PDIR
Katalog jest katalogiem partycjonowanym.

FSF_PSDIR
Katalog jest podkatalogiem partycjonowanym.

FSF_PSSDIR
Katalog jest pod-podkatalogiem partycjonowanym.

FSF_TLIB
Obiekt jest oznaczony jako część biblioteki zaufanej (Trusted Library). Komputer musi działać w trybie konfiguracji lub opcja bezpieczeństwa jądra **trustedlib_enabled** musi być wyłączona (OFF).

FSF_TLIB_PROC
Procesy oznaczone jako TLIB mogą dowiązywać tylko biblioteki oto ***.so** z ustawioną opcją **TLIB**. System musi działać w trybie konfiguracji lub opcja bezpieczeństwa jądra **trustedlib_enabled** musi być wyłączona (OFF).

Komendy systemu Trusted AIX

Do zarządzania systemem Trusted AIX udostępniono komendy dotyczące bezpieczeństwa:

labck
Sprawdza plik LabelEncodings.

getsecconf
Wyświetla flagi bezpieczeństwa jądra.

setsecconf
Zmienia flagi bezpieczeństwa jądra systemu Trusted AIX.

getsyslab
Wyświetla minimalną i maksymalną etykietę jądra.

setsyslab
Ustawia minimalną i maksymalną etykietę jądra.

getrunmode
Wyświetla bieżący tryb działania systemu.

setrunmode
Przełącza tryb działania systemu.

pdlink
Tworzy dowiązania między plikami w podkatalogach partycjonowanych.

pdmkdir
Tworzy katalogi i podkatalogi partycjonowane.

pdmode
Zwraca bieżący tryb dostępu katalogu partycjonowanego lub uruchamia komendę z podanym trybem dostępu katalogu partycjonowanego.

pdrmdir
Usuwa katalogi partycjonowane i powiązane z nimi podkatalogi.

pdset
Ustawia/anuluje ustawienie katalogów i podkatalogów partycjonowanych.

bootauth
Sprawdza, czy system jest startowany przez autoryzowanego użytkownika.

chuser
Zmienia atrybuty zezwoleń użytkownika.

lsuser
Wyświetla atrybuty zezwoleń użytkownika.

chsec
Zmienia atrybuty zezwoleń użytkownika i etykiety portów.

lssec
Wyświetla atrybuty zezwoleń użytkownika i etykiety portów.

trustchk
Sprawdza atrybuty plików.

lstxattr
Wyświetla etykietę i atrybuty flag bezpieczeństwa plików, procesów i obiektów IPC.

settxattr
Zmienia etykietę i atrybuty flag bezpieczeństwa plików, procesów i obiektów IPC.

Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju/regionie można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi IBM. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi, pochodzących od producenta innego niż IBM, spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie tego dokumentu nie daje żadnych uprawnień licencyjnych do tychże patentów. Zapytania dotyczące licencji można wysłać na piśmie na adres:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
Stany Zjednoczone

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japonia

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE ("AS IS"), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszym dokumencie mogą zawierać nieścisłości techniczne lub błędy drukarskie. Podane w niej informacje są okresowo aktualizowane; zmiany te zostaną ujęte w jej kolejnych wydaniach. Firma IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Informacje na temat możliwości stosowania tego programu, takie jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym programem) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
Stany Zjednoczone

Informacje takie mogą być udostępniane na odpowiednich warunkach, w niektórych przypadkach za opłatą.

Licencjonowany program opisany w tym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Dane o wydajności i przytoczone przykłady klientów mają charakter wyłącznie ilustracyjny. Rzeczywiste wyniki wydajności mogą być inne w zależności od konkretnych konfiguracji i warunków działania.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są sugerowanymi cenami detalicznymi; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiekolwiek podobieństwo do rzeczywistych osób lub firm jest całkowicie przypadkowe.

LICENCJA NA PRAWA AUTORSKIE:

Publikacja ta zawiera przykładowe aplikacje w kodzie źródłowym, które ilustrują techniki programowania na różnych platformach systemowych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM, w celu projektowania, używania, sprzedaży lub w celu rozpowszechniania aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować ani sugerować niezawodności, użyteczności czy funkcjonalności tych programów. Programy przykładowe są dostarczane w stanie, w jakim się znajdują ("AS IS"), bez udzielania jakichkolwiek gwarancji. IBM nie ponosi odpowiedzialności za żadne szkody wynikłe z użycia programów przykładowych.

Każdy egzemplarz i fragmenty programów przykładowych oraz jakichkolwiek prac pochodnych muszą zawierać następujące uwagi dotyczące praw autorskich:

© (nazwa przedsiębiorstwa użytkownika) (rok).

Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp.

© Copyright IBM Corp. _wpisać rok lub lata_.

Zagadnienia dotyczące strategii prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem", może korzystać z informacji cookie lub z innych technologii do gromadzenia danych o używaniu produktów, do poprawienia jakości usług dla użytkowników końcowych, do dopasowania

interakcji do ich oczekiwań oraz do innych celów. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji pozwalających na identyfikację osoby. Część Oferowanego Oprogramowania może jednak umożliwiać gromadzenie informacji pozwalających na identyfikację osoby. Jeśli Oferowane Oprogramowanie korzysta z informacji cookie do gromadzenia informacji pozwalających na identyfikację osoby, poniżej znajdują się szczegółowe informacje na temat takiego korzystania.

To Oferowane Oprogramowanie nie używa informacji cookie ani innych technologii do gromadzenia informacji pozwalających na identyfikację osoby.

Jeśli konfiguracje Oferowanego Oprogramowania umożliwiają gromadzenie informacji pozwalających na identyfikację użytkowników końcowych za pośrednictwem informacji cookie lub innych technologii, należy wystąpić o poradę prawną w zakresie prawa obowiązującego przy takim gromadzeniu danych, w tym wymagań dotyczących powiadomienia i zgody.

Więcej informacji na temat korzystania z różnych technologii, w tym z informacji cookie, do opisanych wyżej celów znajduje się w sekcji Ochrona prywatności w IBM pod adresem http://www.ibm.com/privacy oraz Oświadczenie IBM o Ochronie Prywatności w Internecie, pod adresem http://www.ibm.com/privacy/details, a także w sekcji zatytułowanej "Cookies, Web Beacons and Other Technologies" oraz "IBM Software Products and Software-as-a-Service Privacy Statement", pod adresem http://www.ibm.com/software/info/product-privacy.

Znaki towarowe

IBM, logo IBM i ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corp. w wielu krajach świata. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych firm. Aktualna lista znaków towarowych IBM jest dostępna w serwisie WWW Copyright and trademark information (Informacje o prawach autorskich i znakach towarowych) pod adresem www.ibm.com/legal/copytrade.shtml.

Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa w Stanach Zjednoczonych i w innych krajach.

Microsoft i Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Java i wszystkie znaki towarowe i logo związane z językiem Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.

Indeks

Znaki specjalne

A

B

C

D

F

G

H

I

K

L

M

N

O

P

R

S

Ś

T

U

V

W

X

Z