IBM Systems Lab Services

Enhanced Role Based Access Control

Overview

AIX Enhanced Role Based Access Control (RBAC) is a powerful and sophisticated access control tool for AIX. Many UNIX security breaches occur because of excessive access to root. One of the most important ways to protect your AIX environment is to lessen unnecessary root access. RBAC provides a rich set of tools for allowing administrators to gain the access they need to do their jobs without having to grant root access. RBAC is also important for many companies to implement to satisfy regulatory security requirements.

Technical Details

- RBAC adoption enables superior auditing configuration options
- 3rd party scripts and executable files can be configured as RBAC commands
- RBAC deployment can be centrally managed by using a RFC2307AIX compatible LDAP Server
- Domain RBAC can be added to your RBAC implementation to provide extra access control options

Common Use Cases

- An AIX organization that would like to reduce unnecessary root access to mitigate security risk
- An AIX administrative team that would like to learn how to configure RBAC
- An AIX organization that would like to implement AIX administrative separation of duties
- An AIX Organization that would like to fulfill security requirements for implementing detailed logging of security events on AIX
- An organization that would like to use the access control features in RBAB that are not possible with sudo

Engagement Process

- Consultant arranges prep call to discuss requirements, scheduling, and agenda
- Consultant works with client to configure RBAC in client proof-of-concept environment
- Consultant provides advice on best practice implementation
- Consultant works with client to verify the RBAC functions that are most important to the client
- Consultant provides presentations to facilitate knowledge transfer

Deliverables

1. Presentation Slides – an electronic copy of presentation slides
2. Configuration documents – an electronic copy of configuration documents