



System i
Telnet en red

Versión 6 Release 1





System i
Telnet en red
Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en: "Avisos", en la página 109.

Esta edición atañe a la versión 6, release 1, modificación 0 de IBM i5/OS (producto número 5761-SS1) y a todos los releases y modificaciones subsiguientes hasta que se indique lo contrario en nuevas ediciones. Esta versión no funciona en todos los modelos RISC (reduced instruction set computer) ni tampoco en los modelos CISC.

© Copyright International Business Machines Corporation 1998, 2008. Reservados todos los derechos.

Contenido

Telnet	1
Archivo PDF de Telnet	1
Casos prácticos de Telnet	1
Caso práctico de Telnet: configuración del servidor Telnet.	2
Caso práctico de Telnet: sesiones Telnet en cascada	4
Casos prácticos de proceso de las peticiones del sistema	5
Utilización de un trabajo de grupo	7
Caso práctico de Telnet: protección de Telnet con SSL	9
Detalles de configuración para proteger Telnet con SSL.	11
Planificación del servidor Telnet	15
Descripciones de dispositivos virtuales	15
Seguridad de Telnet	16
Cómo impedir el acceso mediante Telnet	16
Control del acceso mediante Telnet	17
Configuración del servidor Telnet	21
Inicio del servidor Telnet	21
Establecimiento del número de dispositivos virtuales	22
Configuración automática de dispositivos virtuales	22
Creación de dispositivos virtuales propios	23
Restricción de usuarios privilegiados a dispositivos específicos y limitación del número de intentos de inicio de sesión	24
Establecimiento del parámetro de tiempo de vida de la sesión	25
Asignación de dispositivos a subsistemas	26
Activación del subsistema QSYSWRK	26
Creación de perfiles de usuario.	26
Tipos de emulación soportados por i5/OS	27
Configuración del servidor Telnet para la modalidad de pantalla completa 5250	27
Configuración del servidor Telnet para la modalidad de pantalla completa 3270	27
Tipos de terminal 3270 soportados.	29
Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx	30
Protección de Telnet con SSL	33
Configuración de SSL en el servidor Telnet	33
Eliminación de restricciones de puerto	34
Asignación de un certificado al servidor Telnet	34
Habilitación de la autenticación de clientes para el servidor Telnet.	36
Habilitación de SSL en el servidor Telnet	38
Inicialización y negociación de SSL	38
Gestión del servidor Telnet	39
Configuración de sesiones de impresora Telnet	40
Requisitos para las sesiones de impresora Telnet	41

Soporte de impresión del servidor Telnet para el cliente System i Access para Windows Telnet	41
Finalización de la sesión del servidor Telnet	42
Finalización de trabajos del gestor de dispositivos	42
Utilización de programas de punto de salida de Telnet	43
Programa de salida de inicialización de dispositivos	44
Formato de punto de salida de Telnet	
INIT0100: grupo de parámetros necesarios	45
INIT0100: Formato de la información de descripción del usuario	46
INIT0100: Formato de la información de descripción del dispositivo	47
INIT0100: Formato de la información de descripción de la conexión	49
Programa de salida de finalización de dispositivos	51
Ejemplos: programas de salida de Telnet.	51
Gestión del cliente Telnet.	52
Control de las funciones de servidor Telnet desde el cliente	53
Sesiones de cliente Telnet 5250	54
Inicio de una sesión de cliente Telnet.	54
Sesiones de cliente Telnet 3270	56
Inicio de una sesión de cliente Telnet 3270	56
Consideraciones sobre la pantalla completa 3270	57
Utilización de una estación de pantalla	59
Correlación de teclado 3270 para servidores Telnet	60
Sesiones de cliente VTxxx.	62
Inicio de una sesión de cliente Telnet VTxxx	62
Consideraciones sobre la modalidad de pantalla completa VTxxx	63
Opciones de emulación de VTxxx	68
Valores de las teclas VTxxx	69
Soporte de idioma nacional de VTxxx	75
Modalidad nacional de VTxxx	76
Teclado numérico	78
Teclado de edición	80
Valores de las teclas VTxxx por función 5250.	82
Modalidades operativas de la estación de trabajo VT220.	86
Teclas de función de la fila superior de VT220	87
Palabras clave de caracteres de control de VT100 y VT220	88
Establecimiento de una sesión Telnet en cascada	89
Paso de una sesión Telnet en cascada a otra	90
Finalización de una sesión de cliente Telnet.	91
Resolución de problemas de Telnet	91
Determinación de problemas con Telnet	91

Emisión de un mandato Ping al servidor de hospedaje	94	Material necesario para informar de problemas de Telnet	105
Resolución de problemas relacionados con los tipos de emulación	95	Información de diagnóstico generada automáticamente	106
Resolución de problemas del servidor Telnet SSL	98	Información relacionada con Telnet	107
Comprobación del estado del sistema.	98		
Comprobación de la existencia de un escucha SSL activo	99	Apéndice. Avisos.	109
Comprobación de las anotaciones de trabajo de Telnet	99	Información sobre la interfaz de programación	110
Códigos de retorno de SSL	100	Marcas registradas.	110
Salidas del programa de servicio TRCTCPAPP	102	Términos y condiciones	111

Telnet

Telnet es un protocolo que permite conectarse a un sistema remoto y utilizarlo como si se estuviera conectado directamente a él dentro de la red local.

El sistema (normalmente un PC) ante el que se encuentra físicamente es el cliente Telnet. El servidor Telnet es el sistema remoto al que se conecta el cliente. TCP/IP soporta tanto el cliente como el servidor Telnet.

Una de las funciones más importantes de Telnet es su capacidad de negociar la transmisión de corrientes de datos entre el cliente y el servidor Telnet. Este tipo de negociación hace posible que tanto el cliente como el servidor inicien o acepten una petición.

- | Dispone de varios tipos distintos de emulación para la negociación de peticiones y su conversión en salida. En Telnet, el tipo preferido es la emulación 5250. Telnet también admite las estaciones de trabajo de tipo 3270 y VTxxx, así como las modalidades de soporte de impresora Request for Comments (RFC) 4777 (TN5250E). Este tema incluye una introducción a Telnet y proporciona información sobre la administración de Telnet en el sistema.

Nota: al utilizar los ejemplos de código, acepta los términos de la “Información sobre licencia de código y exención de responsabilidad” en la página 108.

Archivo PDF de Telnet

Puede ver e imprimir un archivo PDF de esta información.

Para ver o descargar la versión PDF de este documento, seleccione Telnet (aproximadamente 1300 KB).

Cómo guardar los archivos PDF

Si desea guardar un archivo PDF en su estación de trabajo para verlo o imprimirlo:

1. Pulse con el botón derecho del ratón el enlace PDF en el navegador.
2. Pulse la opción que guarda el PDF localmente.
3. Navegue hasta el directorio en el que desea guardar el PDF.
4. Pulse **Guardar**.

Cómo descargar Adobe Reader

Para poder ver o imprimir archivos PDF, debe instalar Adobe Reader en su sistema. Puede descargar una copia gratuita desde el sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Referencia relacionada

“Información relacionada con Telnet” en la página 107

Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas de Telnet. Puede ver o imprimir los archivos PDF que desee.

Casos prácticos de Telnet

Los casos prácticos proporcionan ejemplos de utilización de Telnet a modo de introducción de los principales conceptos y las tareas de configuración básicas.

Caso práctico de Telnet: configuración del servidor Telnet

En este caso práctico se describe cómo configura un administrador un servidor Telnet, incluidos los objetivos, los requisitos previos y los supuestos, así como los detalles de configuración.

Situación

Ken Harrison es el administrador de un nuevo entorno i5/OS de la compañía ficticia Culver Pharmaceuticals.

Objetivos

Tiene que configurar el servidor Telnet de modo que cumpla las especificaciones siguientes:

- Permitir que se creen automáticamente hasta 100 dispositivos virtuales.
- Mostrar siempre la ventana de inicio de sesión.
- Restringir usuarios privilegiados a dispositivos específicos.
- Limitar cada usuario a una sesión de dispositivo.

Prerrequisitos y supuestos

En este caso práctico se supone lo siguiente:

- Culver Pharmaceuticals ejecuta el sistema operativo i5/OS.
- TCP/IP está configurado.
- Ken Harrison tiene la autorización *IOSYSCFG.

Detalles de configuración

Siga estos pasos para configurar el servidor Telnet en System i Navigator.

1. Inicie el servidor Telnet:
 - a. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. En el panel de la derecha, en la columna Nombre de servidor, busque **Telnet**.
 - c. Confirme que en la columna Estado aparece **Iniciado**.
 - d. Si el servidor no está en ejecución, pulse **Telnet** con el botón derecho del ratón y seleccione **Iniciar**.
2. Establezca el número de dispositivos virtuales:
 - a. Seleccione *su sistema* → **Configuración y servicio** → **Valores del sistema**.
 - b. En el panel de la derecha, pulse **Dispositivos** con el botón derecho del ratón y seleccione **Propiedades**.
 - c. En la página Valores del sistema de dispositivos, habilite **Dispositivos de paso a través y TELNET** y establezca el valor de **Número máximo de dispositivos** en 100.
3. Configure las propiedades del servidor Telnet:
 - a. Seleccione *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. En el panel de la derecha, pulse **Telnet** con el botón derecho del ratón y seleccione **Propiedades**.

Tabla 1. Valores de las propiedades de Telnet

Pulse esta pestaña...	Y...
Inicio de sesión del sistema	Seleccione: <ul style="list-style-type: none">• Restringir usuarios privilegiados a dispositivos específicos.• Limitar cada usuario a una sesión de dispositivo.

Tabla 1. Valores de las propiedades de Telnet (continuación)

Pulse esta pestaña...	Y...
Inicio de sesión remoto	Especifique el número de intentos de inicio de sesión permitidos y la acción que debe llevarse a cabo si se alcanza el número máximo de intentos de inicio de sesión.
Remoto	Seleccione la opción Visualizar siempre pantalla de inicio de sesión en Utilizar Telnet para inicio de sesión remoto .
Tiempo de espera	Especifique la acción que debe llevarse a cabo cuando los trabajos alcancen un valor de tiempo de espera. También puede especificar cuánto tiempo se concede a una operación antes de que el trabajo exceda el tiempo de espera. Puede especificar información tanto para los trabajos inactivos como para los trabajos desconectados.

Nota: estos valores son válidos para todos los trabajos y dispositivos interactivos del sistema, no solo para Telnet.

4. Asigne dispositivos a los subsistemas.

En la interfaz basada en caracteres, escriba:

ADDWSE SBS(DQINTER) WRKSTNTYPE(*ALL)

5. Active el subsistema QSYSWRK:

Compruebe el estado del subsistema QSYSWRK:

- a. En la interfaz basada en caracteres, escriba WRKSBS (Trabajar con subsistemas).
- b. Verifique que se visualizan los sistemas siguientes:
 - QSYSWRK
 - QINTER
 - QSPL

Si el subsistema QSYSWRK no está activo, siga estos pasos:

- a. En la interfaz basada en caracteres, escriba STRSBS (Arrancar subsistema).
- b. Escriba **QSYSWRK** para la descripción de subsistema y **QSYS** para la biblioteca; a continuación, pulse **Intro**.
- c. Repita la acción para el valor de nombre de subsistema **QINTER** con la biblioteca **QSYS**, y el valor de nombre de subsistema **QSPL** con la biblioteca **QSYS**.

6. Cree perfiles de usuario Telnet:

- a. Inicie System i Navigator y expanda *su sistema*.
- b. Pulse **Usuarios y grupos** con el botón derecho del ratón y seleccione **Usuario nuevo**.
- c. Escriba el nombre, la descripción y la contraseña del usuario.
- d. Para especificar una descripción de trabajo, pulse **Trabajos** y escriba la descripción del trabajo.
- e. Pulse **Aceptar**.

7. Verifique que Telnet funciona.

Ken inicia una sesión de emulación 5250 y se conecta al servidor Telnet.

Conceptos relacionados

“Tipos de emulación soportados por i5/OS” en la página 27

La emulación preferida para el sistema es la emulación 5250. No obstante, el sistema también da soporte a la emulación 3270 y VTxxx.

Tareas relacionadas

“Configuración del servidor Telnet” en la página 21

Este tema contiene información sobre cómo llevar a cabo la configuración del servidor Telnet para varios tipos de emulación.

Caso práctico de Telnet: sesiones Telnet en cascada

El caso práctico muestra la posibilidad de iniciar sesiones Telnet mientras todavía se está en una sesión Telnet. Una vez conectado, puede pasar de un sistema a otro utilizando los valores de petición del sistema.

En este caso práctico, la usuaria establece sesiones Telnet con varios servidores. Esto se denomina una *sesión Telnet en cascada*. Con este método, podrá:

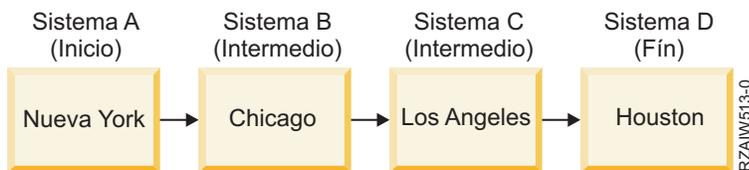
- Establecer sesiones Telnet entre la oficina central y Chicago.
- Conectar con servidores Telnet adicionales sin finalizar la sesión inicial.
- Pasar de una sesión a otra para volver a un trabajo del sistema de Nueva York.

Situación

Janice Lowe es la directora de marketing de Culver Pharmaceuticals. Se conecta desde la oficina de Nueva York y accede al sistema principal de Chicago mediante Telnet. Después de establecer una sesión de cliente con el servidor Telnet en Chicago, se da cuenta de que necesita trabajar con algunos archivos de la oficina de Los Ángeles.

Objetivos

Janice Lowe utiliza el cliente Telnet de Chicago para conectarse al servidor Telnet de Los Ángeles. Mientras está conectada a Los Ángeles, decide establecer una sesión con Houston.



Esta figura muestra las conexiones que establece Janice Lowe. El sistema desde el que inicia el trabajo en Nueva York se denomina sistema inicial. Desde ahí se conecta al sistema intermedio B de Chicago y, a continuación, se conecta al sistema intermedio C de Los Ángeles, que se conecta al sistema final D de Houston.

Prerrequisitos y supuestos

En este caso práctico se supone lo siguiente:

- El servidor Telnet está en ejecución en todos los sistemas.
- Janice Lowe tiene un inicio de sesión en todos los sistemas.
- Todos los sistemas ejecutan i5/OS o superior.

Detalles de configuración

Janice Lowe lleva a cabo los pasos siguientes para conectar con los servidores Telnet:

1. En el sistema de Nueva York, escriba STRTCPTLN CHICAGO.
2. En el sistema de Chicago, escriba STRTCPTLN LA.
3. En el sistema de Los Ángeles, escriba STRTCPTLN HOUSTON.

Una vez que se ha conectado al sistema de Houston, desea llevar a cabo una tarea en el sistema de Nueva York (inicial).

1. Pulse la tecla **Petición de sistema**.
2. Seleccione la opción 14 (Transferir a sistema inicial). De este modo se le devolverá al trabajo alternativo en el sistema de Nueva York.

Una vez que ha terminado el trabajo en el sistema de Nueva York, puede volver al sistema de Houston realizando estas tareas:

1. Pulse la tecla **Petición de sistema**.
2. Seleccione la opción 15 (Transferir a sistema final). De este modo pasará de un sistema intermedio o inicial al sistema final.

Para finalizar todas las sesiones, utiliza el mandato SIGNOFF. Este mandato finaliza la sesión actual y se devuelve a Janice Lowe a la pantalla de inicio de sesión del sistema inicial.

Referencia relacionada

“Establecimiento de una sesión Telnet en cascada” en la página 89

Puede establecer otra sesión Telnet mientras está en una sesión Telnet actual. Una vez establecida una sesión en cascada, puede moverse entre los distintos sistemas.

“Paso de una sesión Telnet en cascada a otra” en la página 90

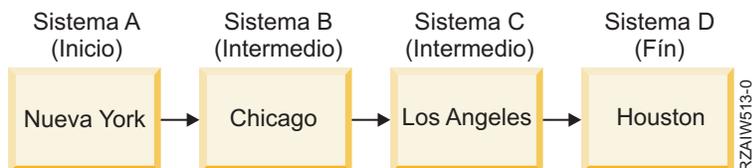
Una vez que haya iniciado una sesión Telnet en cascada, pulse la tecla Pet Sis y pulse Intro para visualizar el menú Petición Sistema.

Casos prácticos de proceso de las peticiones del sistema

Los casos prácticos describen cómo funciona el proceso de las peticiones del sistema con varios tipos de sistemas.

Caso práctico 1

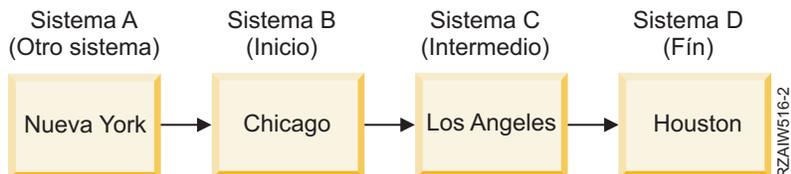
La imagen muestra la siguiente configuración: el sistema inicial A de Nueva York se conecta al sistema intermedio B de Chicago, que se conecta al sistema intermedio C de Los Ángeles, que a su vez se conecta al sistema final D de Houston.



Caso práctico 2

El sistema de Nueva York utiliza Telnet 3270 o VTxxx. Es un sistema distinto de System i.

La imagen muestra la siguiente configuración: el sistema A de Nueva York se conecta al sistema inicial B de Chicago, que se conecta al sistema intermedio C de Los Ángeles, que a su vez se conecta al sistema final D de Houston.

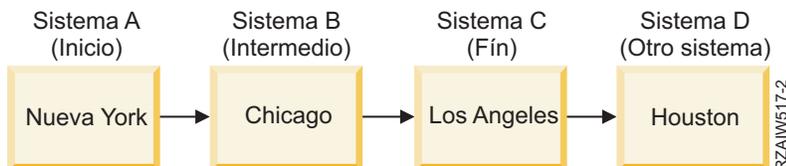


El proceso de las peticiones del sistema funciona igual que en el primer caso práctico con la excepción de que Chicago se considera el sistema inicial. Todas las peticiones del sistema enviadas al sistema inicial se procesan en el sistema de Chicago.

Caso práctico 3

El sistema de Houston utiliza Telnet 3270 o VTxxx. Es un sistema distinto de System i.

La imagen muestra la siguiente configuración: el sistema inicial A de Nueva York se conecta al sistema intermedio B de Chicago, que se conecta al sistema intermedio C de Los Ángeles, que a su vez se conecta al sistema final D de Houston.



El proceso de las peticiones del sistema funciona igual que en el primer caso práctico con la excepción de que Los Ángeles se considera el sistema final para todo el proceso de peticiones del sistema. Si pulsa la tecla Petición de sistema y a continuación pulsa la tecla Intro, se visualiza el menú Petición Sistema para Los Ángeles.

Caso práctico 4

El sistema de Los ángeles utiliza Telnet 3270 o VTxxx. Es un sistema distinto de System i.

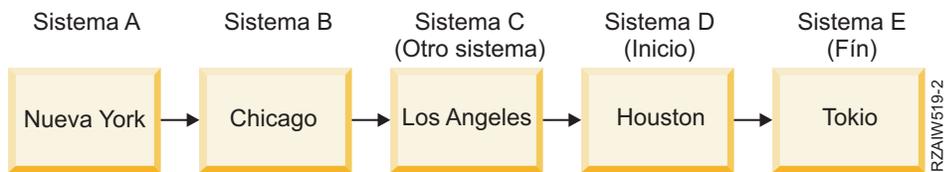
El sistema inicial A de Nueva York se conecta al sistema final B de Chicago, que se conecta al sistema C de Los Ángeles, que se conecta al sistema inicial D de Houston, que se conecta al sistema final E de Tokio.



El proceso de las peticiones del sistema funciona igual que en el primer caso práctico con la excepción de que Chicago se considera el sistema final para el proceso de peticiones del sistema. Si pulsa la tecla Petición de sistema y a continuación pulsa la tecla Intro, se visualiza el menú Petición Sistema para Chicago.

Si desea enviar una petición del sistema al sistema de Tokio, puede correlacionar una tecla de función en el sistema de Houston con la tecla Petición de sistema. Si correlaciona esta función, el sistema de Tokio será el sistema final y Houston será el sistema inicial.

La imagen muestra la siguiente configuración: el sistema A de Nueva York se conecta al sistema B de Chicago, que se conecta al sistema C de Los Ángeles, que se conecta al sistema inicial D de Houston, que se conecta al sistema final E de Tokio.



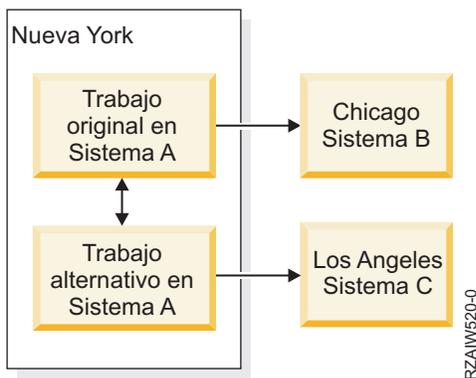
A modo de ejemplo de esta función de correlación para un servidor Telnet 3270, la correlación de teclado predeterminada identifica la tecla Petición de sistema como una tecla 3270 PF11. Para un cliente Telnet 3270, la tecla F11 se correlaciona con la tecla 3270 PF11. Si el sistema de Los Ángeles utiliza la corriente de datos 3270, al pulsar F11 se correlaciona el sistema de Los Ángeles con la tecla Petición de sistema del sistema de Houston. La petición del sistema se transmite al sistema de Tokio y se visualiza el menú Petición Sistema para el sistema de Tokio.

Nota: esta función de correlación es compleja, especialmente si se utiliza la corriente de datos VTxxx y se establece la correlación entre datos de bloques y datos de tipo carácter.

Utilización de un trabajo de grupo

Estos ejemplos contienen información sobre cómo utilizar Telnet, trabajos alternativos y trabajos de grupo para trabajar con varios sistemas.

Puede utilizar Telnet y el trabajo alternativo para conectarse a varios sistemas desde el sistema inicial; considere el ejemplo siguiente:



Telnet establece una sesión de Nueva York a Chicago. También desea ir al sistema de Los Ángeles y permanecer conectado al sistema de Chicago. Puede iniciar un trabajo alternativo en el sistema de Nueva York, utilizando la opción 11 de Petición Sistema. Utilice el mandato Telnet para establecer una sesión con el sistema de Los Ángeles. Puede acceder a otro sistema (por ejemplo, Houston) iniciando otra sesión Telnet desde el sistema de Chicago o desde el sistema de Los Ángeles.

En lugar de emplear el trabajo alternativo puede utilizar un trabajo de grupo. Un trabajo de grupo es uno de hasta 16 trabajos interactivos que están asociados en un grupo con el mismo usuario y dispositivo de estación de trabajo. Para configurar un trabajo de grupo, siga estos pasos:

1. Cambie el trabajo actual por un trabajo de grupo mediante el mandato de cambiar atributos del grupo (CHGGRPA).
CHGGRPA GRPJOB(home)
2. Inicie un trabajo de grupo para el sistema de Chicago mediante el mandato de transferir a trabajo de grupo (TFRGRPJOB).
TFRGRPJOB GRPJOB(CHICAGO) INLGRPPGM(QCMD)
3. Establezca una sesión Telnet con el sistema de Chicago.
Telnet CHICAGO

4. Vuelva al sistema inicial pulsando la tecla Atenc. Al pulsar la tecla Atenc se muestra el menú Enviar Funciones de Control TELNET.
5. En la interfaz basada en caracteres del menú Enviar Funciones de Control Telnet, escriba:
TFRGRPJOB GRPJOB(home)
Esta acción le devuelve al trabajo original.

Puede iniciar otros trabajos de grupo y sesiones Telnet de forma parecida.

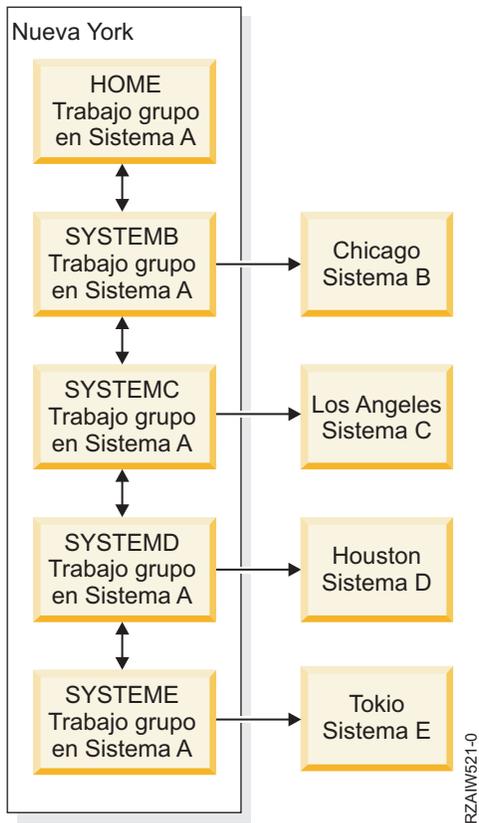
Puede utilizar el mandato TFRGRPJOB GRPJOB(*SELECT) para seleccionar el trabajo de grupo que desea. Por ejemplo, si se inician los trabajos de grupo denominados CHICAGO, LOSANGELES, HOUSTON y TOKYO, el mandato TFRGRPJOB GRPJOB(*SELECT) muestra la pantalla siguiente:

```

                Transferir a trabajo de grupo
Sistema: SYS198
Trabajo de grupo activo . . : HOME
Texto . . . . . :
Escriba una opción y pulse Intro.
    1=Transferir a trabajo de grupo
-----Trabajos de grupo suspendidos-----
Opc Trabajo de grupo  Texto
-      TOKYO
-      HOUSTON
-      LOSANGELES
-      CHICAGO
Final  F3=Salir F5=Renovar F6=Iniciar un trabajo de grupo nuevo F12=Cancelar

```

A continuación puede utilizar Telnet para establecer una sesión con cada sistema desde el trabajo adecuado. El ejemplo siguiente muestra un caso práctico de trabajo de grupo:



El sistema A de Nueva York contiene el trabajo de grupo inicial en el sistema A, con flechas bidireccionales que conectan en sentido descendente a lo largo de una cadena con los elementos siguientes en este orden: trabajo de grupo del sistema B en el sistema A, trabajo de grupo del sistema C en el sistema A, trabajo de grupo del sistema D en el sistema A y trabajo de grupo del sistema E en el sistema A. Cada trabajo de grupo del sistema en el sistema A tiene una flecha que apunta al sistema remoto correlativo (B, C, D y E).

Cuando desee finalizar el trabajo de grupo, utilice el mandato de finalizar trabajo de grupo (ENDGRPJOB).

Para cambiar a otro trabajo de grupo mientras se encuentra en una sesión Telnet:

1. Pulse la tecla Atenc.
2. Escriba TFRGRPJOB en la interfaz basada en caracteres.

Caso práctico de Telnet: protección de Telnet con SSL

En este ejemplo de configuración se describe cómo puede utilizar la Capa de sockets seguros (SSL) para proteger Telnet en el sistema.

Situación

Bob está en el proceso de crear un negocio de intermediación financiera con sede en su domicilio particular. Se ha jubilado de su puesto de agente de bolsa de una importante empresa y desea seguir ofreciendo servicios de intermediación financiera a un pequeño número de clientes desde su domicilio. Lleva el negocio en un pequeño sistema, que desea utilizar para proporcionar acceso a las cuentas a sus clientes, mediante sesiones Telnet 5250. En estos momentos Bob se plantea cómo ofrecer a los clientes un acceso continuo a sus cuentas para que puedan gestionar sus acciones. Bob quiere que sus clientes utilicen sesiones Telnet 5250 para acceder a las cuentas, pero le preocupa la seguridad del servidor, así como la seguridad de las sesiones de los clientes. Tras investigar las opciones de seguridad Telnet, Bob decide emplear SSL (capa de sockets seguros) para garantizar la privacidad de los datos en las sesiones Telnet 5250 entre el servidor y los clientes.

Objetivos

En este caso práctico, Bob desea proteger las cuentas de accionistas de las sesiones Telnet 5250 de sus clientes de intermediación financiera en el sistema. Bob desea habilitar SSL para proteger la privacidad de los datos de los clientes en Internet. Asimismo, quiere habilitar los certificados para la autenticación de clientes a fin de garantizar que el sistema verifique que únicamente sus clientes acceden a sus cuentas. Una vez que ha configurado el servidor Telnet para SSL y ha habilitado la autenticación del servidor y los clientes, puede desplegar esta nueva opción de acceso a las cuentas para sus clientes con la garantía de que las sesiones de Telnet 5250 serán seguras:

- Proteger el servidor Telnet con SSL.
- Habilitar el servidor Telnet para la autenticación de clientes.
- Obtener un certificado privado de una autoridad certificadora (CA) local y asignarlo a Telnet.

Detalles

En este caso práctico, la configuración de la empresa de intermediación financiera es la siguiente:

- El sistema ejecuta i5/OS V5R4, o posterior, y proporciona acceso a cuentas de accionistas mediante sesiones Telnet 5250.
- En el sistema se inicia la aplicación de servidor Telnet.
- El servidor Telnet inicializa SSL y comprueba la información del certificado del ID de aplicación QIBM_QTV_TELNET_SERVER.

- Si la configuración del certificado Telnet es correcta, el servidor Telnet empieza a escuchar en el puerto SSL para ver si hay conexiones de cliente.
- Un cliente inicia una petición de acceso al servidor Telnet.
- El servidor Telnet responde proporcionando su certificado al cliente.
- El software del cliente valida el certificado como un origen aceptable y de confianza para comunicarse con el servidor.
- El servidor Telnet solicita un certificado procedente del software del cliente.
- El software del cliente presenta un certificado al servidor Telnet.
- El servidor Telnet valida el certificado y reconoce el derecho del cliente a establecer una sesión 5250 con el servidor.
- El servidor Telnet establece una sesión 5250 con el cliente.

Prerrequisitos y supuestos

En este caso práctico se supone lo siguiente:

- El sistema ejecuta OS/400 V5R2, o i5/OS V5R3, o posterior.
- TCP/IP está configurado.
- Bob tiene la autorización *IOSYSCFG.
- Bob soluciona los problemas en Configuración del servidor Telnet.
- Bob soluciona los problemas en Requisitos previos de SSL.
- Bob crea una autoridad certificadora local en el sistema.

Procedimientos

Hay dos conjuntos de tareas que Bob debe llevar a cabo para implementar este caso práctico: uno le permite configurar el sistema a fin de utilizar SSL y requiere certificados para la autenticación de usuario; el otro permite a los usuarios de los clientes Telnet participar en sesiones SSL con el servidor Telnet de Bob y obtener certificados para la autenticación de usuario.

Bob sigue los procedimientos siguientes para completar este caso práctico:

Procedimiento del servidor Telnet

Para implementar este caso práctico, Bob debe llevar a cabo estas tareas en el sistema:

1. Eliminar restricciones de puerto. Consulte Eliminación de restricciones de puerto.
2. Crear y poner en vigor una autoridad certificadora local. Consulte Crear y operar una autoridad certificadora local.
3. Configurar el servidor Telnet a fin de requerir certificados para la autenticación de clientes. Consulte Configuración del servidor Telnet a fin de requerir certificados para la autenticación de clientes.
4. Habilitar e iniciar SSL en el servidor Telnet. Consulte Habilitación e inicio de SSL en el servidor Telnet.

Procedimiento de configuración de los clientes

Para implementar este caso práctico, cada usuario que accede al servidor Telnet del sistema de Bob debe efectuar estas tareas:

1. Habilitar SSL en el cliente Telnet. Consulte Habilitación de SSL en el cliente Telnet.
2. Habilitar el cliente Telnet a fin de que presente un certificado para la autenticación. Consulte Habilitación del cliente Telnet a fin de que presente un certificado para la autenticación.

Estas tareas permiten implementar tanto SSL como la autenticación de clientes mediante certificados, con lo que se obtiene un acceso protegido por SSL a la información de las cuentas de los clientes de Bob por medio de sesiones Telnet 5250.

Detalles de configuración para proteger Telnet con SSL

Aquí se describen los pasos de configuración detallados para proteger Telnet con la Capa de sockets seguros (SSL).

Paso 1: eliminar restricciones de puerto

En los releases anteriores a V5R1, se empleaban restricciones de puerto ya que el soporte SSL (capa de sockets seguros) no estaba disponible para Telnet. Ahora puede especificar si debe iniciarse el soporte SSL, no SSL o ambos. Por consiguiente, las restricciones de puerto ya no son necesarias. Si ha definido restricciones de puerto en releases anteriores, debe eliminar las restricciones de puerto para utilizar el parámetro SSL.

Para determinar si tiene restricciones de puerto Telnet y eliminarlas para que pueda configurar el servidor Telnet de modo que utilice SSL, siga estos pasos:

1. Para ver las restricciones de puerto actuales existentes, inicie System i Navigator y expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **Restricciones de puerto** para ver una lista de valores de restricciones de puerto.
4. Seleccione la restricción de puerto que desea eliminar.
5. Pulse **Eliminar**.
6. Pulse **Aceptar**.

El valor predeterminado establece iniciar sesiones SSL en el puerto 992 y sesiones no SSL en el puerto 23. El servidor Telnet utiliza la entrada de la tabla de servicio de Telnet para obtener el puerto no SSL y Telnet SSL para obtener el puerto SSL.

Paso 2: crear y operar una autoridad certificadora local

Para emplear el Gestor de Certificados Digitales (DCM) a fin de crear y operar una autoridad certificadora (CA) local en el sistema, siga estos pasos:

1. Inicie el DCM.
2. En el marco de navegación del DCM, seleccione **Crear una autoridad certificadora (CA)** para visualizar una serie de formularios. Estos formularios le guiarán en el proceso de creación de una CA local y en la realización de otras tareas necesarias para empezar a utilizar certificados digitales para SSL, la firma de objetos y la verificación de firmas.
3. Cumplimente todos los formularios que aparezcan. Hay un formulario para cada una de las tareas que debe realizar para crear y poner en vigor una CA local en el sistema. El hecho de cumplimentar estos formularios le permitirá:
 - a. Elegir cómo se almacenará la clave privada para el certificado de la CA local. Este paso solo se incluye si se tiene instalado un coprocesador criptográfico PCI IBM 4758-023 en el sistema. Si el sistema no tiene un coprocesador criptográfico, el DCM automáticamente almacena el certificado y su clave privada en el almacén de certificados de CA local.
 - b. Proporcionar información de identificación para la CA local.
 - c. Instalar el certificado de CA local en el PC o en el navegador. De este modo el software puede reconocer la CA local y validar los certificados que emite la CA.
 - d. Elegir los datos de política para la CA local.
 - e. Utilizar la nueva CA local para emitir un certificado de cliente o servidor que las aplicaciones pueden emplear para las conexiones SSL. Si tiene instalado en el sistema un coprocesador criptográfico PCI IBM 4758-023, este paso le permite seleccionar cómo debe almacenarse la clave

privada del certificado de cliente o servidor. Si el sistema no tiene un coprocesador, el DCM automáticamente coloca el certificado y su clave privada en el almacén de certificados *SYSTEM. El DCM crea el almacén de certificados *SYSTEM en esta tarea.

- f. Seleccionar las aplicaciones que pueden emplear el certificado de cliente o servidor para las conexiones SSL.

Nota: asegúrese de seleccionar el ID de aplicación del servidor Telnet (QIBM_QTV_TELNET_SERVER).

- g. Utilizar la nueva CA local para emitir un certificado de firma de objeto que las aplicaciones pueden emplear para firmar objetos digitalmente. Con ello se crea el almacén de certificados *OBJECTSIGNING, que se puede emplear para gestionar los certificados de firma de objetos.

Nota: aunque en este caso práctico no se utilizan los certificados de firma de objetos, no olvide llevar a cabo este paso. Si cancela el proceso en este punto, la tarea finalizará y deberá llevar a cabo tareas aparte para completar la configuración de los certificados de SSL.

- h. Seleccionar las aplicaciones que se desea que confíen en la CA local.

Nota: asegúrese de seleccionar el ID de aplicación del servidor Telnet (QIBM_QTV_TELNET_SERVER).

Una vez cumplimentados los formularios de esta tarea guiada, podrá configurar el servidor Telnet para exigir la autenticación de los clientes.

Paso 3: configurar el servidor Telnet a fin de exigir certificados para la autenticación de los clientes

Para activar este soporte, el administrador del sistema indica cómo se maneja el soporte SSL. Utilice el panel General de Propiedades de Telnet en System i Navigator para indicar si se iniciará el soporte SSL, no SSL o ambos cuando se inicie el servidor Telnet. De forma predeterminada, siempre se inicia los soportes SSL y no SSL.

El administrador del sistema puede indicar si el sistema requiere la autenticación de clientes SSL para todas las sesiones Telnet. Cuando el soporte SSL está activo y el sistema requiere la autenticación del cliente, la presencia de un certificado de cliente válido significa que el cliente es de confianza.

Para configurar el servidor Telnet con el fin de exigir certificados para la autenticación de los clientes, siga estos pasos:

1. Inicie el DCM.
2. Pulse **Seleccionar un almacén de certificados**.
3. Seleccione *SYSTEM como almacén de certificados que debe abrirse y pulse **Continuar**.
4. Especifique la contraseña adecuada para el almacén de certificados *SYSTEM y pulse **Continuar**.
5. Cuando se renueve el menú de navegación de la izquierda, seleccione **Gestionar aplicaciones** para visualizar una lista de tareas.
6. Seleccione la tarea **Actualizar definición de aplicación** para visualizar una serie de formularios.
7. Seleccione la aplicación de **Servidor** y pulse **Continuar** para ver una lista de aplicaciones de servidor.
8. En la lista de aplicaciones, seleccione el **Servidor Telnet TCP/IP i5/OS**.
9. Pulse **Actualizar definición de aplicación**.
10. En la tabla que aparece, seleccione **Sí** para exigir la autenticación de los clientes.
11. Pulse **Aplicar**. Se visualiza la página **Actualizar definición de aplicación** con un mensaje de confirmación de los cambios efectuados.
12. Pulse **Realizado**.

Ahora que ha configurado el servidor Telnet para que exija certificados para la autenticación de los clientes, puede habilitar e iniciar SSL para el servidor Telnet.

Paso 4: habilitar e iniciar SSL en el servidor Telnet

Para habilitar SSL en el servidor Telnet, siga estos pasos:

1. Abra System i Navigator.
2. Expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
3. Pulse **Telnet** con el botón derecho del ratón.
4. Seleccione **Propiedades**.
5. Seleccione la pestaña **General**.
6. Elija una de estas opciones para el soporte SSL:
 - **Solo seguro**
Seleccione esta opción para permitir únicamente las sesiones SSL con el servidor Telnet.
 - **Solo no seguro**
Seleccione esta opción para que las conexiones con un puerto SSL no se ejecuten correctamente.
 - **Seguro y no seguro**
Permite las sesiones seguras y no seguras con el servidor Telnet.

Para iniciar el servidor Telnet utilizando System i Navigator, siga estos pasos:

1. Expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. En el panel de la derecha, busque **Telnet** en la columna Nombre de servidor.
3. Confirme que en la columna Estado aparece **Iniciado**.
4. Si el servidor no está en ejecución, pulse **Telnet** con el botón derecho del ratón y seleccione **Iniciar**.

Paso 5: habilitar SSL en el cliente Telnet

Para participar en una sesión SSL, el cliente Telnet debe poder reconocer y aceptar el certificado que presenta el servidor Telnet para establecer la sesión SSL. Para autenticar el certificado del servidor, el cliente Telnet debe tener una copia del certificado de la CA en la base de datos de claves de i5/OS. Cuando el servidor Telnet utiliza un certificado de una CA local, el cliente Telnet debe obtener una copia del certificado de CA local e instalarla en la base de datos de claves de i5/OS.

Para añadir un certificado de CA local desde el sistema a fin de que el cliente Telnet pueda participar en sesiones SSL con los servidores Telnet que utilizan un certificado de la CA local, siga estos pasos:

1. Abra System i Navigator.
2. Pulse el nombre de *su sistema* con el botón derecho del ratón.
3. Seleccione **Propiedades**.
4. Seleccione la pestaña **Sockets Seguros**.
5. Pulse **Descargar**. Con esta acción se baja automáticamente el certificado de autoridad certificadora de i5/OS a la base de datos de claves de certificados.
6. Se le solicitará la contraseña de la base de datos de claves. Salvo que antes haya cambiado la contraseña predeterminada por otra distinta, especifique ca400. Aparece un mensaje de confirmación. Pulse **Aceptar**.

El botón de bajada actualiza automáticamente la base de datos de claves de PC de IBM Toolbox para Java.

Paso 6: habilitar el cliente Telnet a fin de que presente un certificado para la autenticación

Ya ha configurado SSL para el servidor Telnet, ha especificado que el servidor debe tener como certificados de confianza los que emita la CA local y ha especificado que debe exigir certificados para la autenticación de los clientes. Ahora los usuarios deben presentar un certificado de cliente válido y de confianza al servidor Telnet en cada intento de conexión.

Para que la autenticación de clientes funcione, antes los clientes deben utilizar la CA local para obtener un certificado para la autenticación del servidor Telnet e importar ese certificado en la base de datos de la Gestión de claves IBM.

En primer lugar, los clientes deben utilizar el DCM para obtener un certificado de usuario siguiendo estos pasos:

1. Inicie el DCM.
2. En el marco de navegación de la izquierda, seleccione **Crear certificado** para visualizar una lista de tareas.
3. En la lista de tareas, seleccione **Certificado de usuario** y pulse **Continuar**.
4. Complimente el formulario **Certificado de usuario**. Solo hay que complimentar los campos marcados como "Necesario". Pulse **Continuar**.
5. En función del navegador que utilice, se le solicitará que genere un certificado que se cargará en el navegador. Siga las indicaciones que le facilita el navegador.
6. Cuando se vuelva a cargar la página **Crear certificado de usuario** del navegador, pulse **Instalar certificado**. De este modo se instalará el certificado en el navegador.
7. Exporte el certificado al PC. Debe almacenar el certificado en un archivo protegido mediante contraseña.

Nota: es preciso utilizar Microsoft Internet Explorer 5 o Netscape 4.5 para emplear las funciones de exportar e importar.

A continuación, debe importar el certificado en la base de datos de la Gestión de claves IBM a fin de que el cliente Telnet pueda utilizarlo para la autenticación del certificado en la clave IBM siguiendo estos pasos:

Debe añadir el cliente de importación que crea el certificado de cliente a la base de datos de claves de PC; de lo contrario, la operación de importación del certificado de cliente no funcionará.

1. Pulse **Inicio** → **Programas** → **IBM System i Access para Windows** → **System i Access para Windows Propiedades**.
2. Seleccione la pestaña **Sockets Seguros**.
3. Pulse **Gestión de claves IBM**.
4. Se le solicitará la contraseña de la base de datos de claves. Salvo que antes haya cambiado la contraseña predeterminada por otra distinta, especifique ca400. Aparece un mensaje de confirmación. Pulse **Aceptar**.
5. En el menú desplegable, seleccione **Certificados personales**.
6. Pulse **Importar**.
7. En la pantalla **Importar clave**, especifique el nombre de archivo y la vía de acceso del certificado. Pulse **Aceptar**.
8. Especifique la contraseña del archivo protegido. Es la misma contraseña que ha especificado al crear un certificado de usuario en el DCM. Pulse **Aceptar**. Cuando el certificado se haya añadido correctamente a los certificados personales en Gestión de claves IBM, podrá utilizar el emulador PC5250 o cualquier otra aplicación Telnet.

Una vez realizados estos pasos, el servidor Telnet puede establecer una sesión SSL con el cliente Telnet y el servidor puede autenticar el acceso del usuario a los recursos a partir del certificado que presenta el cliente.

Tareas relacionadas

Inicio de Digital Certificate Manager

“Asignación de un certificado al servidor Telnet” en la página 34

Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

Planificación del servidor Telnet

Puede determinar el número de dispositivos virtuales que deben asociarse a las estaciones de trabajo conectadas al sistema. Este tema también facilita procedimientos de seguridad para controlar o impedir el acceso mediante Telnet.

Antes de configurar el servidor Telnet, debe tener en cuenta varios aspectos operativos y de seguridad. Tiene que saber cuántos dispositivos virtuales desea que Telnet configure automáticamente o si desea crear sus propios dispositivos virtuales. El número de dispositivos virtuales configurados automáticamente afecta al número de intentos de inicio de sesión permitidos. Cuanto mayor sea el número de intentos de inicio de sesión, mayores serán las probabilidades de que un usuario no autorizado logre acceder al servidor. También puede plantearse otras medidas de seguridad, tales como hacer que el servidor Telnet detecte las conexiones perdidas.

Descripciones de dispositivos virtuales

Telnet utiliza descripciones de dispositivos virtuales para mantener la información de la estación de trabajo cliente correspondiente a las sesiones Telnet abiertas. A continuación, se proporciona información sobre cómo configurar y denominar las descripciones de dispositivos virtuales.

Una estación de trabajo de *dispositivo virtual* conectada es una descripción de dispositivo que se utiliza para crear una conexión entre un usuario y una estación de trabajo física conectada a un sistema remoto. Los dispositivos virtuales proporcionan información acerca del dispositivo físico (pantalla o impresora) a los programas que residen en el sistema. El sistema busca el protocolo de conexión cliente/servidor para especificar un dispositivo virtual. Si el sistema no encuentra un dispositivo virtual específico, busca un dispositivo virtual designado en un programa de salida registrado. Si el sistema no encuentra un dispositivo virtual, intenta emparejar una descripción de dispositivo virtual con un tipo y modelo de dispositivo similar al dispositivo que se encuentra en el sistema local.

Convenios de denominación de Telnet para los controladores y dispositivos virtuales

El servidor Telnet utiliza los siguientes convenios de denominación para los controladores y dispositivos virtuales creados automáticamente, según los estándares de i5/OS:

- En el caso de los controladores virtuales, el servidor utiliza el nombre QPACTL *nm*, donde *nm* es un número decimal superior o igual a 01.
- En el caso de los dispositivos virtuales, el servidor utiliza el nombre QPADEV *xxxx*, donde *xxxx* es un carácter alfanumérico entre 0001 y zzzzz (las vocales están excluidas).
- En el caso de los dispositivos virtuales con nombre, el servidor da a los controladores virtuales el nombre QVIRCD *nnnn*.

Notas:

1. Según el convenio de denominación de i5/OS, el controlador virtual debe tener el nombre QPACTL *nm*.

2. El dispositivo virtual tiene el nombre QPADEV *xxxx*.
3. Debe conceder al perfil de usuario QTCP autorización para los dispositivos virtuales creados por el usuario.
4. Puede cambiar los convenios de denominación para los dispositivos virtuales creados automáticamente empleando la opción *REGFAC de QAUTOVRT.

El número de intentos de inicio de sesión permitidos aumenta con los dispositivos virtuales configurados automáticamente. La cantidad total de intentos de inicio de sesión es igual al número de intentos de inicio de sesión del sistema que están permitidos multiplicado por el número de dispositivos virtuales que pueden crearse. Los valores del sistema de inicio de sesión definen el número de intentos de inicio de sesión permitidos.

El servidor Telnet vuelve a utilizar los dispositivos virtuales existentes disponibles que fueron creados automáticamente, seleccionando dispositivos virtuales del mismo tipo y modelo de dispositivo. Cuando no pueden emparejarse más tipos y modelos de dispositivo, pero aún hay dispositivos virtuales disponibles, se cambia el tipo y modelo de dispositivo para que coincidan con el dispositivo y modelo negociados del cliente. Esto es así tanto para los dispositivos virtuales creados automáticamente (QPADEV *xxxx*) como para los dispositivos virtuales con nombre.

Si opta por crear manualmente dispositivos propios, debe establecer convenios de denominación que permitan gestionar fácilmente la configuración. Puede seleccionar los nombres de dispositivo y los nombres de controlador que desee, siempre y cuando estén conformes con las normas de denominación de objetos de i5/OS.

Conceptos relacionados

“Creación de dispositivos virtuales propios” en la página 23

Puede crear manualmente controladores y dispositivos virtuales, con nombres personalizados o nombres generados automáticamente.

Tareas relacionadas

“Establecimiento del número de dispositivos virtuales” en la página 22

Puede hacer que el servidor Telnet configure automáticamente un número establecido de dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT. También puede limitar el número de intentos de inicio de sesión permitidos.

Referencia relacionada

Valores del sistema de dispositivos: dispositivos de paso a través y Telnet

Seguridad de Telnet

Cuando se inicia Telnet a través de una conexión TCP, debe considerar las medidas de seguridad que impidan o permitan el acceso de usuario al sistema mediante Telnet.

Por ejemplo, debe establecer límites y controles en el número de intentos de inicio de sesión y el número de dispositivos que un usuario puede utilizar para iniciar la sesión.

Cómo impedir el acceso mediante Telnet

Si no desea que nadie utilice Telnet para acceder al sistema, debe impedir la ejecución del servidor Telnet. Para impedir el acceso al sistema mediante Telnet, lleve a cabo las tareas de este tema.

Cómo impedir que Telnet se inicie automáticamente

Para impedir que los trabajos del servidor Telnet se inicien automáticamente al iniciar TCP/IP, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Telnet** con el botón derecho del ratón y seleccione **Propiedades**.
3. Deseleccione **Iniciar cuando se inicia TCP/IP**.

Cómo impedir el acceso a los puertos Telnet

Para impedir que se inicie Telnet e impedir que alguien asocie una aplicación de usuario, como una aplicación de socket, al puerto que el sistema normalmente utiliza para Telnet, siga estos pasos:

1. En System i Navigator, pulse *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la ventana Propiedades de configuración de TCP/IP, pulse la pestaña **Restricciones de puerto**.
4. En la página Restricciones de puerto, pulse **Añadir**.
5. En la página Añadir restricción de puerto, especifique los siguientes valores:
 - **Nombre de usuario:** especifique un nombre de perfil de usuario que esté protegido en el sistema. (Un perfil de usuario protegido es un perfil de usuario que no posee programas que adopten autorizaciones y no tiene una contraseña conocida por otros usuarios.) Al restringir el puerto a un usuario específico, automáticamente se excluyen todos los demás usuarios.
 - **Puerto inicial:** 23 (para TELNET no SSL) o 992 (para TELNET SSL)
 - **Puerto final:** 23 (para TELNET no SSL) o 992 (para TELNET SSL)
 - **Protocolo:** TCP

Nota: estos números de puerto se especifican en la tabla Trabajar con entradas de la tabla de servicios (WRKSRVTBLE) con los nombres de servicio Telnet y Telnet-ssl. Pueden correlacionarse con puertos distintos del 23 y el 992. Repita este proceso para cada puerto que desee restringir. Puede obtener información sobre las asignaciones de números de puerto más habituales en Internet Assigned Numbers Authority (IANA).

6. Pulse **Aceptar** para añadir la restricción.
7. En la página Restricciones de puerto, pulse **Añadir** y repita el procedimiento para el protocolo de datagramas de usuario (UDP).
8. Pulse **Aceptar** para guardar las restricciones de puerto y cerrar la ventana Propiedades de configuración de TCP/IP.
9. La restricción de puerto entrará en vigor la próxima vez que se inicie TCP/IP. Si TCP/IP está activo cuando se establecen las restricciones de puerto, es preciso finalizar TCP/IP y volver a iniciarlo.

Información relacionada

 [Internet Assigned Numbers Authority \(IANA\)](#)

Control del acceso mediante Telnet

Tenga en cuenta las consideraciones sobre seguridad si desea que los clientes Telnet puedan acceder al sistema.

Autenticación de clientes

El servidor Telnet da soporte a la autenticación de clientes además de a la autenticación del servidor SSL. Si esta opción está habilitada, el servidor Telnet autentica los certificados de cliente y servidor cuando los clientes Telnet se conecten al puerto Telnet SSL. Los clientes Telnet que no envíen un certificado de cliente válido al intentar conectarse al puerto Telnet SSL no podrán establecer una sesión de pantalla o impresora.

Protección de contraseñas

Las contraseñas de Telnet no están cifradas cuando se envían entre el cliente tradicional y el servidor. En función de los métodos de conexión que se utilicen, el sistema puede ser vulnerable al robo de contraseñas mediante el husmeo de líneas (sniffing). (La acción de supervisar una línea mediante un equipo electrónico suele recibir el nombre de husmear). Las contraseñas de Telnet están cifradas, si se utilizan las negociaciones de TN5250E para intercambiar una contraseña cifrada. En este caso, el panel de

inicio de sesión puede eludirse y no se envía ninguna contraseña no cifrada por la red. Solo se cifra la contraseña con TN5250E; para cifrar todo el tráfico se necesita SSL.

No obstante, si utiliza el servidor Telnet SSL y un cliente Telnet habilitado para SSL, todas las transacciones, incluidas las contraseñas, están cifradas y protegidas. El puerto Telnet SSL está definido en la entrada WRKSRVTBLE bajo .Telnet-ssl que limita el número de intentos de inicio de sesión. Aunque el valor del sistema QMAXSIGN hace referencia a Telnet, puede disminuir la eficacia de este valor del sistema si se establece el sistema de modo que configure automáticamente los dispositivos virtuales. Cuando el valor del sistema QAUTOVRT tiene un valor superior a 0, el usuario Telnet anómalo puede volver a conectarse y acceder a un dispositivo virtual recién creado. Esto puede continuar hasta que se produzca una de las situaciones siguientes:

- Todos los dispositivos virtuales están inhabilitados y el sistema ha superado el límite de creación de nuevos dispositivos virtuales.
- Todos los perfiles de usuario están inhabilitados.
- El intruso (hacker) consigue iniciar la sesión en el sistema.

Al configurar automáticamente los dispositivos virtuales se multiplica el número de intentos de Telnet disponibles.

Nota: para facilitar el control de los dispositivos virtuales, puede establecer el valor del sistema QAUTOVRT en un valor superior a 0 durante un periodo de tiempo corto. Utilice Telnet para forzar al sistema a crear dispositivos o espere a que otros usuarios hagan que el sistema cree suficientes dispositivos virtuales. A continuación, establezca el valor del sistema QAUTOVRT en 0.

Las mejoras de Telnet permiten limitar el número de veces que un intruso puede intentar acceder al sistema. Puede crear un programa de salida al que llame el sistema cada vez que un cliente intente iniciar una sesión Telnet. El programa de salida recibe la dirección IP del solicitante. Si el programa ve una serie de peticiones de la misma dirección IP en un periodo de tiempo reducido, puede llevar a cabo una acción, como por ejemplo rechazar las peticiones adicionales que procedan de la dirección y enviar un mensaje a la cola de mensajes QSYSOPR. En el tema Visión general de la prestación de programas de salida de Telnet se proporciona información global sobre la prestación de los programas de salida de Telnet.

Nota: si lo prefiere, también puede emplear el programa de salida de Telnet para proporcionar anotaciones. En lugar de que sea el programa el tome decisiones sobre los posibles intentos de intrusión, puede utilizar la prestación de anotaciones para supervisar los intentos de iniciar sesiones Telnet.

Finalización de sesiones inactivas

Las sesiones Telnet se incluyen en el proceso del valor QINACTITV del sistema. El valor del sistema QINACTMSGQ define la acción para las sesiones Telnet interactivas que están inactivas una vez transcurrido el intervalo de tiempo de espera de trabajos inactivos. Si el valor QINACTMSGQ especifica que el trabajo debe desconectarse, la sesión debe dar soporte a la función de desconexión de trabajos. De lo contrario, el trabajo finaliza en lugar de desconectarse. Las sesiones Telnet que siguen utilizando descripciones de dispositivos denominadas QPADEVxxxx no permitirán a los usuarios desconectarse de esos trabajos. Desconectarse de esos trabajos no está permitido ya que la descripción de dispositivo a la que se vuelve a conectar a un usuario es imprevisible. Para desconectar un trabajo se requiere la misma descripción de dispositivo para el usuario una vez reconectado el trabajo.

Limitación del número de intentos de inicio de sesión

El número de intentos de inicio de sesión en Telnet permitidos aumenta si tiene dispositivos virtuales configurados automáticamente. El valor del sistema de dispositivo en System i Navigator define el número de dispositivos virtuales que Telnet puede crear.

Utilice los valores del sistema de inicio de sesión para definir el número de intentos de inicio de sesión en el sistema permitidos. Si desea obtener instrucciones para establecer este valor en System i Navigator, consulte “Restricción de usuarios privilegiados a dispositivos específicos y limitación del número de intentos de inicio de sesión” en la página 24.

Restricción de perfiles de usuario avanzados

Puede emplear el valor del sistema QLMTSECOFR para restringir los usuarios con la autorización especial *ALLOBJ o *SERVICE. El usuario o QSECOFR debe tener una autorización explícita para un dispositivo a fin de iniciar la sesión. De este modo puede impedir que los usuarios con la autorización especial *ALLOBJ utilicen Telnet para acceder al sistema asegurándose de que QSECOFR no tiene autorización para los dispositivos virtuales. En lugar de impedir el acceso de los usuarios de Telnet con la autorización especial *ALLOBJ, puede restringir los usuarios de Telnet avanzados por ubicación. Con el punto de salida de iniciación de Telnet, puede crear un programa de salida que asigne una descripción de dispositivo específica a una petición de sesión a partir de la dirección IP del solicitante.

Control de función por ubicación

Puede controlar qué funciones están permitidas o qué menú ve el usuario según la ubicación donde se origina la petición de Telnet. La API (interfaz de programas de aplicación) QDCRDEVD permite acceder a la dirección IP del solicitante. Vea varias recomendaciones a continuación para utilizar este soporte:

- Puede utilizar la API en un programa inicial para todos los usuarios (si la actividad de Telnet es significativa en su entorno).
- Puede establecer el menú del usuario o incluso cambiar a un perfil de usuario específico en función de la dirección IP del usuario que solicita el inicio de sesión.
- Puede emplear el programa de salida de Telnet para tomar decisiones según la dirección IP del solicitante. De este modo no es necesario definir un programa inicial en cada perfil de usuario. Por ejemplo, puede establecer el menú inicial del usuario, establecer el programa inicial del usuario o especificar con qué perfil de usuario se ejecutará la sesión Telnet.

Además, con el acceso a la dirección IP del usuario, puede permitir la impresión dinámica en una impresora asociada a la dirección IP del usuario. La API QDCRDEVD también devuelve las direcciones IP de las impresoras, así como de las pantallas. Seleccione el formato DEVD1100 para las impresoras y DEVD0600 para las pantallas.

Control del inicio de sesión automático

Telnet da soporte a la posibilidad de que un usuario de System i Access para Windows eluda la pantalla de inicio de sesión enviando un nombre de perfil de usuario y una contraseña con la petición de sesión Telnet. El sistema utiliza el valor establecido para el valor del sistema QRMTSIGN (Inicio de sesión remoto) a fin de determinar cómo manejar las peticiones de inicio de sesión automático. La tabla siguiente muestra las opciones. Estas opciones solo son válidas cuando la petición de Telnet incluye un ID de usuario y una contraseña.

Tabla 2. Opciones del valor del sistema QRMTSIGN

Opción	Cómo funciona QRMTSIGN con Telnet
*REJECT	Las sesiones Telnet que solicitan el inicio de sesión automático no están permitidas.
*VERIFY	Si la combinación de perfil de usuario y contraseña es válida, se inicia la sesión Telnet. ¹
*SAMEPRF	Si la combinación de perfil de usuario y contraseña es válida, se inicia la sesión Telnet. ¹
*FRCSIGNON	El sistema pasa por alto el perfil de usuario y la contraseña. El usuario ve la pantalla de inicio de sesión.

¹- Un programa de salida de Telnet registrado puede alterar temporalmente el valor de QRMTSIGN eligiendo si debe permitirse el inicio de sesión automático para un solicitante (probablemente en función de la dirección IP)

Esta validación se produce antes de que se ejecute el programa de salida de Telnet. El programa de salida recibe una indicación que describe si la validación se ha ejecutado correcta o incorrectamente. De todos modos, el programa de salida puede permitir o denegar la sesión, independientemente del indicador. La indicación tiene uno de los valores siguientes:

- Valor = 0; la contraseña o frase de paso del cliente (o el ticket de Kerberos) no se ha validado o no se ha recibido.
- Valor = 1; la contraseña o frase de paso no cifrada del cliente se ha validado.
- Valor = 2; la contraseña o frase de paso cifrada del cliente (o el ticket de Kerberos) se ha validado.

Habilitación del inicio de sesión anónimo

Puede emplear los programas de salida de Telnet para permitir el uso de Telnet anónimo o de invitado en el sistema. Con el programa de salida, puede detectar la dirección IP del solicitante. Si la dirección IP procede de fuera de la organización, puede asignar la sesión Telnet a un perfil de usuario que tiene autorización limitada en el sistema y un menú específico. Puede eludir la pantalla de inicio de sesión a fin de que el visitante no tenga la posibilidad de utilizar otro perfil de usuario más avanzado. Con esta opción, el usuario no tiene que especificar un ID de usuario y una contraseña.

Visión general de la prestación de programas de salida de Telnet

Puede registrar programas de salida escritos por usuario que se ejecuten cuando se inicie una sesión Telnet y cuando finalice. Puede realizar las siguientes acciones cuando inicie un programa de salida:

- Utilice el certificado de SSL cliente para asociar un perfil de usuario al certificado y asignar ese perfil de usuario a la sesión Telnet, eludiendo la pantalla de inicio de sesión.
- Utilice la dirección IP del sistema (local) en sistemas conectados a más de una red para direccionar las conexiones a distintos subsistemas en función de la interfaz de red (dirección IP).
- Permita o deniegue la sesión, según cualquier criterio conocido, como la dirección IP del usuario, la hora, el perfil de usuario solicitado, el tipo de dispositivo (por ejemplo, una impresora), etc.
- Asigne una descripción de dispositivo de i5/OS específica para la sesión. Esto permite direccionar el trabajo interactivo a cualquier subsistema configurado para recibir estos dispositivos.
- Asigne valores de idioma nacional específicos para la sesión, como por ejemplo el teclado y el juego de caracteres.
- Asigne un perfil de usuario específico para la sesión.
- Inicie la sesión automáticamente en el solicitante (sin visualizar una pantalla de inicio de sesión).
- Configure las anotaciones de auditoría para la sesión.

Conceptos relacionados

“Configuración automática de dispositivos virtuales” en la página 22

Puede hacer que el servidor Telnet configure automáticamente los dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT en System i Navigator.

“Utilización de programas de punto de salida de Telnet” en la página 43

Con el uso de los programas de salida, un programador con experiencia puede crear procesos personalizados durante una aplicación. Si el servidor Telnet encuentra un programa registrado en uno de los puntos de salida del servidor, llama a ese programa utilizando los parámetros definidos por el punto de salida.

Tareas relacionadas

Digital Certificate Manager (DCM)

“Establecimiento del parámetro de tiempo de vida de la sesión” en la página 25
Puede utilizar el parámetro de tiempo de vida TCP para establecer el tiempo máximo de desocupación que permite el protocolo TCP antes de enviar un paquete de prueba para comprobar si una sesión está inactiva.

Referencia relacionada

Valores del sistema: visión general de dispositivos

Valores del sistema: visión general de inicio de sesión

Información relacionada



Technical Studio: Telnet Exit Programs

Configuración del servidor Telnet

Este tema contiene información sobre cómo llevar a cabo la configuración del servidor Telnet para varios tipos de emulación.

Una de las funciones más importantes de Telnet es su capacidad de negociar opciones entre el cliente y el servidor. Este tipo de negociación abierta hace posible que tanto el cliente como el servidor inicien o acepten una petición. Dispone de varios tipos de emulación distintos para la negociación de peticiones y su conversión en salida. El sistema puede soportar estaciones de trabajo de tipo 3270 y estaciones de trabajo VTxxx, pero el tipo preferido es la emulación 5250.

Para configurar el servidor Telnet a fin de utilizarlo con uno de los otros tipos de emulación soportados, realice las siguientes tareas de enlace hijo que contienen procedimientos:

Una vez que haya configurado Telnet, le interesará proteger Telnet con SSL (capa de sockets seguros).

Conceptos relacionados

“Caso práctico de Telnet: configuración del servidor Telnet” en la página 2

En este caso práctico se describe cómo configura un administrador un servidor Telnet, incluidos los objetivos, los requisitos previos y los supuestos, así como los detalles de configuración.

Inicio del servidor Telnet

El servidor Telnet activo tiene una o más instancias de cada uno de los siguientes trabajos en ejecución en el subsistema QSYSWRK: QVTNET y QTVDEVICE.

Para iniciar el servidor Telnet utilizando System i Navigator, siga estos pasos:

1. Expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. En el panel de la derecha, busque **Telnet** en la columna Nombre de servidor.
3. Confirme que en la columna Estado aparece **Iniciado**.
4. Si el servidor no está en ejecución, pulse **Telnet** con el botón derecho del ratón y seleccione **Iniciar**.

Conceptos relacionados

“Finalización de la sesión del servidor Telnet” en la página 42

Al finalizar una sesión Telnet, permite que el dispositivo virtual esté disponible para una nueva sesión Telnet.

Tareas relacionadas

“Activación del subsistema QSYSWRK” en la página 26

El trabajo del sistema para una aplicación TCP/IP debe iniciarse en el subsistema QSYSWRK. El subsistema de spool, QSPL, debe estar activo para ejecutar sesiones de paso a través de impresora.

“Habilitación de SSL en el servidor Telnet” en la página 38

Siga estos pasos para aprender a habilitar la Capa de sockets seguros (SSL) en el servidor Telnet.

“Comprobación del estado del sistema” en la página 98

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

Establecimiento del número de dispositivos virtuales

Puede hacer que el servidor Telnet configure automáticamente un número establecido de dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT. También puede limitar el número de intentos de inicio de sesión permitidos.

Puede especificar el número de dispositivos que se inician automáticamente y el número máximo de dispositivos que el sistema configura automáticamente. El sistema configura o crea un dispositivo cada vez, a medida que es necesario, hasta un límite especificado.

1. En System i Navigator, seleccione *su sistema* → **Configuración y servicio** → **Valores del sistema**.
2. En el panel de la derecha, pulse **Dispositivos** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Valores del sistema de dispositivos, habilite **Dispositivos de paso a través y TELNET** y seleccione una opción para la configuración automática de dispositivos virtuales. Las opciones son:
 - **Sin número máximo de dispositivos** - Permite configurar un número ilimitado de dispositivos.
 - **Número máximo de dispositivos (1-32.500)** - Especifique un valor entre 1 y 32.500 como número máximo de dispositivos que se pueden configurar automáticamente.
 - **Ejecutar programas de salida registrados** - Efectúa una llamada al programa registrado para el punto de salida Selección de dispositivo virtual (QIBM_QPA_DEVSEL) cuando es necesario seleccionar o crear automáticamente un dispositivo virtual.

Conceptos relacionados

“Descripciones de dispositivos virtuales” en la página 15

Telnet utiliza descripciones de dispositivos virtuales para mantener la información de la estación de trabajo cliente correspondiente a las sesiones Telnet abiertas. A continuación, se proporciona información sobre cómo configurar y denominar las descripciones de dispositivos virtuales.

“Configuración automática de dispositivos virtuales”

Puede hacer que el servidor Telnet configure automáticamente los dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT en System i Navigator.

Referencia relacionada

Valores del sistema de dispositivos: dispositivos de paso a través y Telnet

Información relacionada



Technical Studio: Telnet Exit Programs

Configuración automática de dispositivos virtuales

Puede hacer que el servidor Telnet configure automáticamente los dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT en System i Navigator.

Puede especificar el número de dispositivos que se inician automáticamente y el número máximo de dispositivos que el sistema configura automáticamente. El sistema configura o crea un dispositivo cada vez, a medida que es necesario, hasta un límite especificado.

Al configurar automáticamente los dispositivos virtuales con Telnet, el servidor Telnet no suprime los dispositivos virtuales ni los dispositivos cuando se cierra la sesión. El servidor no suprime los dispositivos aunque el número de dispositivos conectados a los controladores virtuales supere el número máximo. Si los dispositivos ya existen en el controlador virtual, el servidor Telnet puede utilizarlos. El servidor Telnet modifica los atributos de un dispositivo existente para que coincidan con la petición del cliente si el dispositivo virtual se solicita por su nombre.

Si nunca ha permitido la configuración automática de los dispositivos virtuales en el sistema, el valor del sistema de dispositivos correspondiente al número máximo de dispositivos es 0. Un intento de conexión

Telnet falla cuando el número de dispositivos en uso supere el número máximo de dispositivos. Un dispositivo en uso tiene el estado activo o pantalla de inicio de sesión. Si intenta iniciar la sesión, recibirá un mensaje (TCP2504) en el que se le indicará que la sesión del cliente Telnet ha finalizado y la conexión se ha cerrado. Además, el trabajo QTCPIP del sistema remoto envía un mensaje (CPF8940) que indica que un dispositivo virtual no puede seleccionarse automáticamente.

Si cambia el número máximo de dispositivos a 10, el siguiente intento de conexión Telnet hace que el servidor Telnet cree un dispositivo virtual. Telnet crea este dispositivo virtual debido a que el número de dispositivos virtuales del controlador (0) es inferior al número especificado en el número máximo de dispositivos (10). Aunque vuelva a cambiar el número especificado a 0, el siguiente intento de conexión Telnet que realice un usuario será satisfactorio. Cuando un intento de conexión Telnet falla porque el sistema no puede crear un dispositivo virtual, se envía el mensaje CPF87D7 a la cola de mensajes del operador del sistema en el servidor Telnet.

Notas:

1. El servidor Telnet no suprime automáticamente los dispositivos virtuales configurados ni los dispositivos con nombre, aunque el número de dispositivos conectados a los controladores virtuales supere el número máximo de dispositivos.
2. Los valores del sistema de dispositivos especifican si los dispositivos virtuales de paso a través y los dispositivos virtuales de pantalla completa Telnet que están conectados a los controladores QPACTL nm se configuran automáticamente. Este valor del sistema no afecta a los dispositivos conectados a los controladores QVIRCD $nnnn$, ya que estos no son los dispositivos del sistema predeterminado. Normalmente, los dispositivos QPADEV $nnnn$ se conectan a los controladores QPACTL nm , mientras que los dispositivos con nombre (como por ejemplo NEWYORK001) se conectan al controlador QVIRCD $nnnn$.

Conceptos relacionados

“Control del acceso mediante Telnet” en la página 17

Tenga en cuenta las consideraciones sobre seguridad si desea que los clientes Telnet puedan acceder al sistema.

Tareas relacionadas

“Establecimiento del número de dispositivos virtuales” en la página 22

Puede hacer que el servidor Telnet configure automáticamente un número establecido de dispositivos y controladores virtuales utilizando los valores del sistema de dispositivos QAUTOVRT. También puede limitar el número de intentos de inicio de sesión permitidos.

Referencia relacionada

Valores del sistema de dispositivos: dispositivos de paso a través y Telnet

Creación de dispositivos virtuales propios

Puede crear manualmente controladores y dispositivos virtuales, con nombres personalizados o nombres generados automáticamente.

Si crea sus propios dispositivos virtuales y permite que el sistema seleccione automáticamente el nombre de dispositivo, debe tener en cuenta las normas siguientes:

- El controlador virtual tiene el nombre QPACTL nm , donde nm es un número decimal superior o igual a 01.
- El dispositivo virtual tiene el nombre QPADEV $xxxx$, donde $xxxx$ es un carácter alfanumérico entre 0001 y $zzzz$. El dispositivo virtual debe tener la clase de dispositivo *VRT. La ubicación del dispositivo virtual es bajo un controlador virtual.

Si decide crear sus propios dispositivos, debe conocer los convenios de denominación de descripciones de dispositivos virtuales empleados por el servidor Telnet. Si desea seleccionar sus propios nombres de dispositivo (utilizando un cliente RFC 4777 o las API de terminal virtual), el controlador virtual tendrá el nombre QVIRCD $nnnn$, donde $nnnn$ es un número decimal igual o mayor que 01.

Conceptos relacionados

“Descripciones de dispositivos virtuales” en la página 15

Telnet utiliza descripciones de dispositivos virtuales para mantener la información de la estación de trabajo cliente correspondiente a las sesiones Telnet abiertas. A continuación, se proporciona información sobre cómo configurar y denominar las descripciones de dispositivos virtuales.

Restricción de usuarios privilegiados a dispositivos específicos y limitación del número de intentos de inicio de sesión

Los valores del sistema de inicio de sesión se utilizan para restringir o limitar los dispositivos en los que un usuario puede iniciar la sesión y para definir el número de intentos de inicio de sesión en el sistema permitidos.

Restricción de usuarios privilegiados a dispositivos específicos

El programa bajo licencia i5/OS utiliza los valores del sistema de inicio de sesión para restringir o limitar los dispositivos en los que un usuario puede iniciar la sesión. La *Autorización sobre todos los objetos* (*ALLOBJ) permite al usuario acceder a cualquier recurso del sistema. La *Autorización especial de servicio* (*SERVICE) permite al usuario realizar funciones específicas de servicio en el sistema. Por ejemplo, el usuario con este tipo de autorización podrá depurar un programa y realizar las funciones de visualización y servicio. Para establecer estos valores utilizando System i Navigator, siga estos pasos:

1. Seleccione *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. En el panel de la derecha, pulse **Telnet** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Propiedades de Telnet - Inicio de sesión del sistema, seleccione las siguientes opciones:
 - **Restringir usuarios privilegiados a dispositivos específicos** Esta selección indica que todos los usuarios con autorización especial para todos los objetos (*ALLOBJ) y de servicio (*SERVICE) necesitan autorización explícita para determinadas estaciones de trabajo.
 - **Limitar cada usuario a una sesión de dispositivo** Esta selección indica que un usuario puede iniciar una sesión solo en una estación de trabajo. Esto no impide que el usuario utilice trabajos de grupo o haga una petición de sistema en la estación de trabajo. Ello reduce la probabilidad de compartir contraseñas y dejar desatendidos los dispositivos.

Limitación del número de intentos de inicio de sesión

Utilice los valores del sistema de inicio de sesión para definir el número de intentos de inicio de sesión en el sistema permitidos. El número de intentos de inicio de sesión en Telnet permitidos aumenta si tiene dispositivos virtuales configurados automáticamente. Para establecer estos valores, siga estos pasos:

1. En System i Navigator, seleccione *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. En el panel de la derecha, pulse **Telnet** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Propiedades de Telnet, pulse la pestaña **Inicio de sesión del sistema**.
4. En la página Propiedades de Telnet - Inicio de sesión del sistema, puede especificar el número de intentos de inicio de sesión permitidos y la acción que debe llevarse a cabo si se alcanza el número máximo de intentos de inicio de sesión.
5. Pulse la pestaña **Remoto**.
6. En la página Propiedades de Telnet - Inicio de sesión remoto, seleccione una opción para **Utilizar Telnet para inicio de sesión remoto**. Las opciones son:
 - **Visualizar siempre pantalla de inicio de sesión** - Todas las sesiones de inicio de sesión remoto deben seguir el proceso de inicio de sesión normal.
 - **Permitir eludir la pantalla de inicio de sesión** - El sistema permite al usuario eludir el panel de inicio de sesión. El usuario inicia la sesión en el sistema, pero el panel de inicio de sesión no se visualiza.

Nota: si se habilita Utilizar paso a través para inicio de sesión remoto, las opciones se seleccionan automáticamente en función de los valores que especifique en Utilizar paso a través para inicio de sesión remoto. Aunque seleccione la opción de paso a través, puede seguir utilizando Telnet para los inicios de sesión remotos.

Conceptos relacionados

Valores del sistema: visión general de inicio de sesión

Establecimiento del parámetro de tiempo de vida de la sesión

Puede utilizar el parámetro de tiempo de vida TCP para establecer el tiempo máximo de desocupación que permite el protocolo TCP antes de enviar un paquete de prueba para comprobar si una sesión está inactiva.

El protocolo envía peticiones de tiempo de vida al cliente remoto cada vez que la sesión permanezca desocupada durante períodos superiores al valor de tiempo de vida. El período de desocupación se define mediante el parámetro de tiempo de espera de tiempo de vida de la sesión en las propiedades de Telnet en System i Navigator o mediante un parámetro del mandato CHGTELNA. Cuando parece que una sesión está inactiva (no se recibe respuesta del cliente remoto a los paquetes de prueba de tiempo de vida), esa sesión se finaliza, el dispositivo virtual asociado a la sesión se devuelve a la agrupación de dispositivos virtuales libre, y el sistema operativo i5/OS lleva a cabo la acción establecida en el valor del sistema QDEVRCYACN sobre el trabajo interactivo que se ejecuta en el dispositivo virtual. Esta acción afecta únicamente a los dispositivos virtuales con nombre. En el caso de los dispositivos virtuales seleccionados automáticamente (QPADEVxxxx), el trabajo interactivo siempre finaliza.

El servidor Telnet define de forma predeterminada el valor de tiempo de vida en 600 segundos.

Este valor entra en vigor al iniciar el servidor. Además del parámetro de tiempo de espera de tiempo de vida de la sesión, también puede repasar los valores de intervalo de tiempo de espera en los Valores del sistema de trabajos inactivos en System i Navigator. Este parámetro de tiempo de espera limita el período de tiempo que puede estar desocupado un trabajo interactivo cualquiera antes de que el sistema operativo i5/OS lleve a cabo la acción establecida en el valor del sistema QINACTMSGQ para el trabajo interactivo. En el caso de los trabajos interactivos conectados por Telnet, se aceptará la acción *DSCJOB únicamente para los dispositivos virtuales con nombre. En el caso de los dispositivos virtuales seleccionados automáticamente (QPADEVxxxx), la acción *DSCJOB hace que se finalice el trabajo interactivo.

Para establecer el parámetro de tiempo de vida para Telnet en System i Navigator, siga estos pasos:

1. En System i Navigator, seleccione *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. En el panel de la derecha, pulse **Telnet** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Propiedades de Telnet, pulse la pestaña **Tiempo de espera**.
4. En la página Propiedades de Telnet - Tiempo de espera, especifique la acción que debe llevarse a cabo cuando los trabajos alcancen un valor de tiempo de espera. También puede especificar cuánto tiempo se concede a una operación antes de que el trabajo exceda el tiempo de espera. Puede especificar información tanto para los trabajos inactivos como para los trabajos desconectados.

Conceptos relacionados

“Control del acceso mediante Telnet” en la página 17

Tenga en cuenta las consideraciones sobre seguridad si desea que los clientes Telnet puedan acceder al sistema.

Referencia relacionada

Valores del sistema: visión general de trabajos

Asignación de dispositivos a subsistemas

Antes de que un usuario pueda iniciar una sesión en el sistema, debe definirse la estación de trabajo en un subsistema. La estación de trabajo es el dispositivo de pantalla virtual seleccionado o creado automáticamente por el servidor Telnet.

El nombre o el tipo de la estación de trabajo debe especificarse en la descripción de subsistema en el sistema. Utilice el mandato Visualizar descripción del subsistema (DSPSBSD) para ver las entradas de estación de trabajo definidas en el subsistema.

Puede utilizar el mandato siguiente para añadir todos los tipos de estación de trabajo a un subsistema denominado QINTER:

```
ADDWSE SBSB(QINTER) WRKSTNTYPE(*ALL)
```

Los dispositivos de impresora siempre se direccionan al subsistema de spool QSPL.

El mandato Añadir entrada de estación de trabajo (ADDWSE) puede emitirse cuando el subsistema está activo. No obstante, los cambios pueden surtir efecto inmediatamente o no. Quizás sea necesario detener y reiniciar el subsistema.

Activación del subsistema QSYSWRK

El trabajo del sistema para una aplicación TCP/IP debe iniciarse en el subsistema QSYSWRK. El subsistema de spool, QSPL, debe estar activo para ejecutar sesiones de paso a través de impresora.

Para comprobar el estado del subsistema QSYSWRK, siga estos pasos:

1. En la interfaz basada en caracteres, escriba WRKSBS (Trabajar con subsistemas activos).
2. Verifique que se visualizan los sistemas siguientes:
 - QSYSWRK
 - QINTER
 - QSPL

Si el subsistema QSYSWRK no está activo, siga estos pasos:

1. En la interfaz basada en caracteres, escriba STRSBS (Arrancar subsistema).
2. Teclee QSYSWRK para la descripción de subsistema y QSYS para la biblioteca; a continuación, pulse Intro.
3. Repita la acción para el valor de nombre de subsistema QINTER con la biblioteca QSYS y el valor de nombre de subsistema QSPL y la biblioteca QSYS.

Si no sabe qué subsistema utilizar para los trabajos interactivos, teclee WRKSBSD *ALL en la interfaz basada en caracteres. Las entradas Tipo de estación de trabajo muestran qué dispositivo está asignado a un subsistema.

Qué hacer a continuación:

Creación de perfiles de usuario

Tareas relacionadas

“Inicio del servidor Telnet” en la página 21

El servidor Telnet activo tiene una o más instancias de cada uno de los siguientes trabajos en ejecución en el subsistema QSYSWRK: QTVTELNET y QTVDEVICE.

Creación de perfiles de usuario

En el servidor Telnet, puede crear perfiles de usuario de Telnet mediante System i Navigator.

Para crear perfiles de usuario de Telnet, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema*.
2. Pulse **Usuarios y grupos** con el botón derecho del ratón y seleccione **Usuario nuevo**.
3. Escriba el nombre, la descripción y la contraseña del usuario.
4. Para especificar una descripción de trabajo, pulse **Trabajos** y escriba la descripción del trabajo.
5. Pulse **Aceptar**.

Tipos de emulación soportados por i5/OS

La emulación preferida para el sistema es la emulación 5250. No obstante, el sistema también da soporte a la emulación 3270 y VTxxx.

Seleccione el tipo de emulación para cuyo uso desea configurar el servidor Telnet.

Conceptos relacionados

“Caso práctico de Telnet: configuración del servidor Telnet” en la página 2

En este caso práctico se describe cómo configura un administrador un servidor Telnet, incluidos los objetivos, los requisitos previos y los supuestos, así como los detalles de configuración.

Configuración del servidor Telnet para la modalidad de pantalla completa 5250

La modalidad de pantalla completa 5250 permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa.

Antes de establecer la sesión de cliente Telnet deberá realizar los siguientes pasos:

1. Inicie el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).
2. Establezca la plataforma System i de modo que configure automáticamente los controladores y dispositivos virtuales. Verifique que los trabajos QTVTELNET y QTVDEVICE del subsistema QSYSWRK están activos siguiendo estos pasos:
 - a. Inicie System i Navigator y expanda *su sistema* → **Gestión de trabajo**.
 - b. Pulse **Subsistemas** con el botón derecho del ratón y seleccione **Abrir**.
 - c. Verifique que el subsistema está activo.
3. Compruebe el valor del sistema QAUTOVRT. Debe ser igual al número máximo de usuarios que tienen iniciada una sesión, utilizando dispositivos virtuales configurados automáticamente, en todo momento. QAUTOVRT soporta valores numéricos de 0 a 32.500 y el valor especial *NOMAX.

Configuración del servidor Telnet para la modalidad de pantalla completa 3270

Los usuarios de clientes Telnet pueden iniciar una sesión y ejecutar aplicaciones 5250 de pantalla completa utilizando la modalidad de pantalla completa 3270.

El sistema negocia el soporte de pantalla completa 3270 con cualquier aplicación de cliente Telnet que dé soporte a las aplicaciones 3270 de pantalla completa, en lugar de a las aplicaciones 5250 de pantalla completa. La familia IBM System z constituye un ejemplo de un sistema que negocia el soporte de pantalla completa 3270.

Telnet 5250 (TN5250) entrega la corriente de datos entre los dos sistemas como EBCDIC. Dado que las corrientes de datos 3270 se convierten en corrientes de datos 5250, los dispositivos de estación de trabajo operan como una pantalla 5251 remota para el sistema y los programas de aplicación.

Tras llevar a cabo la configuración general del servidor Telnet, hay algunos pasos adicionales que debe efectuar para habilitar el soporte de sistema para la modalidad de pantalla completa 3270. La modalidad de pantalla completa es una modalidad de bloques (en oposición a una modalidad de líneas). La modalidad de líneas es aquella en la que los datos se transmiten línea a línea, mientras que en la modalidad de bloques o de pantalla completa se transmite toda la pantalla de una sola vez.

Lleve a cabo las tareas siguientes para configurar el servidor Telnet para la modalidad de pantalla completa 3270:

1. Comprobar el valor del sistema QKBDTYPE. Consulte “Comprobación del valor del sistema QKBDTYPE”
2. Establecer la correlación de teclado predeterminada. Consulte “Establecimiento de la correlación de teclado predeterminada”
3. Cambiar una correlación de teclado. Consulte “Cambio de una correlación de teclado”
4. Cambiar la cola de mensajes. Consulte “Cambio de la cola de mensajes” en la página 29

Comprobación del valor del sistema QKBDTYPE

Cuando el servidor Telnet crea automáticamente dispositivos de pantalla virtuales, utiliza el valor del sistema QKBDTYPE para determinar el tipo de teclado del dispositivo virtual.

Si la creación inicial del dispositivo virtual es anómala con el valor del sistema QKBDTYPE, el servidor Telnet utiliza el valor de teclado USB para intentar crear el dispositivo. Si el segundo intento de crear el dispositivo de pantalla virtual es anómalo con el valor USB, se envía un mensaje (CPF87D7) a la cola de mensajes del operador del sistema. Este mensaje indica que el sistema no puede seleccionar el dispositivo virtual automáticamente.

Establecimiento de la correlación de teclado predeterminada

Una estación de pantalla 3270 conectada a un modelo System i mediante Telnet aparece como una estación de pantalla 5251 en una plataforma System i. El teclado de la estación de pantalla 3270 tiene asociada una correlación de teclado equivalente a 5251. La correlación de teclado equivalente a 5251 permite al teclado de la estación de trabajo de pantalla 3270 llevar a cabo funciones equivalentes a 5251 en el sistema.

Cuando el usuario de un sistema cliente Telnet inicia la sesión por primera vez en la modalidad de pantalla completa 3270, el sistema automáticamente asigna la correlación de teclado predeterminada al teclado 3277, 3278 o 3279 del usuario. Evítelo incluyendo una correlación de teclado definida por el usuario en el procedimiento de inicio de sesión del perfil del usuario. Esto proporciona la correlación necesaria para que los teclados 3270 lleven a cabo gran parte de las mismas funciones que los teclados 5250 equivalentes.

Visualización de una correlación de teclado

Puede utilizar el mandato de visualizar correlación de teclado (DSPKBDMAP) para ver la correlación de teclado actual. Otro método consiste en emplear la opción 6 (Visualizar correlación de teclado 3270) del menú Configurar TCP/IP TELNET, mientras el terminal está en la modalidad de emulación 3270.

Cambio de una correlación de teclado

Utilice el mandato de cambiar correlación de teclado (CHGKBDMAP) si desea efectuar pequeños cambios en la correlación de teclado predeterminada. Este mandato está disponible en el menú Configurar TCP/IP TELNET como opción 7 (Cambiar correlación de teclado 3270).

Si desea establecer una nueva correlación de teclado, utilice el mandato de establecer correlación de teclado (SETKBDMAP). Este mandato es la opción 7 (Cambiar correlación de teclado 3270) del menú Configurar TCP/IP TELNET. Las asignaciones de teclas que especifique estarán en vigor hasta que vuelva a emplear estos mandatos para especificar nuevas asignaciones de teclas o hasta que finalice la sesión.

Nota: la diferencia entre CHGKBDMAP y SETKBDMAP radica en que, con SETKBDMAP, el sistema aplica los valores predeterminados y, a continuación, se aplican los cambios del mandato

SETKBDMAP. Con CHGKBDMAP, el sistema aplica los valores predeterminados más los cambios efectuados anteriormente durante esta sesión y, a continuación, se aplican los cambios del mandato CHGKBDMAP.

Cambio de la cola de mensajes

Una cola de mensajes es como un buzón de correo para mensajes. El sistema tiene varias colas de mensajes que contienen mensajes que proporcionan información útil para localizar problemas e informar de los mismos. Si la cola de mensajes de la estación de trabajo está en modalidad de interrupción, los mensajes aparecen en el dispositivo 3270 exactamente cuando aparecen en la pantalla 5250. Para recibir los mensajes en la modalidad de interrupción, debe especificar *BREAK en el mandato de cambiar cola de mensajes (CHGMSGQ). Si la estación de trabajo no está en modalidad de interrupción, recibirá el siguiente mensaje: Ha llegado un mensaje a una cola de mensajes.

Para recuperar este mensaje y seguir utilizando la estación de trabajo, siga estos pasos:

1. Pulse la tecla de función asignada a la función de ayuda o la tecla de función asignada a la función de restaurar error.
2. Escriba el mandato de visualizar mensaje (DSPMSG) o la tecla de función asignada a la función de petición de sistema y a continuación la opción 4 (Visualizar mensaje) para ver el mensaje en espera.
3. Establezca la cola de mensajes de la estación de trabajo en modalidad de interrupción para ver los mensajes cuando lleguen.

Restablecimiento del indicador de entrada inhibida de la pantalla

Si utiliza un modelo System i desde un terminal de tipo 5250, al pulsar algunas teclas en determinadas circunstancias la entrada queda inhibida. Cuando esto sucede, el terminal 5250 muestra un indicador de entrada inhibida.

Dos asteriscos en la esquina inferior derecha de la pantalla representan el indicador de entrada inhibida. Cuando el teclado está inhibido, las teclas correlacionadas con las teclas de función de i5/OS se pasan por alto.

Para restablecer el teclado, pulse la tecla Intro o pulse la tecla correlacionada con la tecla de restablecer.

Conceptos relacionados

“Sesiones de cliente Telnet 3270” en la página 56

El tipo de emulación 3270 permite acceder a un sistema remoto que tiene una aplicación de servidor Telnet.

“Correlación de teclado 3270 para servidores Telnet” en la página 60

Este tema contiene información sobre la correlación de teclado para el soporte de la emulación 3270.

Referencia relacionada

“Tipos de terminal 3270 soportados”

En este tema se describen las prestaciones de los dispositivos 3270 soportados por Telnet. Compruebe que el cliente Telnet 3270 negocia uno de los tipos de terminal 3270 soportados.

Tipos de terminal 3270 soportados:

En este tema se describen las prestaciones de los dispositivos 3270 soportados por Telnet. Compruebe que el cliente Telnet 3270 negocia uno de los tipos de terminal 3270 soportados.

La tabla siguiente muestra los tipos de terminal soportados.

Tabla 3. Correlaciones de estación de trabajo de pantalla completa

Tipo de dispositivo	Prestaciones del dispositivo
3277	Esta estación de pantalla soporta corrientes de datos 3270 genéricos. Los atributos ampliados, como el subrayado, el parpadeo, el contraste invertido o el color, no están soportados.
3278	Esta estación soporta los atributos ampliados, como por ejemplo el parpadeo, el contraste invertido y el subrayado, si se solicitan mediante las palabras clave DDS (especificaciones de descripción de datos) de i5/OS. Notas: <ol style="list-style-type: none">1. Los atributos ampliados no reciben soporte en algunas implementaciones de cliente Telnet 3270 en modalidad de pantalla completa (TN3270).2. Los terminales de juego de caracteres de doble byte (DBCS) que negocian un tipo de terminal 3278-2-E están soportados.
3279	Esta estación de pantalla soporta los atributos de color y los atributos de corriente de datos ampliados enviados para un dispositivo 3278. Los atributos de color vienen determinados (del mismo modo que en un monitor de color completo 5292) por la interpretación de los atributos DDS tales como el parpadeo, la alta intensidad o las palabras clave de color DDS.

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa 3270” en la página 27
Los usuarios de clientes Telnet pueden iniciar una sesión y ejecutar aplicaciones 5250 de pantalla completa utilizando la modalidad de pantalla completa 3270.

Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx

El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

La aplicación de cliente Telnet debe poder negociar el soporte de terminal VTxxx. Cuando se negocia la modalidad VTxxx de pantalla completa, el servidor Telnet es el encargado de correlacionar las funciones 5250 con las teclas VTxxx, y viceversa.

Aunque el servidor Telnet da soporte a los clientes VTxxx, esta no es la modalidad de uso preferida ya que el terminal VTxxx es un dispositivo de modalidad de caracteres. El sistema operativo i5/OS es un sistema de modalidad de bloques. La mayoría de las implementaciones Telnet dan soporte a un cliente TN3270 o TN5250 que debe utilizarse al conectarse a un servidor Telnet.

En general, cuando se pulsa una tecla en un terminal VTxxx, el código hexadecimal asociado a esa tecla se transmite inmediatamente al servidor Telnet. El servidor Telnet debe procesar esa pulsación y a continuación enviar como eco ese carácter al terminal VTxxx donde se visualiza. Esto supone un uso notable de recursos en cada pulsación. En cambio, los dispositivos de modalidad de bloques 5250 y 3270 guardan todas las pulsaciones en el almacenamiento intermedio del sistema cliente hasta que se pulsa una tecla de identificador de atención (AID). Cuando se pulsa una tecla AID, el cliente envía al servidor la entrada guardada en el almacenamiento intermedio para que la procese. Los dispositivos de modalidad de bloques suponen un menor coste por pulsación y por lo general proporcionan un mejor rendimiento que un dispositivo de modalidad de caracteres, como el terminal VTxxx.

VTxxx entrega los datos entre los dos sistemas como ASCII.

Tras llevar a cabo la configuración general del servidor Telnet, debe llevar a cabo algunos pasos adicionales para habilitar el soporte de servidor para la modalidad de pantalla completa VTxxx.

La modalidad de pantalla completa es una modalidad de bloques (en oposición a una modalidad de líneas). La modalidad de líneas es aquella en la que los datos se transmiten línea a línea, mientras que en la modalidad de bloques o de pantalla completa se transmite toda la pantalla de una sola vez.

Lleve a cabo las tareas siguientes para configurar el servidor en la modalidad de pantalla completa VTxxx:

1. "Comprobación del valor del sistema QKBDTYPE"
2. "Establecimiento de la correlación de teclado predeterminada"
3. "Establecimiento del tipo de terminal virtual de red predeterminado" en la página 32
4. "Establecimiento de las tablas de correlación ASCII/EBCDIC" en la página 32

Comprobación del valor del sistema QKBDTYPE

Cuando el servidor Telnet crea automáticamente dispositivos de pantalla virtuales, utiliza el valor del sistema QKBDTYPE para determinar el tipo de teclado del dispositivo virtual.

Si la creación inicial del dispositivo virtual es anómala con el valor del sistema QKBDTYPE, el servidor Telnet vuelve a intentar crear el dispositivo empleando el valor de tipo de teclado USB. Si el segundo intento de crear el tipo de teclado es anómalo, el sistema envía un mensaje (CPF87D7) a las anotaciones de trabajo QTCPIP. Este mensaje indica que el sistema no puede crear el dispositivo virtual automáticamente. El sistema también envía el mensaje a la cola de mensajes del operador del sistema.

Establecimiento de la correlación de teclado predeterminada

Cuando una sesión Telnet negocia en la modalidad de pantalla completa VTxxx, el sistema utiliza una correlación de teclado predeterminada. Para visualizar la correlación de teclado predeterminada para VTxxx, utilice el mandato Visualizar correlación de teclado de VT (DSPVTMAP). Para cambiar la correlación de teclado de VTxxx, utilice el mandato Cambiar correlación de teclado de VT (CHGVTMAP) o el mandato Establecer correlación de teclado de VT (SETVTMAP).

La tabla de teclado numérico muestra las teclas del teclado numérico auxiliar que normalmente transmiten los códigos de números, punto, signo menos y coma.

La tabla de teclado de edición muestra las teclas que transmiten los códigos de las teclas del teclado de edición.

Dado que el teclado VTxxx no tiene las mismas teclas que un teclado 5250, debe existir una correlación de teclado entre las teclas VTxxx y las funciones de i5/OS. El sistema asigna una correlación de teclado predeterminada cuando una sesión VTxxx se establece por primera vez. En algunos casos, puede haber más de una tecla o secuencia de teclas que se correlacione con una función de i5/OS determinada. En estos casos, puede utilizar cualquiera de las teclas definidas para llamar a la función de i5/OS necesaria.

Notas:

1. Cada uno de los caracteres de control es un valor de 1 byte que se genera desde un teclado VTxxx manteniendo pulsada la tecla Control al tiempo que se pulsa una de las teclas alfabéticas. Los caracteres de control con desplazamiento y sin desplazamiento generan los mismos valores hexadecimales.
2. Las secuencias de escape son varios códigos de bytes que se generan pulsando la tecla Esc seguida de los caracteres que forman la secuencia necesaria.

3. El sistema pasa por alto el atributo de mayúsculas/minúsculas de todos los caracteres alfabéticos de una secuencia de escape. Puede escribir los caracteres alfabéticos de las secuencias de escape en mayúsculas o en minúsculas.
4. Las funciones F1-F12 del sistema se correlacionan con la tecla Esc seguida de una de las teclas de la fila superior de un teclado VTxxx. La tecla Esc seguida de una tecla con desplazamiento más una de las teclas de la fila superior de un teclado VTxxx se correlaciona con las funciones F13-F24.
5. Algunos sistemas cliente Telnet VTxxx utilizan Control-S y Control-Q con fines de control de flujo. Esto se denomina normalmente control de flujo XON/XOFF. Si utiliza un sistema cliente que tiene habilitado XON/XOFF, se recomienda no emplear los valores *CTLS y *CTLQ en la correlación de teclado.

Establecimiento del tipo de terminal virtual de red predeterminado

El parámetro de tipo de terminal virtual de red predeterminado especifica la modalidad que se utilizará cuando el servidor Telnet no pueda negociar uno de los tipos de terminal soportados.

Para establecer el valor de terminal virtual de red predeterminado en *VT100 para la modalidad VT100/VT220 o en *NVT para la modalidad de línea ASCII, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **TELNET** con el botón derecho del ratón y seleccione **Propiedades**.
3. Pulse la pestaña **General** y seleccione el valor adecuado junto a **Terminal virtual de red predeterminado**.
4. Pulse **Aceptar**.

Establecimiento de las tablas de correlación ASCII/EBCDIC

El servidor Telnet utiliza tablas de correlación de ASCII a EBCDIC y de EBCDIC a ASCII predeterminadas en función del parámetro de identificador de conjunto de caracteres codificados (CCSID) en los atributos de TCP/IP Telnet. De forma predeterminada se utiliza el juego de caracteres multinacional (*MULTINAT) DEC. También pueden utilizarse otros CCSID ASCII de 7 bits y 8 bits y cualquiera de los juegos de caracteres de sustitución nacionales DEC de 7 bits.

Nota: para la modalidad VT220 de 8 bits, las tablas de correlación no están disponibles. En esta modalidad, el sistema utiliza los juegos de caracteres de sustitución DEC. Para la modalidad VT220 de 7 bits, puede utilizar las tablas de correlación o los juegos de caracteres de sustitución DEC.

Hay tres formas de cambiar el valor predeterminado. Puede cambiar el parámetro CCSID, especificar valores distintos para las tablas de VTxxx de salida (TBLVTOUT) y de entrada (TBLVTIN) o cambiar las tablas predeterminadas para la sesión actual.

- Para cambiar los valores de las tablas, siga estos pasos:
 1. Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 2. Pulse **TELNET** con el botón derecho del ratón y seleccione **Propiedades**.
 3. Pulse la pestaña **Correlaciones**.
 4. Marque el recuadro de selección **Utilizar tablas de correlación especificadas** y pulse **Tablas**.
 5. Marque los recuadros de selección **Utilizar tabla de correlación de salida** y **Utilizar tabla de correlación entrante** para cambiar el parámetro CCSID.
 6. Pulse **Aceptar**.
 7. Pulse **Aceptar**.
- Para cambiar las tablas predeterminadas para la sesión actual, utilice el mandato de establecer tablas de correlación de VT (SETVTTBL).

Otra forma de acceder a este mandato consiste en utilizar la opción 2 del mandato CHGTCPTELN.

Conceptos relacionados

“Sesiones de cliente VTxxx” en la página 62

Las sesiones de cliente Telnet VTxxx proporcionan información sobre cómo utilizar este tipo de emulación para iniciar la sesión y utilizar aplicaciones en un sistema remoto que tiene una aplicación de servidor Telnet. Esta sección también facilita más información sobre la emulación VTxxx.

Referencia relacionada

“Teclado numérico” en la página 78

A continuación se especifican las teclas del teclado numérico auxiliar que normalmente transmiten los códigos de números, puntos, signos menos y comas.

“Teclado de edición” en la página 80

En esta tabla se muestran las teclas que transmiten los códigos de las teclas del teclado de edición.

“Opciones de emulación de VTxxx” en la página 68

Al utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet, hay varios procedimientos opcionales que puede llevar a cabo para personalizar el tipo de emulación. Puede visualizar la correlación de teclado actual y, a continuación, decidir si desea cambiarla. Asimismo, puede cambiar los caracteres de control al utilizar la modalidad de pantalla completa VT220.

“Valores de las teclas VTxxx por función 5250” en la página 82

En esta tabla se describen los valores de las teclas VT VTxxx función 5250.

Protección de Telnet con SSL

Con el protocolo SSL (capa de sockets seguros), puede establecer conexiones seguras entre la aplicación de servidor Telnet y los clientes Telnet que proporcionan la autenticación de uno o varios puntos finales de la sesión de comunicación. SSL también garantiza la privacidad e integridad de los datos que intercambian las aplicaciones del cliente y el servidor.

Conceptos relacionados

SSL (capa de sockets seguros)

Tareas relacionadas

“Resolución de problemas del servidor Telnet SSL” en la página 98

Aquí se describen los pasos detallados para la resolución de problemas del servidor de Capa de sockets seguros (SSL), con los códigos de retorno del sistema SSL y una lista de los problemas de SSL más habituales.

Configuración de SSL en el servidor Telnet

El factor más importante que debe tenerse en cuenta al habilitar SSL en el servidor Telnet es la confidencialidad de la información que se utiliza en las sesiones de cliente. Si la información es confidencial, o privada, se recomienda proteger el servidor Telnet con SSL.

Para configurar SSL en el servidor Telnet, siga estos pasos:

1. Instale el siguiente software para dar soporte a Telnet SSL y gestionar los certificados digitales:
 - IBM TCP/IP Connectivity Utilities para i5/OS (5761-TC1)
 - Digital Certificate Manager
 - IBM HTTP Server para i5/OS (5761-DG1)
 - IBM Developer Kit para Java (5761-JV1)
2. Compruebe que ha eliminado las restricciones de puerto y que ha permitido que se inicie SSL.
3. Asigne un certificado al servidor Telnet.
4. Habilite la autenticación de clientes para el servidor Telnet (paso opcional).
5. Habilite SSL en el servidor Telnet.
6. Inicie el servidor Telnet.

Conceptos relacionados

“Inicialización y negociación de SSL” en la página 38

Aquí puede encontrar información detallada sobre las interacciones entre clientes, servidores Telnet y la capa de sockets seguros (SSL).

Tareas relacionadas

“Resolución de problemas del servidor Telnet SSL” en la página 98

Aquí se describen los pasos detallados para la resolución de problemas del servidor de Capa de sockets seguros (SSL), con los códigos de retorno del sistema SSL y una lista de los problemas de SSL más habituales.

“Comprobación del estado del sistema” en la página 98

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

Eliminación de restricciones de puerto:

En los releases anteriores a V5R1, se empleaban restricciones de puerto ya que el soporte SSL (capa de sockets seguros) no estaba disponible para Telnet. Ahora puede especificar si debe iniciarse el soporte SSL, no SSL o ambos. Por consiguiente, las restricciones de puerto ya no son necesarias.

Si ha definido restricciones de puerto en releases anteriores, debe eliminar las restricciones de puerto para utilizar el parámetro SSL. A fin de eliminar las restricciones de puerto, siga estos pasos:

1. Para listar las restricciones de puerto, siga estos pasos:
 - a. Inicie System i Navigator y expanda *su sistema* → **Red**.
 - b. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Propiedades**.
 - c. Pulse la pestaña **Restricciones de puerto**.
2. Para eliminar la restricción de puerto, continúe realizando estos pasos:
 - a. Seleccione la restricción de puerto que desea eliminar.
 - b. Pulse **Eliminar**.
 - c. Pulse **Aceptar**.

El valor predeterminado es iniciar SSL en el puerto 992 y no SSL en el puerto 23. El servidor Telnet utiliza la entrada de la tabla de servicio de Telnet para obtener el puerto no SSL y Telnet SSL para obtener el puerto SSL.

Tareas relacionadas

“Asignación de un certificado al servidor Telnet”

Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

Asignación de un certificado al servidor Telnet:

Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

Antes de poder configurar el servidor Telnet para utilizar SSL, debe instalar los programas de prerequisite y configurar los certificados digitales en el sistema.

1. Inicie IBM Digital Certificate Manager (DCM).

Nota: si alberga dudas a la hora de cumplimentar un formulario determinado mientras utiliza DCM, seleccione el signo de interrogación (?) situado en la parte superior de la página para acceder a la ayuda en línea.

2. En el marco de navegación, pulse **Seleccionar un almacén de certificados** y seleccione ***OBJECTSIGNING** o ***SYSTEM** como el almacén de certificados que debe abrirse.
3. Especifique la contraseña para el almacén de certificados y pulse **Continuar**.
4. Una vez renovado el marco de navegación, seleccione **Gestionar certificados** para visualizar una lista de tareas.
5. En la lista de tareas, seleccione **Asignar certificado** para visualizar una lista de los certificados del almacén de certificados actual.
6. Seleccione un certificado de la lista y pulse **Asignar a las aplicaciones** para visualizar una lista de las definiciones de aplicaciones del almacén de certificados actual.
7. Seleccione Telnet en la lista y pulse **Continuar**. Aparecerá una página con un mensaje de confirmación de la asignación seleccionada o un mensaje de error si se ha producido un problema.

Nota: la base de datos de claves de los clientes de System i Access para Windows debe contener una copia de los certificados de Autoridad certificadora (CA) necesarios. En este caso, en la base de datos de claves debe existir un certificado CA para el certificado que asigne a la aplicación de servidor Telnet. La base de datos de claves viene preconfigurada con copias de certificados CA de prácticamente todas las CA públicas más conocidas. No obstante, si opta por asignar un certificado al servidor Telnet que emite una CA local, deberá añadir una copia del certificado CA local a la base de datos de claves del cliente. Si desea saber cómo se añade una copia de un certificado CA local, consulte el Paso 5: habilitación de SSL en el cliente Telnet del tema Caso práctico Telnet: proteger Telnet con SSL - Detalles de configuración.

El servidor Telnet da soporte a la autenticación de clientes como componente opcional en la configuración de SSL. La autenticación de clientes se produce cuando el servidor verifica la identidad del cliente mediante el certificado de cliente pasado a la aplicación de servidor.

Qué hacer a continuación:

Habilite la autenticación de clientes para el servidor Telnet (paso opcional) o habilite SSL en el servidor Telnet.

Conceptos relacionados

Planificación de SSL

“Detalles de configuración para proteger Telnet con SSL” en la página 11

Aquí se describen los pasos de configuración detallados para proteger Telnet con la Capa de sockets seguros (SSL).

Tareas relacionadas

“Eliminación de restricciones de puerto” en la página 34

En los releases anteriores a V5R1, se empleaban restricciones de puerto ya que el soporte SSL (capa de sockets seguros) no estaba disponible para Telnet. Ahora puede especificar si debe iniciarse el soporte SSL, no SSL o ambos. Por consiguiente, las restricciones de puerto ya no son necesarias.

Configuración de certificados por primera vez

Inicio de Digital Certificate Manager

“Habilitación de la autenticación de clientes para el servidor Telnet” en la página 36

El servidor Telnet da soporte a la autenticación de certificados de clientes Telnet. Esto significa que durante la negociación de la capa de sockets seguros (SSL), el servidor no solo generará un certificado de servidor para el cliente, sino que de forma opcional puede comprobar la validez de un certificado de cliente en función de cómo esté configurado el gestor de certificados digitales (DCM).

“Habilitación de SSL en el servidor Telnet” en la página 38

Siga estos pasos para aprender a habilitar la Capa de sockets seguros (SSL) en el servidor Telnet.

“Comprobación del estado del sistema” en la página 98

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

Habilitación de la autenticación de clientes para el servidor Telnet:

El servidor Telnet da soporte a la autenticación de certificados de clientes Telnet. Esto significa que durante la negociación de la capa de sockets seguros (SSL), el servidor no solo generará un certificado de servidor para el cliente, sino que de forma opcional puede comprobar la validez de un certificado de cliente en función de cómo esté configurado el gestor de certificados digitales (DCM).

El DCM permite configurar si se requieren certificados de cliente SSL para las sesiones Telnet.

Para activar este soporte, el administrador del sistema indica cómo se maneja el soporte SSL. Utilice el panel General de Propiedades de Telnet en System i Navigator para indicar si se iniciará el soporte SSL, no SSL o ambos cuando se inicie el servidor Telnet. De forma predeterminada, siempre se inicia el soporte SSL y el soporte no SSL.

El administrador del sistema puede indicar si el sistema requiere la autenticación de clientes SSL para todas las sesiones Telnet. Cuando el soporte SSL está activo y el sistema requiere la autenticación del cliente, la presencia de un certificado de cliente válido significa que el cliente es de confianza.

El sistema aplica las variables RFC 4777 negociadas y las variables de los programas de salida de usuario Telnet tras superar los controles SSL.

Para actualizar las especificaciones de aplicación en IBM DCM y habilitar la autenticación de clientes para el servidor Telnet, siga estos pasos:

1. Inicie IBM DCM. Si necesita obtener o crear certificados, o bien configurar o modificar el sistema de certificados, hágalo ahora.
2. Pulse **Seleccionar un almacén de certificados**.
3. Seleccione ***SYSTEM**. Pulse **Continuar**.
4. Especifique la contraseña adecuada para el almacén de certificados ***SYSTEM**. Pulse **Continuar**.
5. Cuando vuelva a cargarse el menú de navegación izquierdo, expanda **Gestionar aplicaciones**.
6. Pulse **Actualizar definición de aplicación**.
7. En el panel siguiente, seleccione la aplicación **Servidor**. Pulse **Continuar**.
8. Seleccione **Servidor Telnet TCP/IP i5/OS**.
9. Pulse **Actualizar definición de aplicación**.
10. En la tabla que aparece, seleccione **Sí** para requerir la autenticación de clientes.
11. Pulse **Aplicar**.
12. El DCM vuelve a cargar la página Actualizar definición de aplicación con un mensaje de confirmación. Cuando la recarga de DCM haya terminado de recargar y actualizar la definición de aplicación para el servidor Telnet, pulse **Realizado**.

Tareas relacionadas

“Asignación de un certificado al servidor Telnet” en la página 34

Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

Inicio de Digital Certificate Manager

“Habilitación de SSL en el servidor Telnet” en la página 38

Siga estos pasos para aprender a habilitar la Capa de sockets seguros (SSL) en el servidor Telnet.

Información relacionada



Configuración de DCM

Ejemplo: habilitación de la autenticación de clientes para una sesión PC5250:

Cuando haya configurado la Capa de sockets seguros (SSL) para el servidor Telnet y haya especificado utilizar la autenticación de clientes, se solicita a los usuarios que proporcionen un certificado de cliente válido y de confianza al servidor Telnet para cada intento de conexión.

Para que la autenticación de clientes funcione, antes los clientes deben crear un certificado de usuario e importar ese certificado en la base de datos de la Gestión de claves IBM.

Creación de un certificado de usuario en el DCM

1. Inicie IBM Digital Certificate Manager (DCM). Si necesita obtener o crear certificados, o bien configurar o modificar el sistema de certificados, hágalo ahora.
2. Expanda **Crear certificado**.
3. Seleccione **Certificado de usuario**. Pulse **Continuar**.
4. Complimente el formulario Certificado de usuario. Solo hay que complimentar los campos marcados como "Necesario". Pulse **Continuar**.
5. En función del navegador que utilice, se le solicitará que genere un certificado que se cargará en el navegador. Siga las indicaciones que le facilita el navegador.
6. Cuando se vuelva a cargar la página Crear certificado de usuario, pulse **Instalar certificado**. De este modo se instalará el certificado en el navegador.
7. Exporte el certificado al sistema. Debe almacenar el certificado en un archivo protegido mediante contraseña.

Nota: es preciso utilizar Microsoft Internet Explorer 5 o Netscape 4.5 para emplear las funciones de exportar e importar.

Importación del certificado en la herramienta Gestión de claves IBM

1. Pulse **Inicio** → **Programas** → **IBM System i Access para Windows** → **System i Access para Windows Propiedades**.
2. Seleccione la pestaña **Sockets Seguros**.
3. Pulse **Gestión de claves IBM**.
4. Se le solicitará la contraseña de la base de datos de claves. Salvo que antes haya cambiado la contraseña predeterminada por otra distinta, especifique ca400. Aparece un mensaje de confirmación. Pulse **Aceptar**.
5. En el menú desplegable, seleccione **Certificados personales**.
6. Pulse **Importar**.
7. En la pantalla Importar clave, especifique el nombre de archivo y la vía de acceso del certificado. Pulse **Aceptar**.
8. Especifique la contraseña del archivo protegido. Es la misma contraseña que ha creado en el paso 7 del procedimiento de creación de un certificado de usuario en el DCM. Pulse **Aceptar**. Cuando el certificado se haya añadido correctamente a los certificados personales en Gestión de claves IBM, podrá utilizar el emulador PC5250 o cualquier otra aplicación Telnet.

Inicio de una sesión de emulador PC5250 desde System i Navigator

1. Abra System i Navigator.
2. Pulse con el botón derecho del ratón el nombre del sistema que ha configurado para la autenticación de clientes de Telnet.
3. Seleccione **Emulador de pantalla**.
4. Seleccione el menú Comunicación y, a continuación, seleccione **Configurar**.
5. Pulse **Propiedades**.
6. En el diálogo Conexión, seleccione **Utilizar Capa de sockets seguros (SSL)**.

7. Si tiene más de un certificado de cliente, seleccione **Seleccionar certificado al conectarse** o **Utilizar valor predeterminado** para determinar qué certificado de cliente se utilizará.
8. Pulse **Aceptar**.
9. Pulse **Aceptar**.

Tareas relacionadas

Inicio de Digital Certificate Manager

Configuración de DCM

Información relacionada



Configuración de DCM

Habilitación de SSL en el servidor Telnet:

Siga estos pasos para aprender a habilitar la Capa de sockets seguros (SSL) en el servidor Telnet.

1. Abra System i Navigator.
2. Expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
3. Pulse **Telnet** con el botón derecho del ratón.
4. Seleccione **Propiedades**.
5. Seleccione la pestaña **General**.
6. Elija una de estas opciones para el soporte SSL:
 - **Solo seguro**
Seleccione esta opción para permitir únicamente las sesiones SSL con el servidor Telnet.
 - **Solo no seguro**
Seleccione esta opción para prohibir las sesiones seguras con el servidor Telnet. Los intentos de conexión con un puerto SSL no se ejecutarán correctamente.
 - **Seguro y no seguro**
Seleccione esta opción para permitir las sesiones seguras y no seguras con el servidor Telnet.

Tareas relacionadas

“Asignación de un certificado al servidor Telnet” en la página 34

Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

“Habilitación de la autenticación de clientes para el servidor Telnet” en la página 36

El servidor Telnet da soporte a la autenticación de certificados de clientes Telnet. Esto significa que durante la negociación de la capa de sockets seguros (SSL), el servidor no solo generará un certificado de servidor para el cliente, sino que de forma opcional puede comprobar la validez de un certificado de cliente en función de cómo esté configurado el gestor de certificados digitales (DCM).

“Inicio del servidor Telnet” en la página 21

El servidor Telnet activo tiene una o más instancias de cada uno de los siguientes trabajos en ejecución en el subsistema QSYSWRK: QTVTELNET y QTVDEVICE.

Inicialización y negociación de SSL

Aquí puede encontrar información detallada sobre las interacciones entre clientes, servidores Telnet y la capa de sockets seguros (SSL).

¿Qué ocurre durante la inicialización de SSL?

El servidor Telnet intenta inicializar SSL cada vez que se inicia el servidor. Durante la inicialización, el servidor Telnet comprueba la información del certificado de la aplicación QIBM_QTV_TELNET_SERVER. Puede saber que la inicialización de SSL se ha realizado satisfactoriamente cuando en el subsistema

QSYSWRK aparece más de un trabajo QTVTELNET activo. Evidentemente, si el campo de número de trabajos de servidor por iniciar en la página General de las propiedades de Telnet está establecido en 1, solo verá un trabajo QTVTELNET activo.

El servidor Telnet no inicializa SSL cuando se tiene un puerto Telnet SSL restringido. El servidor Telnet envía el mensaje TCP2550 El acceso al puerto 92 está restringido a las anotaciones del trabajo QTVTELNET y a la cola de mensajes QSYSOPR.

Cuando un certificado es incorrecto o ha caducado, la inicialización es anómala y el servidor Telnet envía el mensaje CPDBC nn a las anotaciones del trabajo QTVTELNET.

Aunque en la aplicación QIBM_QTV_TELNET_SERVER no haya ningún certificado o haya un certificado caducado, el servidor Telnet inicializa satisfactoriamente SSL. No obstante, la negociación SSL es anómala cuando el cliente intenta conectarse al servidor Telnet. El servidor Telnet envía el mensaje CPDBC nn a las anotaciones del trabajo QTVTELNET.

¿Qué ocurre durante la reinicialización de SSL?

Cuando el certificado de la aplicación QIBM_QTV_TELNET_SERVER cambia, el servidor Telnet reinicializa SSL si se produce un cambio en el DCM. Esto significa que puede restaurar un certificado caducado o añadir o eliminar certificados de usuario y Telnet tomará los cambios automáticamente. El proceso es el mismo que en la inicialización de SSL. Las nuevas sesiones de cliente Telnet SSL utilizan el nuevo certificado. Las sesiones de cliente Telnet SSL que ya se han establecido utilizan el certificado original. Después de haber finalizado y vuelto a iniciar el servidor Telnet, todas las sesiones de cliente Telnet SSL utilizarán el nuevo certificado.

Si la reinicialización de SSL es anómala, las sesiones SSL ya establecidas utilizan el certificado original que se inicializó cuando se arrancó el servidor y se bloquea la conexión de las sesiones nuevas. La próxima vez que se inicie el servidor Telnet, la inicialización de SSL será anómala, aunque seguirá habiendo un escucha SSL activo. Sin embargo, ninguna conexión SSL nueva será satisfactoria hasta que un cambio en el DCM fuerce al servidor Telnet a reinicializarse correctamente.

¿Qué ocurre durante la negociación SSL?

Cuando el cliente Telnet SSL se conecta al puerto TCP 992 se intenta realizar una negociación SSL con el servidor. Mientras el cliente se está conectando al servidor, muestra números de estado o mensajes en la barra de estado de la ventana abierta.

Si la negociación SSL es anómala, no se establece la sesión Telnet. Por ejemplo, en la ventana del cliente Telnet SSL no aparecerá una pantalla de inicio de sesión. Consulte la guía del usuario o la ayuda en línea del cliente Telnet SSL para obtener información sobre números de estado o mensajes concretos. El servidor Telnet envía el mensaje CPDBC nn a las anotaciones del trabajo QTVTELNET.

Tareas relacionadas

“Configuración de SSL en el servidor Telnet” en la página 33

El factor más importante que debe tenerse en cuenta al habilitar SSL en el servidor Telnet es la confidencialidad de la información que se utiliza en las sesiones de cliente. Si la información es confidencial, o privada, se recomienda proteger el servidor Telnet con SSL.

“Comprobación de las anotaciones de trabajo de Telnet” en la página 99

Cuando la inicialización y negociación de la capa de sockets seguros (SSL) es anómala el servidor Telnet envía mensajes de diagnóstico CPDBC *nn* al trabajo QTVTELNET.

Gestión del servidor Telnet

Aprenda a trabajar con el servidor Telnet y cómo utilizar los programas de salida para controlar el acceso de usuario.

El servidor Telnet permite a un usuario TCP/IP de un cliente Telnet remoto iniciar la sesión y ejecutar aplicaciones en la plataforma System i. El soporte de servidor Telnet negocia la transmisión de datos con la aplicación de cliente Telnet remoto para diversas modalidades operativas.

Las aplicaciones de cliente y servidor Telnet negocian estas modalidades operativas. Las funciones disponibles dependen del tipo de terminal que se negocia.

Con mínimos cambios en los valores del sistema, el servidor Telnet puede dar soporte a las conexiones Telnet cuando se inicia TCP/IP. Para todas las modalidades operativas salvo la modalidad de línea ASCII, el sistema automáticamente envía la pantalla de inicio de sesión cuando se efectúa una conexión Telnet. En el caso de la modalidad de línea ASCII, debe haber activa una aplicación de cliente que visualice datos.

Configuración de sesiones de impresora Telnet

Este tema contiene instrucciones para conectar a impresoras en el sistema desde ubicaciones remotas de la red.

Debe crear un dispositivo de impresora virtual 3812 o 5553 para utilizar la emulación de impresora Telnet. Este dispositivo es necesario para generar las corrientes de datos de impresora que se envían para la sesión de impresora. Las impresoras empleadas con la impresión Telnet pueden estar conectadas al PC o a la misma red que el PC. Las sesiones de impresora Telnet negocian con un cliente Telnet remoto de un sistema que soporte la emulación de impresora Telnet.

Las sesiones de impresora Telnet entregan la corriente de datos de impresora entre los dos sistemas como datos EBCDIC o ASCII, en función de las preferencias del cliente que efectúa la petición.

Las sesiones de impresora Telnet están activas inmediatamente después de la inicialización de Telnet. Las funciones de impresión no requieren perfiles de usuario ni contraseñas. Sin embargo, si la seguridad lo requiere, puede emplear programas de punto de salida de Telnet para bloquear el inicio de las sesiones de impresora.

Al utilizar las sesiones de impresora Telnet, todos los datos de impresión se guardan en spool en una cola de transcriptor de impresora para su impresión. No puede imprimirse directamente en un dispositivo de impresión. Cuando se utilizan los mandatos de archivo de impresora para crear un archivo de impresora (CRTPRTF), cambiar un archivo de impresora (CHGPRTF) y sobrescribir un archivo de impresora (OVRPRTF), se debe utilizar el parámetro SPOOL (*YES) predeterminado. Además, Telnet establece el nombre del transcriptor de impresora o de la cola de salida en el mismo nombre que el de la impresora.

Para configurar las sesiones de impresora Telnet, siga estos pasos:

1. Compruebe que la pila TCP está activa. Si no lo está, emita el mandato STRTCP para iniciar la pila TCP.
2. Inicie el servidor Telnet. Consulte Inicio del servidor Telnet
3. Establezca el número de dispositivos virtuales. Consulte Establecimiento del número de dispositivos virtuales.
4. Establezca el parámetro de tiempo de vida de la sesión Telnet. Consulte Establecimiento del parámetro de tiempo de vida de la sesión Telnet.
5. Cree controladores y dispositivos virtuales. Consulte Creación de controladores y dispositivos virtuales.
6. Active el subsistema QSPL. Consulte Activación del subsistema QSPL.
7. Pruebe la configuración con un archivo de impresora de prueba.
8. Imprima un archivo mediante una sesión de impresora Telnet.

Nota: el subsistema QSYSWRK se inicia cuando se inicia la pila TCP.

Requisitos para las sesiones de impresora Telnet

Si piensa utilizar sesiones de impresora Telnet, consulte con el proveedor del cliente Telnet si soporta la función de sesión de impresora.

Los siguientes clientes soportan la función de sesión de impresora:

- IBM System i Access para Windows
- Personal Communications
- IBM Host OnDemand

Las sesiones de impresora Telnet soportan las siguientes impresoras EBCDIC genéricas:

- IBM-3812-1 para el juego de caracteres de un solo byte (SBCS)
- IBM-5553-B01 para el juego de caracteres de doble byte (DBCS)

Puede especificar cualquiera de los tipos de dispositivo genérico solicitando la función Host Print Transform (HPT) y seleccionando el tipo de fabricación específico. Si está utilizando System i Access para Windows, puede utilizar la tabla de definición de impresoras (PDT) o la interfaz de dispositivo gráfico (GDI) para definir un hardware específico. El sistema envía la corriente de datos de impresora en ASCII.

Mejora de la API del sistema

La API del sistema Recuperar descripción de dispositivo (QDCRDEVD) proporciona la dirección IP del cliente Telnet. Hay varios campos para los dispositivos de pantalla (*DSP) e impresión (*PRT): Protocolo de red, Dirección del protocolo de red y Dirección IP en formato decimal con puntos. Estos campos proporcionan a la aplicación información a nivel de sockets sobre la conexión TCP/IP del cliente.

Soporte de impresión del servidor Telnet para el cliente System i Access para Windows Telnet:

El cliente IBM System i Access para Windows proporciona emulación de pantalla, cliente Telnet 5250 de pantalla completa y emulación de impresora.

Para iniciar una sesión de impresora, seleccione una de las opciones siguientes:

1. **System i Access para Windows** → **Emuladores** → **Iniciar o configurar sesión** en el menú de inicio del programa.
2. Seleccione el nombre de un modelo System i al que desee conectarse.
3. Utilice el campo **ID de estación de trabajo** para solicitar específicamente un nombre de dispositivo virtual. Puede dejar el campo en blanco y el servidor Telnet seleccionará automáticamente un dispositivo virtual compatible (QPADEVxxxx) y devolverá el nombre en el panel de control de impresora.
4. Para el tipo de emulación:
 - a. Seleccione una impresora.
 - b. Pulse el recuadro **Configuración** para iniciar el diálogo de configuración de emulación de impresora PC5250

En el diálogo de configuración, puede configurar aspectos tales como el font, la cola de mensajes y la función de host HPT. Las funciones de host HPT incluyen la transformación de datos de impresión en ASCII en el sistema operativo i5/OS. Si se selecciona la transformación de impresión en host (HPT) se habilitan otros elementos de configuración, como por ejemplo las opciones de selección del modelo de impresora y la bandeja del medio. También existe una opción de reconexión automática y una opción para alterar temporalmente el número de puerto Telnet predeterminado (23).

Para finalizar la sesión, pulse **Comunicación** → **Desconectar desde la barra de menús**.

Finalización de la sesión del servidor Telnet

Al finalizar una sesión Telnet, permite que el dispositivo virtual esté disponible para una nueva sesión Telnet.

Cuando está conectado a un sistema, al finalizar la sesión no necesariamente se finaliza la sesión del servidor Telnet. El dispositivo de impresora o pantalla virtual sigue activo y ninguna otra sesión Telnet puede utilizarlo. Para finalizar la sesión del servidor, debe especificar una tecla o secuencia de teclas para colocar el cliente Telnet en la modalidad de mandatos local. A continuación, puede especificar el mandato para finalizar la sesión. Utilice una de las secuencias de teclas siguientes para finalizar una sesión de servidor Telnet.

- En el sistema operativo i5/OS, pulse la tecla **Atención** y, a continuación, seleccione la opción 99 (Finalizar sesión Telnet - QUIT).
- En la mayor parte de los demás sistemas operativos, finalice la sesión.

Si no sabe qué tecla o secuencia de teclas hace que el cliente entre en la modalidad de mandatos, consulte con el administrador del sistema o repase la documentación del cliente Telnet.

También puede utilizar el parámetro de finalización de conexión (ENDCNN) del mandato SIGNOFF para finalizar la sesión del sistema y finalizar la conexión Telnet. Por ejemplo, SIGNOFF ENDCNN(*YES) le devuelve al sistema cliente (si solo ha establecido una sesión Telnet). Si ha establecido más de una sesión Telnet, el mandato le devuelve al sistema anterior.

Tareas relacionadas

“Inicio del servidor Telnet” en la página 21

El servidor Telnet activo tiene una o más instancias de cada uno de los siguientes trabajos en ejecución en el subsistema QSYSWRK: QTVTELNET y QTVDEVICE.

Finalización de trabajos del gestor de dispositivos

En ocasiones es necesario finalizar y reiniciar los trabajos del gestor de dispositivos; por ejemplo, al aplicar un arreglo temporal del programa (PTF) al programa. En este tema se proporcionan instrucciones para finalizar y reiniciar trabajos del gestor de dispositivos.

Al iniciar y detener Telnet, se finalizan los trabajos del servidor Telnet, pero no los trabajos del gestor de dispositivos. Ello se debe a que la naturaleza de los trabajos del gestor de dispositivos requiere que estén en ejecución todo el tiempo, o como mínimo hasta que se vuelva a reiniciar el sistema. Para establecer un ciclo en los trabajos del gestor de dispositivos, debe seguir los pasos especiales 2 y 3. Luego, la próxima vez que se inicie Telnet, este verá que no hay ningún trabajo del gestor de dispositivos en ejecución y los iniciará. Siga estos pasos para finalizar los trabajos del gestor de dispositivos:

1. Finalice los trabajos del servidor Telnet activos con el procedimiento siguiente:
 - a. Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. Pulse **Telnet** con el botón derecho del ratón y seleccione **Detener**.
2. Busque todos los trabajos del gestor de dispositivos Telnet activos con el procedimiento siguiente:
 - a. Inicie System i Navigator y expanda *su sistema* → **Gestión de trabajo**.
 - b. Seleccione **Trabajos activos**.
 - c. Busque QTVDEVICE.
3. Finalice todos los trabajos que haya encontrado en el paso 2 pulsándolos con el botón derecho del ratón y seleccionando **Suprimir/finalizar**. Debe esperar a que finalicen todos los trabajos antes de llevar a cabo el paso siguiente.
4. Inicie los trabajos del servidor Telnet y del gestor de dispositivos en el panel Suprimir/finalizar. Puede que los dispositivos virtuales Telnet que sigan en proceso de finalización cuando hayan finalizado todos los trabajos del gestor de dispositivos queden inaccesibles hasta que se vuelva a llevar a cabo la operación de reiniciar.

Utilización de programas de punto de salida de Telnet

Con el uso de los programas de salida, un programador con experiencia puede crear procesos personalizados durante una aplicación. Si el servidor Telnet encuentra un programa registrado en uno de los puntos de salida del servidor, llama a ese programa utilizando los parámetros definidos por el punto de salida.

Un *punto de salida* es un punto específico del programa Telnet donde el control puede pasar a un programa de salida. Un *programa de salida* es un programa al que el punto de salida pasa el control.

Para cada uno de los puntos de salida, hay una interfaz de programación asociada, denominada **interfaz de punto de salida**. El punto de salida utiliza esta interfaz para pasar información entre la aplicación Telnet y el programa de salida. Cada uno de los puntos de salida tiene un nombre exclusivo. Cada interfaz de punto de salida tiene un nombre con un formato de punto de salida que define cómo se pasa la información entre la aplicación Telnet y el programa de salida escrito por el cliente.

Distintos puntos de salida pueden compartir la misma interfaz de punto de salida. En este caso, varios puntos de salida pueden llamar a un único programa de salida.

Rendimiento de los puntos de salida

El tiempo que tardará en responder el servidor Telnet a la petición de inicio de sesión incluye el tiempo que emplee el servidor en llamar al programa de salida QIBM_QTG_DEVINIT, procesarlo y devolverlo. Si el programa de salida ha de realizar un proceso notable, su repercusión en el rendimiento puede suponer que para establecer la sesión tenga que esperar más tiempo. Si desea modificar el valor de tiempo de espera predeterminado de 60 segundos para los programas de salida de usuario, puede emplear el mandato ADDEXITPGM para añadir datos de usuario que se leen como el valor de tiempo de espera. En el ejemplo siguiente, el parámetro PGMDTA altera temporalmente el tiempo de espera predeterminado de 60 segundos por el de 10 segundos:

```
ADDEXITPGM EXITPNT(QIBM_QTG_DEVINIT) FORMAT(INIT0100)
PGMNBR(1) PGM(USEREXIT/DEVINIT2) REPLACE(*YES)
CRTEXTIPNT(*NO) PGMDTA(*JOB *CALC 10)
```

Una vez establecido el programa Telnet mediante una ventana de inicio de sesión u otro modelo System i, el rendimiento no se ve afectado. Cuando esto se produce, el programa de salida ya no está en la vía de Telnet. Las sesiones Telnet establecidas no experimentan ningún retardo debido al programa de salida QIBM_QTG_DEVINIT.

No existe ninguna repercusión en el rendimiento visible por el usuario que esté asociada a la desconexión de la sesión. Desconectar significa finalizar la sesión de emulación de terminal, no finalizar la sesión y volver al panel de inicio de sesión. Si se desconecta, se llama al programa de salida QIBM_QTG_DEVTERM, que lleva a cabo el proceso de desconexión de la sesión. Los usuarios no pueden verlo, ya que se produce después de que se interrumpa la conexión.

Gestión de trabajos

Puede resolver problemas clave en relación con la gestión de trabajos mediante un programa de salida de Telnet. Entre estos problemas figuran la posibilidad de solicitar descripciones de dispositivos distintas de QPADEVxxxx, permitir el control de la gestión de trabajos de los trabajos interactivos de las estaciones de trabajo virtuales y direccionar estos trabajos a subsistemas específicos.

Direccionamiento de subsistemas y selección de nombres de dispositivo

Los usuarios pueden disponer de mejores nombres de dispositivo virtual Telnet y configurar sus subsistemas interactivos para subdividir el trabajo. Para ello se utiliza el mandato Añadir entrada de estación de trabajo (ADDWSE). Este mandato permite especificar a qué dispositivos debe o no asignar un subsistema un nombre concreto de dispositivos de terminales virtuales.

El mandato siguiente hace que se asigne QINTER a todas las estaciones de trabajo QPADEV*, lo que significa que todos estos dispositivos se direccionan al subsistema QINTER:

```
ADDWSE SBS(D(QINTER) WRKSTN(QPADEV*) AT(*SIGNON)
```

El mandato siguiente hace que QINTER no se asigne a todas las estaciones de trabajo QPADEV*, lo que significa que estos dispositivos pueden asignarse a otro subsistema:

```
ADDWSE SBS(D(QINTER) WRKSTN(QPADEV*) AT(*ENTER)
```

Los usuarios pueden desarrollar sus propios convenios de denominación de dispositivos para subdividir el trabajo. Por ejemplo, un tipo de subdivisión consiste en direccionar determinados dispositivos a subsistemas relacionados con el soporte de idioma nacional (NLS) en dos ubicaciones.

Ejemplo

Los dos usuarios se encuentran en Chicago y Nueva York. Los usuarios se asignan a los subsistemas CHICAGO o NEWYORK, según su ubicación geográfica. Las características de este ejemplo son:

- Las direcciones IP de Chicago empiezan por 1.2.3.*.
- Las direcciones IP de Nueva York empiezan por 2.3.4.*.
- Para que todas las sesiones Telnet de Chicago se ejecuten en el subsistema CHICAGO se emplea el programa de salida de usuario. El programa de salida crea un nombre de dispositivo virtual que empieza por 'CHICAGO' para todas las conexiones Telnet desde 1.2.3. El programa de salida de usuario también crea un nombre de dispositivo virtual que empieza por 'NEWYORK' para todas las conexiones desde 2.3.4.
- El programa de salida de usuario asigna el nombre de dispositivo virtual 'CHICAGO01' para la dirección IP 1.2.3.47. El programa asigna el nombre de dispositivo virtual 'NEWYORK01' para la dirección IP 2.3.4.48. El programa adjunta una parte variable ('01', '02', etc.) al nombre raíz 'CHICAGO' y comprueba que el dispositivo todavía no se utiliza antes de asignarlo al usuario actual.

Para asegurarse de que el dispositivo virtual CHICAGO01 vaya al subsistema Chicago y el dispositivo virtual NEWYORK01 vaya al subsistema Nueva York, configure las entradas de las estaciones de trabajo como se indica a continuación:

Nota: Al utilizar los ejemplos de código, acepta los términos de la Información de licencia de código y declaración de limitación de responsabilidad.

```
ADDWSE SBS(D(QINTER) WRKSTN(CHICAGO*) AT(*ENTER)
ADDWSE SBS(D(QINTER) WRKSTN(NEWYORK*) AT(*ENTER)
ADDWSE SBS(D(CHICAGO) WRKSTN(CHICAGO*) AT(*SIGNON)
ADDWSE SBS(D(NEWYORK) WRKSTN(NEWYORK*) AT(*SIGNON)
```

Conceptos relacionados

“Control del acceso mediante Telnet” en la página 17

Tenga en cuenta las consideraciones sobre seguridad si desea que los clientes Telnet puedan acceder al sistema.

Programa de salida de inicialización de dispositivos

La aplicación de servidor Telnet incluye puntos de salida que permiten conectarse a la lógica de inicio de sesión y finalización de Telnet. Puede utilizar los mandatos Trabajar con información de registro (WRKREGINF) o Añadir programa de salida (ADDEXITPGM) para asociar el programa de salida personalizado a un punto de salida.

Si el servidor Telnet encuentra un programa registrado en uno de los puntos de salida del servidor, llama a ese programa utilizando los parámetros definidos por el punto de salida. Estos parámetros incluyen elementos como la dirección IP, el nombre de usuario y el nombre de dispositivo virtual. A continuación el programa de salida personalizado procesa la información. Por ejemplo, anota un mensaje y devuelve el control al servidor Telnet. De retorno, el programa de salida indica al sistema si debe aceptar o rechazar este cliente y las alteraciones temporales de usuario o contraseña opcionales.

Cada uno de los puntos de salida tiene un nombre y una interfaz de punto de salida. La interfaz de punto de salida es una lista de parámetros de entrada y salida que el servidor Telnet intercambia con el programa de salida. Hay dos puntos de salida para el servidor Telnet:

- QIBM_QTG_DEVINIT
- QIBM_QTG_DEVTERM

Tabla 4. Grupo de parámetros obligatorios

No.	Interfaz de punto de salida	¿Entrada o salida?	Parámetros
1	Información de descripción del usuario	E/S	Char(*)
2	Información de descripción del dispositivo	E/S	Char(*)
3	Información de descripción de la conexión	Entrada	Char(*)
4	Opciones de entorno	Entrada	Char(*)
5	Longitud de las opciones de entorno	Entrada	Binary(4)
6	Permitir conexión	Salida	Char(1)
7	Permitir inicio de sesión automático	Salida	Char(1)

Nombre de miembro QSYSINC: ETGDEVEX
 Nombre de punto de salida: QIBM_QTG_DEVINIT
 Nombre con un formato de punto de salida: INIT0100

El servidor Telnet permite de forma opcional seleccionar o establecer el nombre de dispositivo que se empleará a lo largo de la sesión Telnet, y permite que un cliente Telnet eluda la inicialización de dispositivos tradicional. Los administradores pueden controlar estas funciones nuevas mediante el uso de un programa de salida nuevo que opcionalmente se inicia inmediatamente después del establecimiento de la sesión de cliente. Se proporcionan al programa de salida varios parámetros para utilizarse en el proceso de decisión; el programa de salida puede establecer o cambiar diversos parámetros antes de volver al servidor Telnet. Se puede registrar de forma opcional un segundo programa de salida que se inicie inmediatamente antes de que termine la sesión. Se puede utilizar este segundo programa de salida para la auditoría de sesiones o la gestión de dispositivos virtuales.

Formato de punto de salida de Telnet INIT0100: grupo de parámetros necesarios:

Aquí se proporciona una descripción detallada del grupo de parámetros necesarios.

Información de descripción del usuario

E/S; CHAR(*)

Información sobre el usuario que el sistema emplea en el proceso de inicio de sesión automático.

Información de descripción del dispositivo

E/S; CHAR(*)

Información que el sistema emplea para crear o cambiar el dispositivo que utiliza para esta sesión Telnet.

Información de descripción de la conexión

E/S; CHAR(*)

Información sobre la conexión del cliente que el programa de salida puede utilizar.

Opciones de entorno

ENTRADA; CHAR(*)

Matriz que contiene todas las opciones de entorno RFC 4777 negociadas por el cliente. Tendrán el formato exacto que tenían cuando se recibieron del cliente y que especifica RFC 4777. Por lo general, la matriz constará de uno o más pares de nombres de variable de entorno y valores asociados. La especificación RFC establece que cada nombre de variable siempre estará precedido por X'01' o X'03' según si es una variable definida por RFC 4777 (VAR) o una variable definida por una aplicación específica (USERVAR). Si se asocia un valor con una variable VAR (o USERVAR), ese valor aparecerá junto a la matriz con el carácter de valor (VALUE) X'01' definido por la especificación RFC 1572 antepuesto. Esta secuencia de pares de variable y valor (VAR/VALUE) se repetirá hasta un máximo de 1024 bytes de datos de negociación en total. La especificación RFC 4777 y las especificaciones RFC de negociación de Telnet más generales también permiten que aparezcan caracteres de control dentro de los nombres de variables VAR/USERVAR o de sus valores asociados. Ello está permitido mediante el uso del carácter ESC X'02' y las reglas que se aplican cuando el propio carácter ESC o los caracteres de control Telnet IAC deben aparecer en la secuencia de negociación. Consulte el documento RFC 1572 para obtener una descripción más completa de las reglas de escape de los caracteres de control. Mientras que el almacenamiento intermedio de opciones de entorno muestra las negociaciones efectuadas por el cliente, con las contraseñas incluidas, Telnet siempre recubre los valores de contraseñas cifradas o no cifradas en el almacenamiento intermedio para evitar riesgos en materia de seguridad.

Longitud de las opciones de entorno

La longitud de las opciones de entorno a las que se hace referencia en el párrafo anterior normalmente es de 1024 bytes. Dado que las negociaciones de opciones tienen una longitud no definida, las negociaciones que superen la longitud especificada pueden truncarse para tener cabida en el almacenamiento intermedio de opciones de entorno.

Permitir conexión

SALIDA; CHAR(1)

Se aplica a todos los dispositivos e indica al servidor Telnet si todos los dispositivos deben permitir que el cliente que se conecte al servidor Telnet. Si el tipo de dispositivo es de pantalla y ha habilitado el inicio de sesión automático, este cliente también puede eludir la pantalla de inicio de sesión en el sistema. Los valores válidos son los siguientes:

- 0 Rechazar la petición del cliente
- 1 Aceptar la petición del cliente

Permitir inicio de sesión automático

SALIDA; CHAR(1)

Se aplica a los tipos de dispositivo de pantalla e indica al servidor Telnet si debe permitirse que se lleve a cabo la operación de inicio de sesión automático para este cliente concreto. Este parámetro se aplica a los tipos de dispositivo de pantalla. Si se permite el inicio de sesión automático, este cliente puede eludir el dispositivo de inicio de sesión en el sistema. Los valores válidos son los siguientes:

- 0 Rechazar la petición de la aplicación del cliente. El sistema no tiene en cuenta los parámetros de salida Perfil de usuario, Biblioteca actual, Programa al que llamar, Menú inicial y Nombre de dispositivo.
- 1 Aceptar la petición de la aplicación del cliente. El sistema puede considerar válidos los parámetros de salida Perfil de usuario, Biblioteca actual, Programa al que llamar, Menú inicial y Nombre de dispositivo si el programa de salida los devuelve.

INIT0100: Formato de la información de descripción del usuario:

El proceso de inicio de sesión automático utiliza la información sobre el usuario.

La tabla siguiente muestra el formato de la información de descripción del usuario:

Tabla 5. Formato de la información de descripción del usuario

Despl dec	Despl hex	Tipo	Campo
0	0	INT(4)	Longitud de la información de descripción del usuario
4	4	CHAR(10)	Perfil de usuario
14	E	CHAR(10)	Biblioteca actual
24	18	CHAR(10)	Programa al que llamar
34	22	CHAR(10)	Menú inicial

Descripción de los campos de información de descripción del usuario

Biblioteca actual

Nombre de la biblioteca que será la actual si se habilita el distintivo de inicio de sesión automático. Este parámetro es opcional, pero si lo proporciona debe asegurarse de alinearlos a la izquierda y rellenarlo con blancos. El valor es el siguiente:

nombre de biblioteca

Nombre de la biblioteca que desea que el sistema designe como biblioteca actual.

Menú inicial

Nombre del menú inicial que se visualizará si se ha habilitado el distintivo de inicio de sesión automático. Los valores válidos son los siguientes:

nombre de menú

Nombre de un menú que se visualizará.

Longitud de la información de descripción del usuario

Longitud de la estructura de la información de descripción del usuario.

Programa al que llamar

Nombre de un programa al que el sistema llama si se ha habilitado el distintivo de inicio de sesión automático. Este parámetro es opcional, pero si lo proporciona debe alinearlos a la izquierda y rellenarlo con blancos. El valor es el siguiente:

nombre de programa

Nombre de un programa que el sistema iniciará.

Perfil de usuario

Perfil de usuario que el sistema utiliza para el procedimiento de inicio de sesión si se ha habilitado el distintivo de inicio de sesión automático. Este parámetro es obligatorio y debe alinearse a la izquierda y rellenarse con blancos.

INIT0100: Formato de la información de descripción del dispositivo:

Aquí se describen los formatos para crear o cambiar el dispositivo utilizado para una sesión Telnet.

La tabla siguiente muestra el formato de la información de descripción del dispositivo, que describe las características del dispositivo que se asociará a esta sesión.

Tabla 6. Formato de la información de descripción del dispositivo

Despl dec	Despl hex	Tipo	Campo
0	0	CHAR(10)	Nombre de dispositivo
10	A	CHAR(8)	Formato del dispositivo
18	12	CHAR(2)	Reservado

Tabla 6. Formato de la información de descripción del dispositivo (continuación)

Despl dec	Despl hex	Tipo	Campo
20	14	BINARY(4)	Desplazamiento hasta estructura de atributos del dispositivo
24	18	BINARY(4)	Longitud de la estructura de los atributos del dispositivo
28	1C	CHAR(*)	Estructura de atributos del dispositivo

Descripciones de campo de información de descripción del dispositivo

Nombre de dispositivo

Dispositivo virtual específico que se asociará a esta sesión Telnet. En el caso de los dispositivos de pantalla, si el valor del sistema de creación automática de dispositivos QAUTOVRT lo permite, el sistema crea automáticamente el dispositivo si todavía no existe y lo activa. En el caso de los dispositivos de impresión, el sistema crea automáticamente el dispositivo si todavía no existe. Si el programa de salida no proporciona ningún valor, el servidor Telnet utiliza de forma predeterminada los métodos de selección de dispositivo virtual Telnet tradicionales. El nombre de dispositivo debe ser un nombre de descripción de dispositivo de pantalla o impresión válido y debe cumplir los convenios de denominación de objetos de i5/OS estándar.

Formato del dispositivo

Tipo de dispositivo virtual específico asociado a esta sesión Telnet. Actualmente solo los dispositivos de pantalla que soporta el sistema.

DSPD0100

El dispositivo es una pantalla. El sistema devuelve los atributos de pantalla.

Reservado

Reservado para uso futuro.

Desplazamiento hasta estructura de atributos del dispositivo

Desplazamiento desde el inicio de la información de descripción del dispositivo hasta el inicio de la estructura de los atributos del dispositivo.

Longitud de la estructura de los atributos del dispositivo

Longitud en el espacio de usuario de la estructura de los atributos del dispositivo.

INIT0100: Formato de la información de descripción del dispositivo de pantalla (DSPD0100)

La tabla siguiente muestra el formato de la información de descripción del dispositivo de pantalla, que describe las características del dispositivo que se asociará a esta sesión.

Tabla 7. Formato de la información de descripción del dispositivo de pantalla (DSPD0100)

Despl dec	Despl hex	Tipo	Campo
0	0	CHAR(3)	Identificador de teclado
3	3	CHAR(1)	Reservado
4	4	BINARY(4)	Página de códigos
8	8	BINARY(4)	Juego de caracteres

Descripciones de los campos de DSPD0100

Juego de caracteres

El juego de caracteres que el sistema utiliza para este trabajo interactivo. Puede encontrar los

valores válidos en el soporte de idioma nacional (NLS). Este campo es idéntico al parámetro Juego de caracteres de la API de abrir vía de terminal virtual (QTVOPNVT).

Página de códigos

La página de códigos que el sistema utiliza para este trabajo interactivo. Puede encontrar los valores válidos en NLS. Este campo es idéntico al parámetro Página de códigos de la API de abrir vía de terminal virtual (QTVOPNVT).

Identificador de teclado

El identificador de teclado de 3 caracteres que el sistema utiliza para este trabajo interactivo. El identificador de teclado especifica implícitamente la página de códigos y el juego de caracteres que se va a utilizar, salvo que se altere temporalmente como parte de los parámetros Página de códigos y Juego de caracteres. Puede encontrar los identificadores válidos en NLS. Este campo es idéntico al parámetro Tipo de idioma de teclado de la API de abrir vía de terminal virtual (QTVOPNVT).

Reservado

Reservado para uso futuro.

Referencia relacionada

API de abrir vía de terminal virtual QTVOPNVT

INIT0100: Formato de la información de descripción de la conexión:

Este tema contiene información sobre la conexión del cliente que puede utilizar el programa de salida.

La tabla siguiente muestra el formato de la información de descripción de la conexión, que describe información sobre la conexión y el cliente para esta sesión.

Tabla 8. Formato de la información de descripción de la conexión

Despl dec	Despl hex	Tipo	Campo
0	0	INT(4)	Longitud de la información de descripción de la conexión
4	4	CHAR(20)	Dirección Internet del cliente
24	18	CHAR(1)	Contraseña del cliente validada
25	19	CHAR(12)	Tipo de estación de trabajo
39	27	CHAR(1)	Conexión de capa de sockets seguros
40	28	CHAR(20)	Dirección Internet del servidor (local)
60	3C	CHAR(1)	Nivel de autenticación del cliente
61	3D	CHAR(3)	Reservado
64	40	INT(4)	Código de retorno de certificado de cliente válido
68	44	INT(4)	Desplazamiento hasta certificado de cliente
72	48	INT(4)	Longitud del certificado de cliente

Descripciones de campo de información de descripción de la conexión

Longitud de la información de descripción de la conexión

Longitud de la estructura de descripción de la conexión.

Dirección Internet del cliente

Dirección IP (o estructura de tipo) del cliente que efectúa la petición, que siempre se proporciona al programa de salida. El diseño de los campos nuevos es:

Tabla 9. Diseño de la dirección IP del cliente

Nombre	Tamaño	Descripción
sin_len	CHAR(1)	Tamaño de la estructura sockaddr_in.
sin_family	CHAR(1)	Familia o protocolo. IP (Versión 4) es hex 02
sin_port	CHAR(2)	Número de puerto sin signo de 16 bits.
sin_addr	CHAR(16)	Sin signo de 4 bytes.

Contraseña del cliente validada

Especifica si Telnet ha validado la contraseña cifrada del cliente (si se ha recibido). El sistema establece este valor si los clientes TN5250E envían la contraseña cifrada para la validación. La contraseña se comprueba mediante las llamadas a funciones de servicio. Esto permite al programa de salida garantizar un proceso de inicio de sesión de cliente seguro.

- Valor = 0; la contraseña o frase de paso del cliente (o el ticket de Kerberos) no se ha validado o no se ha recibido.
- Valor = 1; la contraseña o frase de paso no cifrada del cliente se ha validado.
- Valor = 2; la contraseña o frase de paso cifrada del cliente (o el ticket de Kerberos) se ha validado.

Tipo de estación de trabajo

Tipo de estación de trabajo solicitado por el cliente, que es una de las especificaciones de Internet que figuran en la tabla Correlaciones de estación de trabajo e impresora.

Capa de sockets seguros

Indica si la conexión es una conexión SSL (Capa de sockets seguros):

- 0** La conexión no utiliza SSL.
- 1** La conexión utiliza SSL.

Dirección Internet del servidor

Dirección IP (o estructura de tipo) de la interfaz de red de host (local), que siempre se proporciona al programa del punto de salida. El diseño de los campos nuevos es el siguiente.

Tabla 10. Diseño de la dirección IP del cliente

Nombre	Tamaño	Descripción
sin_len	CHAR(1)	Tamaño de la estructura sockaddr_in.
sin_family	CHAR(1)	Familia o protocolo. IP es hex 02, IPX es hex 06
sin_port	CHAR(2)	Número de puerto sin signo de 16 bits.
sin_addr	CHAR(16)	Dirección de red sin signo de 4 bytes.

Nivel de autenticación del cliente

Indica si se requieren certificados de SSL cliente para conectarse al sistema.

- 0 No se necesita ningún certificado de cliente.
- 1 Se necesita un certificado de cliente válido.

Código de retorno de certificado de cliente válido

Código de retorno recibido durante la operación de negociación de SSL una vez validado el certificado de cliente.

Desplazamiento hasta certificado de cliente

Desplazamiento desde el inicio de la estructura de conexión hasta el primer byte del certificado de cliente.

Longitud del certificado de cliente

Longitud del certificado de cliente que se ha recibido. Si no se ha recibido ningún certificado, la longitud es 0.

Conceptos relacionados

“Resolución de problemas relacionados con los tipos de emulación” en la página 95
 Al desarrollar un cliente Telnet, es importante que negocie el tipo de estación de trabajo de emulación correcto. Las funciones permitidas varían según el tipo de estación de trabajo. La siguiente guía permite conocer el tipo de estación de trabajo y las funciones de esa estación de trabajo.

Programa de salida de finalización de dispositivos

El punto de salida QIBM_QTG_DEVTERM se produce cuando un cliente Telnet finaliza la sesión Telnet. Esto permite anotar la información de finalización de sesión y llevar a cabo operaciones de restablecimiento de dispositivos o limpieza.

En la tabla siguiente se muestran los parámetros del punto de salida QIBM_QTG_DEVTERM.

1	Nombre de dispositivo	Entrada	Char(10)
---	-----------------------	---------	----------

Nombre de miembro QSYSINC: NONE
 Nombre de punto de salida: QIBM_QTG_DEVTERM
 Nombre con un formato de punto de salida: TERM0100

El servidor Telnet permite de forma opcional la detención del dispositivo, las actividades de auditoría de sesión y la gestión de dispositivos virtuales en relación con el dispositivo asociado a la sesión Telnet finalizada.

Grupo de parámetros obligatorios

Nombre de dispositivo

Entrada; CHAR(10) Dispositivo virtual específico asociado a esta sesión Telnet.

Ejemplos: programas de salida de Telnet

Los programas de ejemplo pueden ayudarle a utilizar puntos de salida de Telnet en el sistema.

Los programas de ejemplo descargables contienen los recursos siguientes:

- **Ejemplo de código de utilidad de CL Crear programa de salida de Telnet (TELCRT)**
 Utilice este ejemplo de código para crear, instalar o registrar programas de salida de Telnet. Está escrito en el lenguaje de programación CL (Lenguaje de control) de i5/OS.
- **Ejemplo de código de utilidad de CL Suprimir programa de salida de Telnet (TELDLT)**
 Utilice este ejemplo de código para desinstalar y suprimir programas de salida de Telnet desde el sistema. Está escrito en lenguaje de programación CL.
- **El programa de salida de inicialización de Telnet de ejemplo básico (DEVINIT1)**
 El programa de salida de inicialización de Telnet básico (DEVINIT1) le permite seleccionar clientes de Telnet. Puede decidir quién puede conectarse al servidor de Telnet y quién no. Se trata de un ejemplo

básico porque está diseñado para aprovechar partido de las otras muchas funciones disponibles para programas de salida de Telnet. El programa de salida de Telnet avanzado está diseñado para aprovechar esas funciones.

Es recomendable empezar con el programa de salida de inicialización de Telnet básico hasta comprender el funcionamiento para después migrar al programa de salida de inicialización de Telnet avanzado si necesita correlación de dispositivos virtuales u otras funciones avanzadas.

- **El ejemplo de programa de salida de inicialización de Telnet avanzado (DEVINIT2)**

El programa de salida de inicialización de Telnet avanzado (logon) utiliza las listas de acceso MAP y DISALLOW. Al utilizar la lista MAP en lugar de la lista ALLOW, que es más sencilla, el programa de inicialización avanzado aprovecha más de la interfaz de punto de salida que la versión básica. Esto permite establecer o alterar temporalmente los valores de sesión de Telnet, lo que constituye una función que corresponde normalmente a los entornos de Client Access. A continuación, se proporcionan algunos ejemplos de los tipos de valores de sesión:

- Seleccionar un dispositivo de terminal virtual para esta sesión
- Dejar de lado la pantalla de inicio de sesión
- Configurar el soporte de idioma nacional (NLS)

- **Ejemplo de programa de salida de finalización de Telnet (DEVTERM)**

DEVTERM QCSRC es un simple programa de registro de anotaciones que anota un mensaje de desconexión.

Es un programa compañero de DEVINIT1 QCSRC y DEVINIT2 QCSRC. Los mensajes de finalización anotados se pueden comparar con los mensajes de inicialización para determinar la duración de la sesión de Telnet.

Archivos de ejemplo de programa de salida de Telnet

Hay dos formatos de archivo disponibles para descargarse: ZIP y SAVF. Ambos formatos contienen los mismos archivos.

Los archivos .zip están en un formato compatible con los PC. Seleccione el archivo .zip para descargar el programa y los archivos de información en el PC, descomprímalos y transfíralos al sistema. Debe redenominar la mayoría de los archivos una vez guardados en el sistema.

Un archivo .savf es un archivo de guardar de i5/OS. Descárguelo en el PC y transfíralo al sistema. Puede crear una biblioteca temporal en el sistema y transferir el archivo de guardar a la biblioteca. Desempaquete el archivo de guardar en la biblioteca temporal y siga las instrucciones del archivo readme.

Pulse el enlace del formato de archivo que desee y pulse **Guardar**.

Nota: Al utilizar los ejemplos de código, acepta los términos de la “Información sobre licencia de código y exención de responsabilidad” en la página 108.

- telnet.zip (924 KB)
- telnet.savf (5,45 MB)

Gestión del cliente Telnet

Puede iniciar una sesión de cliente Telnet utilizando distintos tipos de emulación. Este tema también describe cómo establecer una sesión Telnet en cascada.

El cliente Telnet permite a un usuario TCP/IP iniciar una sesión y utilizar aplicaciones en un sistema remoto mediante una aplicación de servidor Telnet. Telnet permite conectarse al sistema remoto y utilizarlo como si se estuviera conectado directamente a él. Puede ejecutar programas, cambiar configuraciones o llevar a cabo prácticamente cualquier otra acción.

Telnet hace que su sistema actúe como estación de trabajo de un gran ordenador. Dicho de otro modo, al utilizar Telnet, su sistema (el cliente) se hace pasar por (emula) un terminal conectado directamente al sistema remoto (el servidor Telnet).

El cliente Telnet también da soporte a Request for Comments (RFC) 4777. Los clientes RFC 4777 obtienen más control sobre el dispositivo virtual del servidor Telnet en la plataforma System i por medio de varios parámetros nuevos del mandato STRTCPTELN (TELNET). Los nuevos parámetros son:

- Pantalla virtual remota (RMTVRTDSP)
- Usuario remoto (RMTUSER)
- Contraseña remota (RMTPWD) (con soporte para las nuevas contraseñas de 128 bytes si el servidor Telnet las soporta)
- Cifrado de contraseña remota (RMTPWENC) (incluido el cifrado DES7 y SHA1)
- Programa inicial remoto (RMTINLPGM)
- Menú inicial remoto (RMTINLMNU)
- Biblioteca actual remota (RMTCURLIB)
- Tipo de teclado remoto (RMTKBDTYPE)
- Juego de caracteres remoto (RMTCHRSET)
- Página de códigos remota (RMTCODPAG)

Control de las funciones de servidor Telnet desde el cliente

Puede utilizar el cliente Telnet para controlar el proceso de estación de trabajo en el servidor Telnet cuando esté en una sesión de cliente.

Para cada una de las funciones de mandato se listan tanto el nombre i5/OS como el nombre TCP/IP.

Para seleccionar las funciones de servidor que desea controlar, debe acceder al menú Enviar Funciones de Control TELNET. Para acceder a este menú, pulse la tecla **Atención** en el teclado 5250.

La lista siguiente proporciona una breve descripción de cada una de las funciones de control del cliente Telnet:

- **Interrumpir un proceso en el sistema Proceso interrupción o IP:** esta función cancela, interrumpe o suspende un proceso que se ha iniciado en el servidor. Por ejemplo, puede utilizar IP cuando un proceso parezca estar en un bucle permanente o si ha iniciado un proceso accidentalmente.
- **Consultar estado de conexión cuando el sistema queda inactivo Consultar estado de conexión o AYT:** esta función proporciona un mensaje procedente del servidor que informa de que el sistema sigue ejecutándose. Puede utilizar esta función de control cuando el sistema esté inactivo de forma inesperada durante un período largo de tiempo.
- **Descartar salida remota antes de que llegue a la estación de trabajo Descartar datos de salida remota o AO:** esta función permite finalizar la ejecución de un proceso que está generando datos de salida sin enviar la salida a la estación de trabajo. Esta función elimina los datos de salida del sistema que ya se han generado pero que todavía no se han visualizado en la estación de trabajo.
- **Borrado de la vía de datos entre el sistema cliente y el servidor Borrar la vía de acceso de los datos o SYNCH:** esta función elimina todos los caracteres (excepto los mandatos Telnet) entre el sistema cliente y el servidor. Puede utilizar esta función cuando los mecanismos de control de flujo de la red provocan que se guarden en almacenamiento intermedio otras funciones, como por ejemplo IP o AO.
- **Finalizar la sesión Telnet Finalizar sesión TELNET o QUIT:** esta función finaliza la sesión Telnet y cierra la conexión TCP/IP con el sistema (sistema remoto). Puede solicitar esta función en cualquier momento durante la sesión Telnet, pero debe finalizar la sesión en el sistema remoto antes de seleccionar esta función. Si no finaliza la sesión, seguirá conectado al sistema debido a que el protocolo Telnet no proporciona ninguna secuencia de fin de sesión.

- **Utilización de la tecla Atención a la opción de host remoto Tecla Atenc a host remoto:** pulse la tecla Atención para visualizar el menú Enviar Funciones de Control TELNET.

Notas:

1. Esta opción solo es válida para la modalidad 5250.
2. Si ejecuta la modalidad VTxxx (VT100 o VT220), hay dos opciones adicionales en este menú:
 - Para las sesiones VT100, la opción 6 (Cambiar correlación de teclado primaria de VT100) y la opción 7 (Cambiar correlación de teclado alternativa de VT100).
 - Para la sesión VT220, la opción 8 (Cambiar correlación de teclado primaria de VT220) y la opción 9 (Cambiar correlación de teclado alternativa de VT220).

Conceptos relacionados

“Inicio de una sesión de cliente Telnet”

Debe conocer el nombre o la dirección Internet del sistema remoto en el que desea iniciar la sesión Telnet.

“Inicio de una sesión de cliente Telnet 3270” en la página 56

Cuando inicia una sesión de cliente Telnet utilizando la emulación 3270, la aplicación del sistema remoto controla la pantalla. Recibirá las mismas pantallas y especificará los datos de la misma forma que para otros dispositivos 3270 conectados localmente al sistema remoto.

“Inicio de una sesión de cliente Telnet VTxxx” en la página 62

Puede iniciar una sesión de cliente Telnet utilizando la emulación VTxxx. Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

Sesiones de cliente Telnet 5250

Puede utilizar este tipo de emulación para iniciar la sesión y utilizar aplicaciones en un sistema remoto que tiene una aplicación de servidor Telnet.

El soporte de cliente Telnet 5250 permite a los usuarios iniciar la sesión en otros sistemas y acceder a aplicaciones 5250 de pantalla completa. El soporte de 5250 en modalidad de pantalla completa solo puede negociarse con una aplicación de servidor Telnet que se ejecute en un sistema operativo i5/OS o en un sistema que dé soporte al servidor Telnet 5250. La negociación del soporte de estación de trabajo 525x con la aplicación de servidor Telnet remoto activa el soporte de 5250 en modalidad de pantalla completa.

Inicio de una sesión de cliente Telnet

Debe conocer el nombre o la dirección Internet del sistema remoto en el que desea iniciar la sesión Telnet.

Para iniciar una sesión Telnet con un sistema remoto, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Tabla de hosts** para visualizar las direcciones Internet y los nombres de host.
 1. Escriba el mandato STRTCPTELN (Arrancar TCP/IP TELNET) o escriba TELNET en la línea de mandatos y pulse Intro.
 2. Teclee el nombre del sistema remoto. Si desea emplear los parámetros opcionales, pulse F10; de lo contrario, pulse Intro.
Si ha escrito *INTNETADR en el campo **Sistema remoto**, el servidor le solicitará el campo **Dirección Internet**.
 3. Escriba la dirección Internet del sistema remoto. Si desea emplear los parámetros opcionales, pulse F10; de lo contrario, pulse Intro. La pantalla muestra los valores de parámetros opcionales y la información de la dirección Internet.
 4. Para utilizar los valores predeterminados de los parámetros, pulse Intro.
 5. Al iniciar una sesión en modalidad de pantalla completa 5250, también son válidos los parámetros opcionales siguientes:

- Tiempo de espera de host (INZWAIT)
- Tipo de idioma de teclado (KBDTYPE)
- Número de puerto de la aplicación de servidor de hospedaje remoto (PORT)
- Pantalla virtual remota (RMTVRTDSP)
- Usuario remoto (RMTUSER)
- Contraseña remota (RMTPWD)
- Cifrado de contraseña remota (RMTPWDENC)
- Programa inicial remoto (RMTINLPGM)
- Menú inicial remoto (RMTINLMNU)
- Biblioteca actual remota (RMTCURLIB)
- Tipo de teclado remoto (RMTKBDTYPE)
- Juego de caracteres remoto (RMTCHRSET)
- Página de códigos remota (RMTCODPAG)

La próxima es la pantalla de inicio de sesión en el sistema remoto.

Notas:

1. La pantalla de inicio de sesión sólo se visualiza si no se especifica ninguno de los parámetros de inicio de sesión automático en el mandato STRTCPTLN (RMTUSER, RMTPWD, RMTPWDENC) o si se produce un error al especificar estos parámetros. Si estos valores se especifican correctamente, no se visualiza ninguna pantalla de inicio de sesión. La sesión del usuario se inicia automáticamente y se visualiza el panel inicial que se haya definido para el usuario.
2. Además, se cumplen las condiciones siguientes:
 - Si el mandato STRTCPTLN proporciona los parámetros RMTUSER, RMTPWD y RMTPWDENC correctos, y también se suministra un parámetro RMTINLPGM correcto, se inicia la sesión del usuario. Además, se ejecuta el programa inicial proporcionado.
 - No obstante, si el parámetro RMTINLPGM no es válido, se inicia la sesión del usuario pero aparece el mensaje el trabajo ha finalizado de forma anómala. Las mismas acciones tienen lugar para el parámetro RMTINLMNU.
3. En el caso del parámetro RMTCURLIB, la especificación de un valor correcto hace que se inicie la sesión del usuario. Además, se ejecuta el programa inicial y/o el menú que se hayan definido en el perfil del usuario o en el mandato STRTCPTLN. Además, la biblioteca actual se establece en el valor del parámetro. Si se proporciona un valor que no es válido para el parámetro RMTCURLIB, se visualiza un panel de inicio de sesión con un mensaje en el que se indica que el valor de la biblioteca actual no es válido.
4. Asimismo, para todos los elementos anteriores, si los parámetros RMTKBDTYPE, RMTCHRSET o RMTCODPAG se proporcionan con valores válidos, habrán entrado en vigor para los intentos de inicio de sesión automático satisfactorios. No entran en vigor para los intentos de inicio de sesión que no hayan sido válidos.

Nota: si el sistema no encuentra o no configura un servidor SOCKS, o si se producen errores al utilizar el servidor SOCKS, se establece una conexión directa.

Tamaño de pantalla de TN5250

La modalidad de pantalla completa Telnet 5250 proporciona soporte para los tamaños de pantalla siguientes:

- 1920 caracteres (24 x 80) en todas las estaciones de pantalla 5250.
- 3564 caracteres (27 x 132) en todas las 3180 Modelo 2, 3197 Modelos D1, D2, W1, W2 y 3477 Modelos FA, FC, FD, FE, FG, FW.

Referencia relacionada

“Control de las funciones de servidor Telnet desde el cliente” en la página 53

Puede utilizar el cliente Telnet para controlar el proceso de estación de trabajo en el servidor Telnet cuando esté en una sesión de cliente.

“Establecimiento de una sesión Telnet en cascada” en la página 89

Puede establecer otra sesión Telnet mientras está en una sesión Telnet actual. Una vez establecida una sesión en cascada, puede moverse entre los distintos sistemas.

Sesiones de cliente Telnet 3270

El tipo de emulación 3270 permite acceder a un sistema remoto que tiene una aplicación de servidor Telnet.

Dado que las corrientes de datos 3270 se convierten en corrientes de datos 5250, los dispositivos de estación de trabajo operan como una pantalla 5251 remota para la plataforma System i y los programas de aplicación.

Nota: al utilizar los ejemplos de código, acepta los términos de la “Información sobre licencia de código y exención de responsabilidad” en la página 108.

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa 3270” en la página 27

Los usuarios de clientes Telnet pueden iniciar una sesión y ejecutar aplicaciones 5250 de pantalla completa utilizando la modalidad de pantalla completa 3270.

Inicio de una sesión de cliente Telnet 3270

Cuando inicia una sesión de cliente Telnet utilizando la emulación 3270, la aplicación del sistema remoto controla la pantalla. Recibirá las mismas pantallas y especificará los datos de la misma forma que para otros dispositivos 3270 conectados localmente al sistema remoto.

Cuando el cliente Telnet negocia el soporte de estación de trabajo 327x con la aplicación de servidor Telnet remoto, el sistema activa la modalidad de pantalla completa 3270. El cliente Telnet negocia el soporte de pantalla completa 3270 con cualquier aplicación de servidor Telnet que dé soporte a las aplicaciones 3270 de pantalla completa, en lugar de a las aplicaciones 5250.

Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

debe conocer el nombre o la dirección Internet del sistema remoto en el que desea iniciar la sesión Telnet. Para visualizar las direcciones Internet y los nombres de host, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Tabla de hosts** para visualizar las direcciones Internet y los nombres de host.
 1. Escriba el mandato STRTCPTELN (Arrancar TCP/IP TELNET) o escriba TELNET en la línea de mandatos y pulse Intro.
 2. Teclee el nombre del sistema remoto. Si desea emplear los parámetros opcionales, pulse F10; de lo contrario, pulse Intro.
Si escribe *INTNETADR para el nombre del **Sistema remoto** y pulsa Intro, el servidor le solicitará el campo **Dirección Internet**.
 3. Escriba la dirección Internet del sistema remoto. Si desea emplear los parámetros opcionales, pulse F10; de lo contrario, pulse Intro. La pantalla muestra los valores de parámetros opcionales y la información de la dirección Internet.
 4. Para utilizar los valores predeterminados de los parámetros, pulse Intro. Se iniciará la conexión con el servidor Telnet.
 5. Durante una sesión en modalidad de pantalla completa 3270, también son válidos los parámetros opcionales siguientes:

- Tiempo de espera de host (INZWAIT)
- Tipo de idioma de teclado (KBDTYPE)
- Tecla Retroceso Página (Giro Abajo) (PAGEUP)
- Tecla Avance Página (Giro Arriba) (PAGEDOWN)
- Tecla de selección del cursor (CSRSLT)
- Tabla de conversión 3270 de salida (TBL3270OUT)
- Tabla de conversión 3270 de entrada (TBL3270IN)
- Teclado de bloqueo numérico (NUMLCK)
- Cambiar cómo se manejan los nulos (NULLS)
- Número de puerto de la aplicación de servidor de hospedaje remoto (PORT)

La próxima es la pantalla de inicio de sesión en el sistema remoto.

Conceptos relacionados

“Correlación de teclado 3270 para servidores Telnet” en la página 60

Este tema contiene información sobre la correlación de teclado para el soporte de la emulación 3270.

“Consideraciones sobre la pantalla completa 3270”

Tenga en cuenta el tamaño de pantalla, la tecla de selección del cursor, los mensajes de error y los caracteres nulos de 3270 al utilizar la emulación 3270.

Referencia relacionada

“Control de las funciones de servidor Telnet desde el cliente” en la página 53

Puede utilizar el cliente Telnet para controlar el proceso de estación de trabajo en el servidor Telnet cuando esté en una sesión de cliente.

Consideraciones sobre la pantalla completa 3270

Tenga en cuenta el tamaño de pantalla, la tecla de selección del cursor, los mensajes de error y los caracteres nulos de 3270 al utilizar la emulación 3270.

Al utilizar la modalidad de pantalla completa 3270 para el cliente Telnet, debe tener presentes las cuestiones siguientes:

- Tamaño de pantalla de 3270
- Tecla de selección del cursor de 3270
- Mensajes de error de 3270
- Caracteres nulos de 3270

Tamaño de pantalla de TN3270

Requisitos de la modalidad de pantalla completa Telnet 3270:

- Si el tipo de dispositivo 3270 negociado requiere 1920 caracteres, el código de cliente Telnet se ejecuta con cualquier tipo de dispositivo 5250 como terminal de cliente.
- Si el tipo de dispositivo 3270 negociado requiere 3564 caracteres, el código de cliente Telnet requiere un tipo de dispositivo 5250 Modelo 3180; 3197 Modelo D1, D2, W1, W2; 3477 Modelo FA, FC, FD, FE, FG; FW como terminal de cliente.
- Hay una pantalla 27x132 cuando se negocia un tipo de dispositivo 3180 Modelo 2; 3197 Modelo D1, D2, W1, W2; 3477 Modelo FA, FC, FD, FE, FG; FW. En los releases anteriores, se necesitaba un área de datos para obtener este soporte.
- Para obtener una pantalla 24x80, ejecute el mandato CRTDTAARA DTAARA(nombrebiblioteca/QTVNO32785) TYPE(*CHAR) VALUE('1').

Tecla de selección del cursor TN3270

La tecla de selección del cursor existente está inhabilitada si elige emular la tecla de selección del cursor. Especificando uno de los parámetros siguientes para el mandato STRTCPTELN se emula la tecla de selección del cursor:

Tabla 11. Parámetros para emular la tecla de selección del cursor

Parámetro	Valor
Tecla Retroceso Página (Giro Abajo)	*CSRSLT
Tecla Avance Página (Giro Arriba)	*CSRSLT
Tecla de selección del cursor	*Tecla F (especifique una tecla de función de *F1 a *F24)

Mensajes de TN3270

Si utiliza la modalidad de pantalla completa Telnet 3270, pueden visualizarse varios tipos de mensajes de error.

- Los errores de entrada de teclas se visualizan como números de 4 dígitos intermitentes en la esquina inferior izquierda de la pantalla. Pulse la tecla Ayuda o F1 (Ayuda) para obtener más información sobre el mensaje. Consulte el manual de funcionamiento del sistema si no logra corregir el error.
- Los mensajes del sistema incluyen los mensajes de Telnet y se emiten desde el sistema.
- Si desea obtener información sobre los mensajes enviados desde el sistema remoto, consulte la documentación del sistema remoto.

TN3270 - Manejo de caracteres nulos

Cuando una estación de pantalla 3270 envía una corriente de datos, se eliminan todos los caracteres nulos. Especifique uno de los valores siguientes para el parámetro de manejo de caracteres nulos (NULLS) del mandato STRTCPTELN:

*REMOVE

Elimina los caracteres nulos iniciales e intercalados.

*BLANK

Cambia los caracteres nulos iniciales e intercalados por blancos. Este es el valor predeterminado. Los caracteres nulos finales siempre se eliminan con ambos valores. Este es el valor predeterminado. Por ejemplo, suponga que los datos constan del siguiente código (0 indica un carácter nulo):

```
0x0yz000
```

La corriente de datos enviada desde una estación de pantalla 5250 que ejecuta la modalidad de pantalla completa Telnet 3270 con el valor predeterminado *BLANK contiene el siguiente código:

```
bxbyz
```

La corriente de datos enviada desde una estación de pantalla 3270 o desde una estación de pantalla 5250 que ejecuta una sesión Telnet 3270 en modalidad de pantalla completa si se ha especificado el valor *REMOVE contendría el siguiente código:

```
xyz
```

El valor *REMOVE es válido para los dispositivos siguientes:

- Todas las pantallas conectadas localmente
- Las pantallas conectadas a un controlador 5394 remoto

- Las pantallas de Personal Computer que utilizan la función de estación de trabajo

Conceptos relacionados

“Inicio de una sesión de cliente Telnet 3270” en la página 56

Cuando inicia una sesión de cliente Telnet utilizando la emulación 3270, la aplicación del sistema remoto controla la pantalla. Recibirá las mismas pantallas y especificará los datos de la misma forma que para otros dispositivos 3270 conectados localmente al sistema remoto.

Utilización de una estación de pantalla

Aquí se describen las diferencias de teclado y pantalla cuando se utiliza una estación de pantalla durante una sesión Telnet 3270 en modalidad de pantalla completa. Otras cuestiones que deben tenerse presentes en relación con la modalidad Telnet 3270 son el número de campos de entrada, los mensajes de error y la finalización de una sesión.

Especificación de juegos de caracteres y teclado

El tipo de idioma de teclado que especifique para la estación de trabajo, con el parámetro de tipo de idioma de teclado del mandato STRTCPTELN, debe coincidir con el parámetro de tipo de idioma de teclado de la estación de trabajo conectada de forma remota. Si especifica un tipo de idioma de teclado que no coincide, algunos de los caracteres no se visualizarán como sería de esperar.

Teclados 5250 y 3270

La posición y la función de las teclas del teclado 5250 (3196G, 3180 Modelo 2 o 5291) son distintas de las del teclado 3278.

Nota: en el caso del cliente Telnet que opera en modalidad de pantalla completa 3270, la función Borrar de 3270 se establece de forma predeterminada en la secuencia de teclas Desplazamiento-Mandato-Retroceso.

El manual System Operation for New Users señala las diferencias de teclado de los teclados siguientes:

- Teclado mejorado IBM
- Teclado de máquina de escribir de 122 teclas
- Teclado 5250
- Teclado para Personal Computer o de estilo IBM AT para Personal Computer
- Teclado de estilo 5250 para Personal Computer o AT para Personal Computer
- Teclado mejorado IBM para Personal Computer

Teclados para Personal Computer

Si el PC utiliza la función de estación de trabajo (WSF) de System i Access para Windows, puede visualizar el diseño del teclado 5250 con el mandato de teclas de función de estación de trabajo (WSFKEYS). Puede modificar el estilo mediante el mandato para configurar función de estación de trabajo (CFGWSF). Estos mandatos se tratan en el manual Client Access/400 for DOS with Extended Memory Setup. Si el PC no utiliza la función de estación de trabajo, consulte la documentación adecuada del emulador (por ejemplo, OS/2 CM/2) para ver o cambiar el estilo de teclado.

TN3270-Signo menos

Si ha especificado el valor *YES para el parámetro de bloqueo de teclado numérico del mandato STRTCPTELN, si utiliza un teclado de entrada de datos y el cursor se encuentra en un campo de contenido únicamente numérico, realice las siguientes tareas para visualizar un signo menos 5250:

1. Pulse la tecla Num (Numérico).
2. Pulse la tecla de signo menos (-).

Para visualizar un signo menos en 3278, pulse la tecla de signo menos.

TN3270-Avance Página y Retroceso Página

Si la aplicación 3270 tiene una pantalla que no permite ver todos los campos de datos de entrada, utilice las teclas 5250 Avance Página y Retroceso Página para escribir información una vez superado el número máximo de campos de entrada de la pantalla.

También puede asignar funciones PF y PA a las teclas de página especificando su uso en el mandato STRTCPTLN.

El cursor siempre aparece como un carácter de subrayado tanto en pantallas 5250 como en pantallas 3270.

Correlación de teclado 3270 para servidores Telnet

Este tema contiene información sobre la correlación de teclado para el soporte de la emulación 3270.

La tabla siguiente muestra las asignaciones de tecla PF predeterminadas para llevar a cabo las diversas funciones 5250. Puede utilizar el mandato de visualizar correlación de teclado (DSPKBDMAP) para ver la correlación de teclado actual. Si lo prefiere, puede emplear la opción 6 (Visualizar correlación de teclado 3270) del menú Configurar TCP/IP TELNET, mientras el terminal está en la modalidad de emulación 3270.

Tabla 12. Asignaciones de tecla PF predeterminadas

Tecla de función 5250	Teclas 3270 predeterminadas para seleccionar la función
Ayuda	PF1
3270 Ayuda	PF2
Borrar	PF3
Imprimir	PF4
Visualizar atributos incorporados	PF5
Petición de prueba	PF6
Giro Abajo	PF7
Giro Arriba	PF8
Restaurar error	PF10 o Intro
Petición de sistema (Pet Sis)	PF11
Retroceso de registro	PF12
De F1 a F12	Pulse PA1 y, a continuación, una de las teclas siguientes: de PF1 a PF12
De F13 a F24	Pulse PA2 y, a continuación, una de las teclas siguientes: de PF1 a PF12 o de PF13 a PF24 (si existen)
Salida de campo	Borrar EOF y, a continuación, tabulador de campo
Atención	Para 3277 utilice Petición de prueba y a continuación PA1. Para 3278/3279 utilice la tecla Atenc

El programa de lenguaje de control (CL) de ejemplo siguiente establece la correlación de teclado para una estación de trabajo de tipo 327x que utiliza Telnet para acceder a una plataforma System i. Este programa correlaciona las teclas de función de i5/OS con sus teclas de función equivalentes de la estación de trabajo 327x. Si intenta ejecutar un mandato CHGKBDMAP desde una estación de trabajo sin estar en la modalidad de emulación 3270, recibirá el mensaje CPF8701. Al supervisar el mensaje, el resto del programa queda inutilizado en estas circunstancias.

Nota: al utilizar los ejemplos de código, acepta los términos de la “Información sobre licencia de código y exención de responsabilidad” en la página 108.

```
PGM
MONMSG      MSGID(CPF8701 CPF0000)
CHGKBDMAP  PF1(*F1) PF2(*F2) PF3(*F3) PF4(*F4) PF5(*F5)
PF6(*F6) PF7(*DOWN) PF8(*UP) PF9(*F9)
PF10(*F10) PF11(*F11) PF12(*F12)
PA1PF1(*HELP) PA1PF2(*HLP3270)
PA1PF3(*CLEAR) PA1PF4(*PRINT)
PA1PF5(*DSPATR) PA1PF6(*TEST) PA1PF7(*F7)
PA1PF8(*F8) PA1PF9(*ATTN) PA1PF10(*RESET)
PA1PF11(*SYSREQ) PA1PF12(*BCKSPC)
ENDPGM
```

Si almacena este fuente CL en el archivo QCLSRC de la biblioteca TCPLIB como miembro CHGKBD, puede crear el programa CL Cambiar correlación de teclado (CHGKBD) en la biblioteca TCPLIB mediante el siguiente mandato CL:

```
CRTLPGM PGM(TCPLIB/CHGKBD) SRCFILE(TCPLIB/QCLSRC)
TEXT('Cambiar la correlación de teclado para terminales 327x')
```

Desde este momento, cualquier usuario que utilice Telnet con una plataforma System i puede llamar al programa CHGKBD. También se le puede llamar automáticamente en el momento de iniciar la sesión especificando el programa CHGKBD como el parámetro de programa inicial del mandato Cambiar perfil de usuario (CHGUSRPRF); el programa inicial del perfil también puede llamar al programa CHGKBD.

Teclas PA1 y PA2 en un teclado de PC

Las teclas PA1 y PA2 no aparecen en un teclado de PC. Una correlación de teclado en el emulador 3270 proporciona la función de estas teclas 3270 en un teclado de PC.

La correlación de teclado 3270 Telnet predeterminada utiliza estas teclas. Por consiguiente, es importante que sepa dónde están estas teclas en el teclado antes de iniciar una sesión 3270 Telnet. Esto tiene especial relevancia si prevé iniciar una sesión sin cambiar la correlación de teclado. Consulte en la documentación del emulador las teclas o pulsaciones necesarias para proporcionar estas funciones.

Hay algunas secuencias de teclas 5250 para las que no existe ninguna secuencia de teclas 3270 soportada, por lo que no es posible establecer estos mandatos de teclado en un 3270. Estas secuencias de teclas son las siguientes:

- Campo más
- Campo menos
- Borrar todos los campos de entrada

La función de tecla Salida de campo 5250 se realiza en un teclado 3270 mediante la tecla Borrar EOF y a continuación la tecla tabulador.

Circunstancias especiales

Al utilizar Telnet 3270 en modalidad de pantalla completa desde el terminal 3270 antes de que se cambie la correlación predeterminada para el terminal, las teclas PF1-PF12 pueden emularse mediante la secuencia de teclas PA1 PFx. Por consiguiente, instrucciones como "Pulse PF3" o "Pulse PF4" deben leerse del modo siguiente: "Pulse PA1 PF3" y "Pulse PA1 PF4", antes de crear una nueva correlación de teclado.

Según la instalación del cliente Telnet para el host (por ejemplo, el cliente Telnet de máquina virtual (VM)), al pulsar PA1, el usuario podría obtener la instrucción Mandato TELNET: en la línea situada en la parte inferior de la pantalla. Si el sistema visualiza esta instrucción, escriba PA1 y pulse la tecla Intro, mueva el cursor a la línea de mandatos y pulse la tecla PF necesaria.

Nota: *Host Command Facility (HCF)* es una función disponible en los sistemas de hospedaje System/370, 43xx y 30xx. Esta función permite a un usuario del sistema de hospedaje utilizar las aplicaciones de una plataforma System i. Si utiliza HCF para conectarse a una plataforma System i y, a continuación, utiliza Telnet para iniciar sesión en otra plataforma System i desde dicha plataforma, estará en una sesión 3270 en modalidad de pantalla completa. El teclado se correlaciona dos veces, una para la sesión HCF inicial y otra para la sesión Telnet. Para utilizar las teclas PF como lo haría normalmente, debe cambiar la correlación de teclado en ambas plataformas. Asegúrese de que utiliza la misma correlación de teclado en cada una de las plataformas.

Conceptos relacionados

“Inicio de una sesión de cliente Telnet 3270” en la página 56

Cuando inicia una sesión de cliente Telnet utilizando la emulación 3270, la aplicación del sistema remoto controla la pantalla. Recibirá las mismas pantallas y especificará los datos de la misma forma que para otros dispositivos 3270 conectados localmente al sistema remoto.

“Configuración del servidor Telnet para la modalidad de pantalla completa 3270” en la página 27

Los usuarios de clientes Telnet pueden iniciar una sesión y ejecutar aplicaciones 5250 de pantalla completa utilizando la modalidad de pantalla completa 3270.

Sesiones de cliente VTxxx

Las sesiones de cliente Telnet VTxxx proporcionan información sobre cómo utilizar este tipo de emulación para iniciar la sesión y utilizar aplicaciones en un sistema remoto que tiene una aplicación de servidor Telnet. Esta sección también facilita más información sobre la emulación VTxxx.

El soporte Telnet VTxxx permite a los usuarios iniciar la sesión en plataformas distintas de la plataforma System i como si estuvieran en un terminal VTxxx conectado al sistema de forma local. Con el soporte de cliente VTxxx, un usuario puede iniciar la sesión en cualquier sistema remoto de una red TCP/IP que dé soporte a la corriente de bytes de VTxxx. Como usuario de Telnet, debe conocer las diferencias físicas y operativas que existen entre las sesiones VTxxx y 5250.

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx” en la página 30

El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

Inicio de una sesión de cliente Telnet VTxxx

Puede iniciar una sesión de cliente Telnet utilizando la emulación VTxxx. Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

debe conocer el nombre o la dirección Internet del sistema remoto en el que desea iniciar la sesión Telnet.

Para iniciar una sesión Telnet VTxxx con el sistema remoto, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Tabla de hosts** para visualizar las direcciones Internet y los nombres de host.
3. Escriba el mandato STRTCPELN (Arrancar TCP/IP TELNET) o escriba TELNET en la línea de mandatos y pulse Intro.
4. Escriba el nombre del sistema remoto, o escriba *INTERNETADR si prefiere utilizar la dirección Internet. Si desea ver los parámetros opcionales, pulse F10; de lo contrario, pulse Intro.

Si ha escrito *INTERNETADR en el campo **Sistema remoto**, el sistema le solicitará el campo **Dirección Internet**.

5. Escriba la dirección Internet del sistema remoto. Si desea emplear los parámetros opcionales, pulse F10; de lo contrario, pulse Intro. La pantalla muestra los valores de parámetros opcionales y la información de la dirección Internet.
6. Para utilizar los valores predeterminados de los parámetros, pulse Intro.
7. Durante una sesión en modalidad de pantalla completa VTxxx, también son válidos los parámetros opcionales siguientes:
 - Tabla de conversión ASCII de entrada (TBLVTIN)
 - Tabla de conversión ASCII de salida (TBLVTOUT)
 - Tabla de salida especial (TBLVTDRAWO)
 - Tabla de entrada especial (TBLVTDRAWI)
 - Opciones seleccionadas (VTOPT)
 - Visualizar atributos de carácter (DSPCHRATTR)
 - Función de desplazamiento de página (PAGE_SCROLL)
 - Función de respuesta (ANSWERBACK)
 - Topes de tabulador (TABSTOP)
 - Tiempo de espera de host (INZWAIT)
 - Identificador de juego de caracteres (CCSID)
 - Modalidad operativa ASCII (ASCOPRMOD)-- válido únicamente para la inicialización de una sesión VT220 (no tiene ningún efecto en las negociaciones)
 - Número de puerto de la aplicación de servidor de hospedaje remoto (PORT)
 - Caracteres de control (CTLCHAR)

Nota: pueden aparecer caracteres imprevistos por la configuración incorrecta del sistema remoto. Si esto sucede, verifique que el valor de tipo de estación de trabajo sea adecuado para una estación de trabajo en modalidad de pantalla completa VTxxx. También puede utilizar el mandato set term para cambiar la modalidad de pantalla completa de la conexión.

La próxima es la pantalla de inicio de sesión en el sistema remoto.

Conceptos relacionados

“Consideraciones sobre la modalidad de pantalla completa VTxxx”

Al igual que sucede con cualquier tipo de emulación, debe tener en cuenta determinadas consideraciones antes de utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet. Entre estas consideraciones se encuentran algunas cuestiones de seguridad, así como condiciones de error posibles e indicadores luminosos. Si se familiariza con estas consideraciones, aprenderá a utilizar de forma eficaz la modalidad de pantalla completa VTxxx.

Referencia relacionada

“Control de las funciones de servidor Telnet desde el cliente” en la página 53

Puede utilizar el cliente Telnet para controlar el proceso de estación de trabajo en el servidor Telnet cuando esté en una sesión de cliente.

“Valores de las teclas VTxxx” en la página 69

Los valores de las teclas VTxxx proporcionan la correlación de teclado para el soporte de la emulación VTxxx. El soporte de sesión de cliente para las modalidades VT100 y VT220 proporciona una correlación de teclado primaria y otra alternativa.

“Modalidad nacional de VTxxx” en la página 76

La modalidad nacional de VTxxx soporta el juego de caracteres de sustitución nacional, que es un grupo de juegos de caracteres de 7 bits.

Consideraciones sobre la modalidad de pantalla completa VTxxx

Al igual que sucede con cualquier tipo de emulación, debe tener en cuenta determinadas consideraciones antes de utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet. Entre estas

consideraciones se encuentran algunas cuestiones de seguridad, así como condiciones de error posibles e indicadores luminosos. Si se familiariza con estas consideraciones, aprenderá a utilizar de forma eficaz la modalidad de pantalla completa VTxxx.

Además de las cuestiones sobre seguridad, hay otros aspectos que deben tenerse en cuenta antes de utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet. Al utilizar la modalidad de pantalla completa VTxxx, debe tener presentes las cuestiones siguientes:

- “Consideraciones sobre seguridad en la modalidad de pantalla completa VTxxx”
- “Consideraciones sobre Telnet y el paso a través de 5250 SNA en la modalidad de pantalla completa VTxxx”
- “Proceso de las peticiones del sistema para sesiones VTxxx”
- “Condiciones de error en el teclado 5250” en la página 65
- “Estaciones de pantalla y soporte VTxxx” en la página 65
- “Diferencias operativas entre los terminales VTxxx y 5250.” en la página 65
- “Características del teclado” en la página 66
- “Características de la pantalla” en la página 67
- “Tamaño de pantalla de VTxxx” en la página 67
- “Atributos de carácter de VTxxx” en la página 67

Consideraciones sobre seguridad en la modalidad de pantalla completa VTxxx

El número de intentos de inicio de sesión permitidos aumenta si Telnet configura automáticamente los dispositivos virtuales. El número de intentos de inicio de sesión es igual al número de intentos de inicio de sesión del sistema que están permitidos multiplicado por el número de dispositivos virtuales posibles.

El valor del sistema QMAXSIGN define el número de intentos de inicio de sesión permitidos en el sistema. El valor del sistema QAUTOVRT define el número de dispositivos virtuales que Telnet puede crear.

Consideraciones sobre Telnet y el paso a través de 5250 SNA en la modalidad de pantalla completa VTxxx

La plataforma System i soporta el paso a través de 5250. El paso a través de 5250 es parecido a Telnet, pero se ejecuta en una red de protocolo SNA (arquitectura de red de sistemas) en lugar de hacerlo en una red IP. El paso a través de 5250 utiliza pantallas virtuales para dirigir la salida a los dispositivos físicos, justo igual a como lo hace Telnet. En el paso a través de 5250, el sistema crea automáticamente dispositivos virtuales del mismo modo que lo hace para Telnet. Por consiguiente, el valor del sistema de dispositivos controla el número de dispositivos virtuales configurados automáticamente tanto para el paso a través de 5250 como para Telnet.

Proceso de las peticiones del sistema para sesiones VTxxx

El proceso de las peticiones del sistema para las sesiones VTxxx es algo distinto del de una estación de trabajo 5250 normal.

Cuando se pulsa la tecla Petición de sistema en una estación de trabajo 5250, aparece una línea de mandatos de petición del sistema en la parte inferior de la pantalla. Si pulsa la tecla Intro, aparece el menú Petición Sistema.

Para las sesiones VTxxx, cuando se llama a la función de petición del sistema, de inmediato se visualiza el menú Petición Sistema.

Condiciones de error en el teclado 5250

Determinadas condiciones de error hacen que un teclado 5250 se bloquee y que se visualice un código de error en la línea de mensajes. Un ejemplo de esta condición es pulsar una tecla cuando el cursor no está en un campo de entrada. En el caso de las sesiones VTxxx, estos errores hacen que se emita el sonido de una campana en la estación de trabajo VTxxx y que el teclado continúe desbloqueado.

Determinadas aplicaciones i5/OS también pueden bloquear el teclado 5250 y activar el indicador de entrada inhibida de 5250. El usuario debe pulsar la tecla de restaurar error para que el teclado quede desbloqueado. En las sesiones VTxxx, el bloqueo del teclado 5250 hace que se emita el sonido de una campana en el terminal VTxxx cada vez que se pulsa una tecla. Para desbloquear el teclado, debe pulsarse la tecla VTxxx correlacionada con la tecla de restaurar error. En la correlación de teclado de VTxxx predeterminada, la tecla Control-R se correlaciona con la tecla de restaurar error.

Estaciones de pantalla y soporte VTxxx

Cuando el sistema negocia el soporte VTxxx, el servidor Telnet transmite pantallas con un máximo de 24 filas por 80 columnas. El sistema cliente VTxxx ve estas pantallas de forma bastante parecida a como aparecen en una estación de trabajo 5251 Modelo 11. Sin embargo, hay algunas diferencias:

Una estación de trabajo 5251 tiene indicadores luminosos en la parte derecha que indican: sistema disponible, mensaje en espera, modalidad de teclado, modalidad de inserción y entrada inhibida.

El soporte de servidor VTxxx emula el indicador de sistema disponible colocando un asterisco en la columna 80 de la fila 9. En el caso de los indicadores de mensaje en espera, modalidad de inserción y entrada inhibida, el asterisco aparece en la columna 80 de las filas 11, 13 o 15. Cuando aparece un asterisco, el asterisco sobrescribe el carácter que antes se visualizaba en esa posición de la pantalla. De forma predeterminada, el servidor VTxxx no visualiza los indicadores luminosos. Puede habilitar o inhabilitar estos indicadores pulsando la secuencia de teclas correlacionada con la función de conmutación de indicadores luminosos. La secuencia de teclas predeterminada para esta función es ESC-T.

Notas:

- Si se utiliza un cliente VTxxx para conectarse al servidor Telnet, observe que puede que los indicadores de modalidad de inserción y entrada inhibida no siempre se visualicen tal como se ha descrito anteriormente. 5250 soporta la conexión como función local mientras que VTxxx no tiene este recurso. Sin embargo, los indicadores de sistema disponible y mensaje en espera se visualizarán correctamente.
- Una pantalla 5251 soporta un atributo de pantalla denominado separador de columna. El separador de columna es una línea vertical visualizada entre caracteres. Esta línea no ocupa un espacio de carácter. VTxxx no soporta este atributo. Si una aplicación de i5/OS genera una pantalla que utiliza el atributo de separador de columna, esa pantalla se visualiza en el sistema cliente VTxxx con el separador de columna correlacionado con el atributo de subrayado de VTxxx.

Diferencias operativas entre los terminales VTxxx y 5250.

Como usuario de Telnet, debe conocer las diferencias físicas y operativas que existen entre los terminales VTxxx y 5250.

5250 es un terminal de modalidad de bloques. Los datos escritos en un 5250 se acumulan en un almacenamiento intermedio y únicamente se envían a la plataforma System i cuando se pulsa una tecla AID (identificador de atención). Una tecla AID de un teclado 5250 es una tecla que inicia una función. En la lista siguiente se muestran las teclas AID de un teclado 5250:

- Borrar

- Función de mandato de 1 a 24
- Intro/Avance de registro
- Ayuda
- Imprimir
- Función de retroceso de registro
- Giro Abajo (Retroceso Página)
- Giro Arriba (Avance Página)

Los terminales VTxxx operan en una modalidad de caracteres. Los caracteres se transmiten inmediatamente al host cuando se pulsa una tecla.

Otra diferencia es la forma en que llegan los datos a la pantalla. El sistema escribe los datos en un terminal VTxxx carácter por carácter y los datos se ven llegar como corrientes de caracteres. Con el 5250, el sistema escribe los datos por bloques y de una sola vez cambia la totalidad o parte de la pantalla.

Características del teclado

Evite utilizar las teclas de desplazamiento del cursor de 5250. En su lugar, utilice las teclas de función asociadas a las palabras clave *CSRUP, *CSRDOWN, *CSRRIGHT y *CSRLEFT. De forma predeterminada estas son las teclas F13, F14, F15 y F16. Si emplea las teclas de desplazamiento del cursor de 5250, puede que la aplicación VTxxx que utilice no funcione como sería de esperar. Esto es debido a que el resultado de utilizar estas teclas no se transmite al sistema remoto hasta que se pulsa una tecla de identificador de atención (AID).

Por ejemplo, si se utiliza Telnet con el sistema System p y se obtiene la emulación VT220, el mandato SMIT (System Management Interface Tool) proporciona una interfaz dirigida por menús con AIX. Aquí las teclas de función asociadas a las palabras clave *CSRxx actúan de la misma forma que las teclas de desplazamiento del cursor. Sin embargo, las teclas de desplazamiento del cursor de 5250, aunque físicamente hacen avanzar el cursor por la pantalla y seleccionan correctamente la opción de SMIT, no hacen que la opción seleccionada quede resaltada. El resaltado en contraste invertido permanece con la primera opción del menú de SMIT, independientemente de la posición de la tecla.

Teclear un carácter de control en un teclado es distinto de teclear un carácter de control en un terminal VTxxx real. En un terminal VTxxx, pulse la tecla de control y manténgala pulsada al tiempo que pulsa el carácter asociado a la función de control.

Al utilizar el soporte de Telnet, se obtiene el resultado equivalente tecleando un indicador de control de 2 caracteres y a continuación pulsando la tecla de función asociada a la función predeterminada de envío sin retorno de carro (*SENDWOCR) (la tecla F11). Por ejemplo, si están en vigor la correlación de teclado predeterminada y los parámetros predeterminados del mandato STRTCPTELN, la función Control-C de VTxxx puede entrarse tecleando &C y a continuación pulsando la tecla F11. <F12> también puede entrar esta función, utilizando la correlación de teclado predeterminada. Este ejemplo ilustra el fundamento de la tecla *SENDWOCR y se incluye por si se utiliza una aplicación donde <F12> esté reasignada.

Utilice el parámetro CTLCHAR del mandato STRTCPTELN para seleccionar el carácter empleado para indicar un carácter de control. El valor predeterminado es &. Los caracteres &C deben ser los últimos caracteres que se escriban antes de pulsar la tecla de función *SENDWOCR; de lo contrario &C no se interpretará como un carácter de control. Un carácter de control solo se transmite cuando se pulsa la tecla de función *SENDWOCR. Es posible asignar caracteres de control de VTxxx que se utilicen con frecuencia a una tecla de función. A continuación figura un ejemplo descriptivo del mandato Control-C. Al utilizar un cliente Telnet para conectarse a un sistema System p, el sistema normalmente negocia la emulación VT220. La secuencia Control-C es importante en AIX para finalizar los mandatos de larga ejecución, tales como PING. Conviene que sepa efectuar este procedimiento antes de emitir cualquier mandato System p.

De forma predeterminada la secuencia es &C<F11>. Observe que debe entrar estas teclas rápidamente y puede que sean necesarios varios intentos para que la tarea de System p acepte la entrada.

Pulse la tecla de función asociada a la función *HIDE (F6 en la correlación de teclado predeterminada), si no desea visualizar los caracteres escritos. Utilice esta función al escribir una contraseña.

Si desea que los caracteres que se hayan escrito se envíen al sistema remoto para procesarse sin pulsar la tecla Intro, pulse la tecla de función asociada a la función *SENDWOCR (F11 en la correlación de teclado predeterminada).

A menudo resulta de utilidad poder recordar los mandatos entrados anteriormente. En la plataforma System i, la tecla F9 suele proporcionar esta función. En AIX, esta función se puede activar tecleando el mandato set -o vi y pulsando Intro. Tras esta acción, podrá empezar a recuperar mandatos con la secuencia Esc-K. Para ejecutar esta secuencia empleando la correlación de teclado predeterminada mientras está en emulación VTxxx, debe utilizar la secuencia <F5>k<F11>. El carácter Esc inicia la recuperación de mandatos. A continuación utilice la letra k para recuperar más mandatos. Mientras se opera en esta modalidad, se aplican los mandatos H para derecha, L para izquierda, X para suprimir, I para insertar y R para sustituir. La secuencia <F5>i<F11> desactiva esta función.

Características de la pantalla

El carácter situado en la posición inmediatamente anterior a la posición del cursor siempre estará en blanco. El carácter real se guarda internamente y se muestra cuando se renueva la pantalla con el cursor en otra posición.

Una aplicación de VTxxx que utiliza la fila 1 y la columna 1 de la pantalla no funciona igual al utilizar el soporte de cliente Telnet. La mayoría de las estaciones de pantalla de tipo 5250 no admiten entradas en la fila 1 y columna 1. Si la aplicación de VTxxx coloca el cursor en la fila 1 y columna 1, el sistema automáticamente coloca el cursor en la fila 1 y columna 2.

Debido a diferencias de arquitectura, el sistema omite determinados mandatos o secuencias no soportados. Los juegos de caracteres transferibles en sentido descendente son un ejemplo de ello.

Tamaño de pantalla de VTxxx

La modalidad de pantalla completa Telnet VTxxx proporciona soporte para los tamaños de pantalla siguientes:

- En estaciones de pantalla 3180:
 - Las pantallas VTxxx 24 x 80 deben visualizarse como 24 x 80.
 - Las pantallas VTxxx 24 x 132 deben visualizarse como 24 x 132.
- En estaciones de pantalla 5250:
 - Las pantallas VTxxx 24 x 80 deben visualizarse como 24 x 80.
 - Las pantallas 24 x 132 requieren la tecla de función asignada a *SHIFTDSP (F10 en la correlación de teclado predeterminada) para desplazar la información en la pantalla a la derecha o a la izquierda.

Atributos de carácter de VTxxx

Un terminal VTxxx da soporte a los atributos siguientes:

- Parpadeo
- Negrita
- Contraste invertido
- Subrayado
- Cualquier combinación de los atributos anteriores

La corriente de datos 5250 da soporte a los atributos anteriores de modo que una estación de pantalla 5250 puede representar todos los atributos de VTxxx. Sin embargo, hay algunas limitaciones:

- La corriente de datos 5250 solo puede dar soporte a tres de los atributos de carácter a la vez. Los atributos de subrayado, parpadeo y contraste invertido se visualizan cuando el sistema remoto selecciona todos los atributos de VTxxx a la vez. Una estación de pantalla 5250 no puede visualizar la combinación de subrayado, negrita y contraste invertido. Se visualizan los atributos de subrayado y contraste invertido cuando una aplicación de VTxxx selecciona esta combinación.
- El byte de atributo ocupa un espacio en las estaciones de pantalla 5250 que no dan soporte a los atributos ampliados. Los atributos no ocupan espacio en un terminal VTxxx. Esto significa que si selecciona atributos de carácter, no verá todos los datos que se visualizan en la pantalla 5250. Al recibir datos de VTxxx que deben visualizarse con atributos de carácter, el byte de atributo de 5250 recubre la posición anterior a los datos. El carácter que se visualizaba en esa posición se pierde. Si un carácter debe visualizarse en la fila 1 y columna 1 con los atributos establecidos, ese carácter no se visualiza. Puede elegir que no se visualicen los atributos de carácter especificando DSPCHRATTR(*NO) en el mandato STRTCPTLN. Esto le permite ver todos los datos en la pantalla sin atributos.

Nota: esta restricción no es válida para las pantallas que dan soporte a los atributos ampliados tales como la pantalla 3477.

Indicador de teclado de VT100

Un terminal VT100 tiene un indicador L1 que puede programarse para distintas aplicaciones. El soporte de Telnet no emula este indicador.

Conceptos relacionados

“Inicio de una sesión de cliente Telnet VTxxx” en la página 62

Puede iniciar una sesión de cliente Telnet utilizando la emulación VTxxx. Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

“Determinación de problemas con Telnet” en la página 91

Necesita información de diagnóstico para solucionar los problemas de Telnet, que incluye un diagrama de flujo para el análisis de los problemas del sistema, y necesita una lista del material necesario para informar de problemas de Telnet.

Opciones de emulación de VTxxx

Al utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet, hay varios procedimientos opcionales que puede llevar a cabo para personalizar el tipo de emulación. Puede visualizar la correlación de teclado actual y, a continuación, decidir si desea cambiarla. Asimismo, puede cambiar los caracteres de control al utilizar la modalidad de pantalla completa VT220.

Visualización de una correlación de teclado de VTxxx

Para visualizar la correlación de teclado actual, utilice el mandato de visualizar correlación de teclado de VT (DSPVTMAP). Este mandato no tiene parámetros. Se visualizan las teclas VTxxx que están correlacionadas con las funciones de i5/OS.

El mandato DSPVTMAP solo es válido cuando se le llama desde dentro de una sesión de servidor Telnet que opera en modalidad de pantalla completa VTxxx.

Teclee DSPVTMAP para ver la pantalla siguiente y a continuación pulse la tecla Avance Página para ver las pantallas adicionales. Puede visualizar la correlación de teclado de VT con la opción 3 del menú Configurar TCP/IP TELNET.

Establecimiento de una correlación de teclado de VTxxx

Para cambiar la correlación de teclado predeterminada, utilice el mandato de establecer correlación de teclado de VT (SETVTMAP). Este mandato también está disponible mediante la opción 5, de establecer

correlación de teclado de VT, del menú Configurar TCP/IP TELNET. La correlación de teclado predeterminada especificada se restaura tras ejecutar el mandato sin utilizar ningún parámetro especificado por el usuario. Puede especificar hasta 4 de los valores especiales definidos para cada parámetro. No se puede emplear un valor especial para especificar más de una función de i5/OS.

Cambio de una correlación de teclado de VTxxx

Al igual que SETVTMAP, el mandato de cambiar correlación de teclado de VT (CHGVTMAP) permite personalizar la correlación de teclado al conectarse a un servidor Telnet en modalidad VTxxx. En cambio, de forma predeterminada los parámetros del mandato CHGVTMAP son los valores establecidos actualmente. Salvo por esta diferencia, los dos mandatos son idénticos.

Acomodación automática de VTxxx

El servidor VTxxx requiere que el cliente VTxxx tenga activada la opción de acomodación automática. Cuando la acomodación automática está activa, al escribir un carácter en la columna 80 de VTxxx el cursor se desplaza a la columna 1 de la línea siguiente. Consulte la documentación del cliente VTxxx para obtener más información sobre cómo establecer esta opción.

Caracteres de control de VT220

Cuando se negocia la emulación VT220 de 8 bits, los caracteres de X'80' a X'9F' están protegidos como caracteres de control C1 tal como define la arquitectura en el manual DEC VT220 Programmer Reference Manual. Esto puede hacer que el sistema interprete los caracteres sucesivos de una corriente de datos como datos en relación con estos caracteres. Si el sistema negocia VT220 de 7 bits o VT100, el rango completo de caracteres de X'80' a X'F' está disponible para la conversión de caracteres. Interprete el rango de X'80' a X'9F' como caracteres de control C1 en la modalidad de control VT220 de 8 bits únicamente.

Esto es especialmente importante para el soporte de idioma nacional (NLS), ya que varios idiomas distintos del inglés utilizan estos valores para caracteres específicos del idioma. En estos casos, puede que la emulación VT220 de 8 bits no funcione como se prevé.

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx” en la página 30
El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

Referencia relacionada

“Valores de las teclas VTxxx”

Los valores de las teclas VTxxx proporcionan la correlación de teclado para el soporte de la emulación VTxxx. El soporte de sesión de cliente para las modalidades VT100 y VT220 proporciona una correlación de teclado primaria y otra alternativa.

Valores de las teclas VTxxx

Los valores de las teclas VTxxx proporcionan la correlación de teclado para el soporte de la emulación VTxxx. El soporte de sesión de cliente para las modalidades VT100 y VT220 proporciona una correlación de teclado primaria y otra alternativa.

Para dar cabida a las prestaciones de teclado adicionales de la modalidad VT220, puede guardar la correlación de teclado. Utilizando la tecla F6 en la pantalla Cambiar correlación de teclado de VTxxx, puede guardar todos los cambios efectuados en estas correlaciones de teclado para sesiones posteriores. La información se guarda en el perfil de usuario y se aplicará automáticamente la próxima vez que se active la emulación Telnet VTxxx.

La opción de teclado que seleccione en el menú Enviar Funciones de Control TELNET determinará la correlación de teclado que utilizará. Las figuras de la 2 a la 9 muestran las funciones de VTxxx que corresponden a la tecla AID de 5250. En la lista siguiente se indica el número de opción y las figuras correspondientes:

- La Figura 1 y la Figura 2 en la página 71 muestran la opción 6 (Cambiar correlación de teclado primaria de VT100).
- La Figura 3 en la página 71 y la Figura 4 en la página 72 muestran la opción 7 (Cambiar correlación de teclado alternativa de VT100).
- La Figura 5 en la página 72 y la Figura 6 en la página 73 muestran la opción 8 (Cambiar correlación de teclado primaria de VT220).
- La Figura 7 en la página 73 y la Figura 8 en la página 74 muestran la opción 9 (Cambiar correlación de teclado alternativa de VT220).

El nivel de soporte negociado entre la plataforma System i y el servidor Telnet determina las opciones que se visualizan en el menú Enviar Funciones de Control TELNET. El menú visualiza las opciones 6 y 7 si inicialmente se negocia el soporte en modalidad de pantalla completa VT100. El menú visualiza las opciones 8 y 9 si inicialmente se negocia el soporte en modalidad de pantalla completa VT220.

Nota: no existe ninguna diferencia en los valores predeterminados de las correlaciones de teclado primaria y alternativa de VT100.

Las figuras siguientes muestran las correlaciones de teclado predeterminadas. Puede cambiar cualquiera de los valores. Si pulsa la tecla Intro, los cambios se guardarán únicamente para la sesión actual. Si pulsa F6 (Guardar), los cambios se guardarán de forma permanente y entrarán en vigor la próxima vez que inicie una sesión Telnet VTxxx.

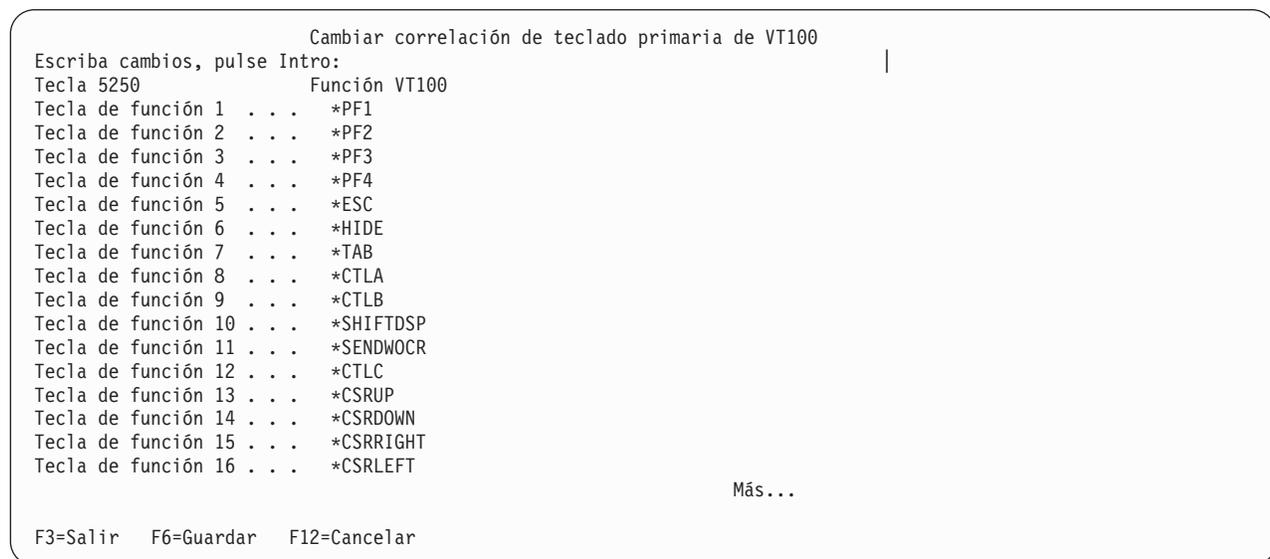


Figura 1. Cambiar correlación de teclado primaria de VT100 (Pantalla 1)

```
                                Cambiar correlación de teclado primaria de VT100
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT100
Tecla de función 17 . . . *CTLD
Tecla de función 18 . . . *CTLE
Tecla de función 19 . . . *CTLF
Tecla de función 20 . . . *CTLG
Tecla de función 21 . . . *CTLH
Tecla de función 22 . . . *CTLI
Tecla de función 23 . . . *CTLJ
Tecla de función 24 . . . *CTLK
Tecla de avance . . . . *CTLL
Tecla de retroceso . . . *CTLM

                                Final

F3=Salir  F6=Guardar  F12=Cancelar
```

Figura 2. Cambiar correlación de teclado primaria de VT100 (Pantalla 2)

```
                                Cambiar correlación de teclado alternativa de VT100
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT100
Tecla de función 1 . . . . *PF1
Tecla de función 2 . . . . *PF2
Tecla de función 3 . . . . *PF3
Tecla de función 4 . . . . *PF4
Tecla de función 5 . . . . *ESC
Tecla de función 6 . . . . *HIDE
Tecla de función 7 . . . . *TAB
Tecla de función 8 . . . . *CTLA
Tecla de función 9 . . . . *CTLB
Tecla de función 10 . . . . *SHIFTDSP
Tecla de función 11 . . . . *SENDWOCR
Tecla de función 12 . . . . *CTLC
Tecla de función 13 . . . . *CSRUP
Tecla de función 14 . . . . *CSRDOWN
Tecla de función 15 . . . . *CSRRIGHT
Tecla de función 16 . . . . *CSRLEFT

                                Más...

F3=Salir  F6=Guardar  F12=Cancelar
```

Figura 3. Cambiar correlación de teclado alternativa de VT100 (Pantalla 1)

```

                                Cambiar correlación de teclado alternativa de
VT100
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT100
Tecla de función 17 . .        *CTLD
Tecla de función 18 . .        *CTLE
Tecla de función 19 . .        *CTLF
Tecla de función 20 . .        *CTLG
Tecla de función 21 . .        *CTLH
Tecla de función 22 . .        *CTLI
Tecla de función 23 . .        *CTLJ
Tecla de función 24 . .        *CTLK
Tecla de avance . . . .        *CTLL
Tecla de retroceso . . . .     *CTLM

                                Final

F3=Salir  F6=Guardar  F12=Cancelar

```

Figura 4. Cambiar correlación de teclado alternativa de VT100 (Pantalla 2)

Puede pasar de la correlación de teclado primaria a la alternativa, y a la inversa, durante una sesión VTxxx mediante la tecla de función asignada a las palabras clave *KEYPRI y *KEYALT. Puede asignar estas palabras clave a cualquiera de las teclas de función de 5250 disponibles. Se recomienda asignar *KEYPRI a la tecla de función de 5250 Retroceso Página y *KEYALT a la tecla de función de 5250 Avance Página para las correlaciones de teclado primaria y alternativa.

```

                                Cambiar correlación de teclado primaria de VT220
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT220
Tecla de función 1 . . . .     *PF1
Tecla de función 2 . . . .     *PF2
Tecla de función 3 . . . .     *PF3
Tecla de función 4 . . . .     *PF4
Tecla de función 5 . . . .     *ESC
Tecla de función 6 . . . .     *HIDE
Tecla de función 7 . . . .     *TAB
Tecla de función 8 . . . .     *CTLA
Tecla de función 9 . . . .     *CTLB
Tecla de función 10 . . . .    *SHIFTDSP
Tecla de función 11 . . . .    *SENDWOCR
Tecla de función 12 . . . .    *CTLC
Tecla de función 13 . . . .    *CSRUP
Tecla de función 14 . . . .    *CSRDOWN
Tecla de función 15 . . . .    *CSRRIGHT
Tecla de función 16 . . . .    *CSRLEFT

                                Más...

F3=Salir  F6=Guardar  F12=Cancelar

```

Figura 5. Cambiar correlación de teclado primaria de VT220 (Pantalla 1)

```

                                Cambiar correlación de teclado primaria de VT220
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT220
Tecla de función 17 . . . *CTLD
Tecla de función 18 . . . *CTLE
Tecla de función 19 . . . *CTLF
Tecla de función 20 . . . *CTLG
Tecla de función 21 . . . *CTLH
Tecla de función 22 . . . *CTLI
Tecla de función 23 . . . *CTLJ
Tecla de función 24 . . . *CTLK
Retroceso página . . . *KEYPRI
Avance página . . . . . *KEYALT

                                Final

F3=Salir  F6=Guardar  F12=Cancelar

```

Figura 6. Cambiar correlación de teclado primaria de VT220 (Pantalla 2)

```

                                Cambiar correlación de teclado alternativa de
VT220
Escriba cambios, pulse Intro:
Tecla 5250                      Función VT220
Tecla de función 1 . . . *PF1
Tecla de función 2 . . . *PF2
Tecla de función 3 . . . *PF3
Tecla de función 4 . . . *PF4
Tecla de función 5 . . . *ESC
Tecla de función 6 . . . *HIDE
Tecla de función 7 . . . *TAB
Tecla de función 8 . . . *CTLA
Tecla de función 9 . . . *CTLB
Tecla de función 10 . . . *SHIFTDSP
Tecla de función 11 . . . *SENDWOCR
Tecla de función 12 . . . *CTLC
Tecla de función 13 . . . *CSRUP
Tecla de función 14 . . . *CSRDOWN
Tecla de función 15 . . . *CSRRIGHT
Tecla de función 16 . . . *CSRLEFT

                                Más...

F3=Salir  F6=Guardar  F12=Cancelar

```

Figura 7. Cambiar correlación de teclado alternativa de VT220 (Pantalla 1)

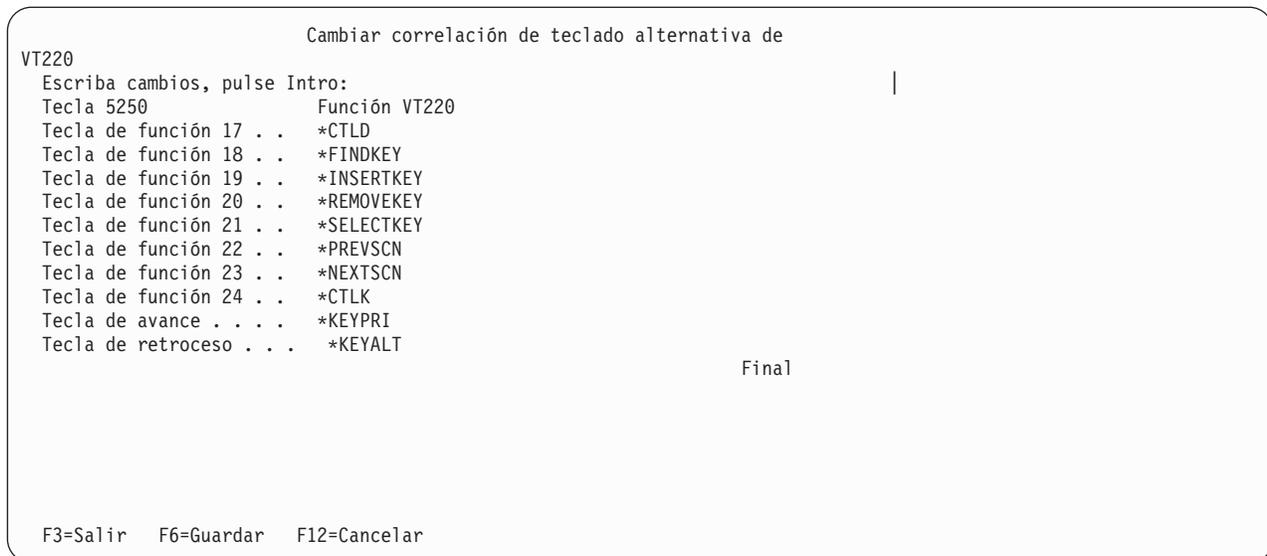


Figura 8. Cambiar correlación de teclado alternativa de VT220 (Pantalla 2)

Puede especificar distintos tipos de información de VTxxx para cambiar la correlación de teclado. A continuación se indican algunos ejemplos:

Datos de tipo carácter: Puede asignar una serie de caracteres a una tecla de función. Por ejemplo, supongamos que está en un modelo System i y que está utilizando Telnet para establecer una conexión al sistema System p. Para asignar la serie de caracteres `set term=vt100` a la tecla de función siguiente:

```
Tecla de función 24 . . *CTLK
```

En el sistema, puede escribir:

```
Tecla de función 24 . . 'set term=vt100'
```

Esto permite pulsar una tecla de función en lugar de tener siempre que escribir esa serie de caracteres.

Al pulsar la tecla de función durante una sesión VTxxx, la serie de caracteres asignada a esa tecla de función se transmite al sistema remoto con los caracteres de retorno de carro y salto de línea añadidos. Si escribe información antes de pulsar la tecla de función, el sistema añade la serie de caracteres a la información que escribe. Esto permite asignar una serie de mandato utilizada con frecuencia a una tecla de función. Los datos de tipo carácter que escribe se correlacionan de EBCDIC a ASCII, antes de transmitirse al sistema remoto.

Palabras clave de tecla de control: Puede asignar una pulsación de control de VTxxx a una tecla de función mediante una palabra clave definida. Por ejemplo, si deseara asignar una pulsación de control de VTxxx distinta a la tecla de función siguiente:

```
Tecla de función 24 . . *CTLK
```

Puede escribir:

```
Tecla de función 24 . . *CTLZ
```

Al pulsar la tecla de función, el nuevo carácter de control asignado a la tecla de función se transmite al sistema remoto. Si escribe información antes de pulsar la tecla de función, el carácter de control se añade a la información escrita y se transmite al sistema remoto.

Datos hexadecimales: Puede asignar una serie hexadecimal a una tecla de función. Al pulsar la tecla de función, los datos hexadecimales se transmiten al sistema remoto. Los caracteres de retorno de carro y salto de línea no se añaden a los datos hexadecimales. Si escribe información antes de pulsar la tecla de

función, los datos hexadecimales se añaden a la información escrita y se transmiten al sistema remoto. Esto permite escribir un carácter que no esté en el teclado 5250 (por ejemplo, un corchete). Para asignar una serie hexadecimal, escriba X seguido de una serie entrecomillada de caracteres hexadecimales, como por ejemplo X'1A1A'. Los datos hexadecimales no se correlacionan antes de transmitirse al sistema remoto.

Funciones de control de i5/OS locales: Puede asignar una palabra clave que se manejará localmente dentro de la sesión de cliente Telnet. Estas asignaciones o correlaciones puede que no originen la transmisión de tráfico de corriente de datos ASCII a la sesión de servidor Telnet remoto. Estas funciones locales de control son *HIDE, *SHIFTDSP, *KEYPRI y *KEYALT. La función de envío sin retorno de carro (*SENDWOCR) también es una función local, pero en este caso las corrientes de datos ASCII se transmiten a la sesión de servidor Telnet remoto.

Conceptos relacionados

“Inicio de una sesión de cliente Telnet VTxxx” en la página 62

Puede iniciar una sesión de cliente Telnet utilizando la emulación VTxxx. Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

Referencia relacionada

“Opciones de emulación de VTxxx” en la página 68

Al utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet, hay varios procedimientos opcionales que puede llevar a cabo para personalizar el tipo de emulación. Puede visualizar la correlación de teclado actual y, a continuación, decidir si desea cambiarla. Asimismo, puede cambiar los caracteres de control al utilizar la modalidad de pantalla completa VT220.

Soporte de idioma nacional de VTxxx:

El soporte de idioma nacional de VTxxx proporciona métodos alternativos para seleccionar la correlación de caracteres entre clientes y sistemas con la emulación VTxxx.

Estos métodos son los siguientes:

- Identificador de juego de caracteres (CCSID)
- Modalidad multinacional
- Modalidad nacional

Si ninguno de estos métodos es adecuado, puede configurar y especificar sus propias tablas de correlación definidas por el usuario.

Nota: el soporte de VTxxx está limitado a un subconjunto de idiomas de juego de caracteres de un solo byte (SBCS). Más adelante en este tema encontrará una lista de los idiomas soportados. Cualquiera de las tablas de conversión de estos idiomas de un solo byte soportados puede modificarse para establecer la correlación con el idioma de un solo byte que se prefiera y, a continuación, identificarse en el parámetro adecuado para iniciar el cliente Telnet.

La selección de modalidad se efectúa con el parámetro CCSID del mandato Arrancar TCP/IP Telnet (STRTCPTLN). Los parámetros de tabla ASCII/EBCDIC de entrada (TBLVTIN) y tabla EBCDIC/ASCII de salida (TBLVTOU) de este mandato permiten especificar tablas de correlación definidas por el usuario. Si no son necesarias, el valor predeterminado de *CCSID hace que se lleve a cabo la correlación de caracteres utilizando la modalidad especificada en el parámetro CCSID.

Modalidad multinacional de VTxxx

La modalidad multinacional soporta el juego de caracteres multinacional DEC, que es un juego de caracteres de 8 bits que contiene la mayoría de los caracteres utilizados en los principales idiomas europeos. El juego de caracteres ASCII se incluye en el juego de caracteres multinacional DEC. El juego de caracteres DEC se emplea de forma predeterminada.

Modalidad nacional de VTxxx:

La modalidad nacional de VTxxx soporta el juego de caracteres de sustitución nacional, que es un grupo de juegos de caracteres de 7 bits.

Solo hay un juego de caracteres del grupo disponible para ser utilizado en un momento dado cualquiera. VT220 también da soporte al juego de caracteres ASCII de 7 bits estándar como parte de la modalidad nacional. El terminal VT220 soporta los siguientes idiomas nacionales en juegos de caracteres ASCII de 7 bits:

- Inglés británico
- Danés
- Holandés
- Finlandés
- Francés
- Francés/Canadiense
- Alemán
- Italiano
- Noruego
- Español
- Sueco
- Suizo
- Inglés estadounidense

Para utilizar una modalidad nacional, el sistema necesita tablas de correlación para correlacionar los datos ASCII de entrada con el código de intercambio decimal ampliado codificado en binario (EBCDIC) y los datos EBCDIC de salida con ASCII al operar en modalidad VTxxx de pantalla completa.

Utilice el parámetro de identificador de conjunto de caracteres codificados (CCSID) del mandato Telnet para seleccionar una modalidad nacional, esto es, una tabla de correlación NLS.

Especificar un valor numérico que represente un valor de CCSID registrado del rango del 1 al 65.553 es un modo de identificar la tabla de correlación adecuada. El manual AS/400 International Application Development V4R2  contiene información detallada sobre los CCSID registrados.

Las tablas de correlación NLS se generan de forma dinámica en un sistema remoto la primera vez que se utiliza Telnet y se basan en los juegos de caracteres de sustitución nacionales DEC. Dado que los juegos de caracteres están basados en 7 bits, solo pueden contener los caracteres exclusivos de una región. Como el juego de caracteres multinacional DEC está basado en 8 bits, permite incluir caracteres exclusivos de un grupo de países.

Identificación de objetos de tabla

Puede identificar los objetos de tabla (*TBL) mediante el mandato Trabajar con objeto: WRKOBJ OBJ(QUSRSYS/Q*) OBJTYPE(*TBL)

Todos los objetos de tabla del sistema están en la biblioteca QUSRSYS.

Los objetos de tabla se denominan *Qxxxxyyyzzz*, donde *xxx* es la página de códigos origen, *yyy* es el juego de caracteres destino y *zzz* es la página de códigos destino.

Estas son las directrices de la tabla de salida (de EBCDIC a ASCII):

- El ID de página de códigos origen se toma del ID de página de códigos de QCHRID en la descripción del mensaje CPX8416 (utilice WRKMSGD CPX8416 para visualizarlo), 37 en la figura siguiente de un sistema basado en inglés estadounidense.
- El juego de caracteres y la página de códigos destino se obtienen del parámetro CCSID utilizado con el mandato Telnet.

Estas son las directrices de la tabla de entrada (ASCII a EBCDIC):

- El ID de página de códigos origen se deriva del parámetro CCSID utilizado con el mandato Telnet.
- El juego de caracteres y la página de códigos destino se toman del ID de juego de caracteres y del ID de página de códigos de QCHRID en la descripción del mensaje CPX8416 (utilice WRKMSGD CPX8416 para visualizarlo), 697 y 37 en la figura siguiente de un sistema basado en inglés estadounidense.

```

Sistema: SYSNAM01
ID mensaje . . . . . : CPX8416
Archivo mensajes . . . . . : QCPFMSG
Biblioteca . . . . . : QSYS

Mensaje . . . . . :
QCHRID 697 37 QCURSYM $ QDATFMT MDY QDATSEP /
QDECFMT QLEAPADJ 0 QCCSID 37 QTIMSEP : QLANGID ENU
QCNTYRID US QIGCCDEFNT *NONE

```

Figura 9. Mensaje CPX8416 de ejemplo

CCSID	ID real de juego de caracteres	ID de tabla de juego de caracteres	ID real de página de códigos	ID real de página de códigos
MULTINAT	1290	A05	1100	A5U
BRITISH	1291	A06	1101	A5V
1292	A07	1102	A5W	
1293	A08	1103	A5X	
289	289	1104	A5Y	
1192	A8E	1020	A3M	
265	265	1011	A3D	
293	293	1012	A3E	
1297	BAB	1107	A52	
1195	A8H	1023	A3P	
1296	BAA	1106	A51	
1193	A8F	1021	A3N	

Por ejemplo, en un sistema de inglés británico con el QCHRID 697 285 (juego de caracteres 697 y página de códigos 285) en el mensaje CPX8416 que utiliza Telnet con CCSID(*BRITISH), las tablas tendrán los nombres siguientes:

- De salida (EBCDIC a ASCII) Q285A06A5V
- De entrada (ASCII a EBCDIC) QA5V697285

Tablas de correlación definidas por el usuario (modalidad ASCII)

Cuando las tablas de correlación multinacional o NLS no satisfacen las necesidades de un usuario, pueden crearse y emplearse tablas de correlación de caracteres definidas por el usuario.

Asimismo, se pueden especificar tablas de correlación definidas por el usuario con los parámetros de tabla de ASCII a EBCDIC de salida (TBLVTOUT) y tabla de ASCII a EBCDIC de entrada (TBLVTIN) del mandato STRTCPTELN. Se puede especificar una tabla de correlación definida por el usuario o bien para la tabla de correlación de salida o bien para la tabla de correlación de entrada y, a continuación, utilizar el valor predeterminado del sistema para la otra.

Conceptos relacionados

“Inicio de una sesión de cliente Telnet VTxxx” en la página 62

Puede iniciar una sesión de cliente Telnet utilizando la emulación VTxxx. Debe iniciar el servidor Telnet en el sistema remoto (el sistema al que desea conectarse mediante Telnet).

Teclado numérico:

A continuación se especifican las teclas del teclado numérico auxiliar que normalmente transmiten los códigos de números, puntos, signos menos y comas.

Tabla 13. Teclas del teclado numérico auxiliar

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*NUM0	Modalidad VT52	X'30' o X'1B3F70 ¹	Tecla 0 del teclado numérico
*NUM0	Modalidad VT100 o VT220 de 7 bits	X'30' o X'1B4F70 ¹	Tecla 0 del teclado numérico
*NUM0	Modalidad VT220 de 8 bits	X'30' o X'8F70 ²	Tecla 0 del teclado numérico
*NUM1	Modalidad VT52	X'31' o X'1B3F71 ¹	Tecla 1 del teclado numérico
*NUM1	Modalidad VT100 o VT220 de 7 bits	X'31' o X'1B4F71 ¹	Tecla 1 del teclado numérico
*NUM1	Modalidad VT220 de 8 bits	X'31' o X'8F71 ²	Tecla 1 del teclado numérico
*NUM2	Modalidad VT52	X'32' o X'1B3F72 ¹	Tecla 2 del teclado numérico
*NUM2	Modalidad VT100 o VT220 de 7 bits	X'32' o X'1B4F72 ¹	Tecla 2 del teclado numérico
*NUM2	Modalidad VT220 de 8 bits	X'32' o X'8F72 ²	Tecla 2 del teclado numérico
*NUM3	Modalidad VT52	X'33' o X'1B3F73 ¹	Tecla 3 del teclado numérico
*NUM3	Modalidad VT100 o VT220 de 7 bits	X'33' o X'1B4F73 ¹	Tecla 3 del teclado numérico
*NUM3	Modalidad VT220 de 8 bits	X'33' o X'8F73 ²	Tecla 3 del teclado numérico
*NUM4	Modalidad VT52	X'34' o X'1B3F74 ¹	Tecla 4 del teclado numérico
*NUM4	Modalidad VT100 o VT220 de 7 bits	X'34' o X'1B4F74 ¹	Tecla 4 del teclado numérico
*NUM4	Modalidad VT220 de 8 bits	X'34' o X'8F74 ²	Tecla 4 del teclado numérico
*NUM5	Modalidad VT52	X'35' o X'1B3F75 ¹	Tecla 5 del teclado numérico

Tabla 13. Teclas del teclado numérico auxiliar (continuación)

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*NUM5	Modalidad VT100 o VT220 de 7 bits	X'35' o X'1B4F75 ¹	Tecla 5 del teclado numérico
*NUM5	Modalidad VT220 de 8 bits	X'35' o X'8F75 ²	Tecla 5 del teclado numérico
*NUM6	Modalidad VT52	X'36' o X'1B3F76 ¹	Tecla 6 del teclado numérico
*NUM6	Modalidad VT100 o VT220 de 7 bits	X'36' o X'1B4F76 ¹	Tecla 6 del teclado numérico
*NUM6	Modalidad VT220 de 8 bits	X'36' o X'8F76 ²	Tecla 6 del teclado numérico
*NUM7	Modalidad VT52	X'37' o X'1B3F77 ¹	Tecla 7 del teclado numérico
*NUM7	Modalidad VT100 o VT220 de 7 bits	X'37' o X'1B4F77 ¹	Tecla 7 del teclado numérico
*NUM7	Modalidad VT220 de 8 bits	X'37' o X'8F77 ²	Tecla 7 del teclado numérico
*NUM8	Modalidad VT52	X'38' o X'1B3F78 ¹	Tecla 8 del teclado numérico
*NUM8	Modalidad VT100 o VT220 de 7 bits	X'38' o X'1B4F78 ¹	Tecla 8 del teclado numérico
*NUM8	Modalidad VT220 de 8 bits	X'38' o X'8F78 ²	Tecla 8 del teclado numérico
*NUM9	Modalidad VT52	X'39' o X'1B3F79 ¹	Tecla 9 del teclado numérico
*NUM9	Modalidad VT100 o VT220 de 7 bits	X'39' o X'1B4F79 ¹	Tecla 9 del teclado numérico
*NUM9	Modalidad VT220 de 8 bits	X'39' o X'8F79 ²	Tecla 9 del teclado numérico
*NUMMINUS	Modalidad VT52	X'2D' o X'1B3F6D ¹	Tecla menos del teclado numérico
*NUMMINUS	Modalidad VT100 o VT220 de 7 bits	X'2D' o X'1B4F6D ¹	Tecla menos del teclado numérico
*NUMMINUS	Modalidad VT220 de 8 bits	X'2D' o X'8F6D ²	Tecla menos del teclado numérico
*NUMCOMMA	Modalidad VT52	X'2C' o X'1B3F6C ¹	Tecla de coma del teclado numérico
*NUMCOMMA	Modalidad VT100 o VT220 de 7 bits	X'2C' o X'1B4F6C ¹	Tecla de coma del teclado numérico
*NUMCOMMA	Modalidad VT220 de 8 bits	X'2C' o X'8F6C ²	Tecla de coma del teclado numérico
*NUMPERIOD	Modalidad VT52	X'2E' o X'1B3F6E ¹	Tecla de punto del teclado numérico
*NUMPERIOD	Modalidad VT100 o VT220 de 7 bits	X'2E' o X'1B4F6E ¹	Tecla de punto del teclado numérico
*NUMPERIOD	Modalidad VT220 de 8 bits	X'2E' o X'8F6E ²	Tecla de punto del teclado numérico

Tabla 13. Teclas del teclado numérico auxiliar (continuación)

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*PF1	Modalidad VT52	X'1B50'	Tecla PF1 del teclado numérico
*PF1	Modalidad VT100 o VT220 de 7 bits	X'1B4F50'	Tecla PF1 del teclado numérico
*PF1	Modalidad VT220 de 8 bits	X'8F50' ²	Tecla PF1 del teclado numérico
*PF2	Modalidad VT52	X'1B51'	Tecla PF2 del teclado numérico
*PF2	Modalidad VT100 o VT220 de 7 bits	X'1B4F51'	Tecla PF2 del teclado numérico
*PF2	Modalidad VT220 de 8 bits	X'8F51' ²	Tecla PF2 del teclado numérico
*PF3	Modalidad VT52	X'1B52'	Tecla PF3 del teclado numérico
*PF3	Modalidad VT100 o VT220 de 7 bits	X'1B4F52'	Tecla PF3 del teclado numérico
*PF3	Modalidad VT220 de 8 bits	X'8F52' ²	Tecla PF3 del teclado numérico
*PF4	Modalidad VT52	X'1B53'	Tecla PF4 del teclado numérico
*PF4	Modalidad VT100 o VT220 de 7 bits	X'1B4F53'	Tecla PF4 del teclado numérico
*PF4	Modalidad VT220 de 8 bits	X'8F53' ²	Tecla PF4 del teclado numérico

¹- Se transmite un solo carácter cuando se está en modalidad de teclado numérico; cuando se está en modalidad de teclado de aplicación se envía una secuencia de 3 caracteres.

²- Esta secuencia es una versión abreviada de la secuencia de 7 bits. Se presenta cuando opera en modalidad de 8 bits, a la que puede llamar el servidor o host VT220 remoto, o que puede especificar en el parámetro ASCOPRMOD del mandato Arrancar TCP/IP TELNET (STRTCPTELN).

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx” en la página 30
El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

Teclado de edición:

En esta tabla se muestran las teclas que transmiten los códigos de las teclas del teclado de edición.

Tabla 14. Teclas que transmiten los códigos de las teclas del teclado de edición

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*CSRUP	Modalidad VT52	X'1B41'	Tecla de cursor arriba
*CSRUP	Restablecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B5B41'	Tecla de cursor arriba

Tabla 14. Teclas que transmiten los códigos de las teclas del teclado de edición (continuación)

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*CSRUP	Restablecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'9B41'	Tecla de cursor arriba
*CSRUP	Establecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B4F41'	Tecla de cursor arriba
*CSRUP	Establecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'8F41'	Tecla de cursor arriba
*CSRDOWN	Modalidad VT52	X'1B42'	Tecla de cursor abajo
*CSRDOWN	Restablecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B5B42'	Tecla de cursor abajo
*CSRDOWN	Restablecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'9B42'	Tecla de cursor abajo
*CSRDOWN	Establecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B4F42'	Tecla de cursor abajo
*CSRDOWN	Establecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'8F42'	Tecla de cursor abajo
*CSRRIGHT	Modalidad VT52	X'1B43'	Tecla de cursor derecha
*CSRRIGHT	Restablecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B5B43'	Tecla de cursor derecha
*CSRRIGHT	Restablecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'9B43'	Tecla de cursor derecha
*CSRRIGHT	Establecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B4F43'	Tecla de cursor derecha
*CSRRIGHT	Establecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'8F43'	Tecla de cursor derecha
*CSRLEFT	Modalidad VT52	X'1B44'	Tecla de cursor izquierda
*CSRLEFT	Restablecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B5B44'	Tecla de cursor izquierda
*CSRLEFT	Restablecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'9B44'	Tecla de cursor izquierda

Tabla 14. Teclas que transmiten los códigos de las teclas del teclado de edición (continuación)

Palabra clave	Modalidad	Carácter hexadecimal transmitido	Descripción del carácter de control
*CSRLEFT	Establecimiento de modalidad de tecla de cursor de VT100 o VT220 de 7 bits	X'1B4F44'	Tecla de cursor izquierda
*CSRLEFT	Establecimiento de modalidad de tecla de cursor de VT220 de 8 bits	X'8F44'	Tecla de cursor izquierda
*FINDKEY	Modalidad VT220 de 7 bits	X'1B5B317E'	Tecla Buscar del teclado de edición
*FINDKEY	Modalidad VT220 de 8 bits	X'9B317E ¹	Tecla Buscar del teclado de edición
*INSERTKEY	Modalidad VT220 de 7 bits	X'1B5B327E'	Tecla Insertar aquí del teclado de edición
*INSERTKEY	Modalidad VT220 de 8 bits	X'9B327E ¹	Tecla Insertar aquí del teclado de edición
*REMOVEKEY	Modalidad VT220 de 7 bits	X'1B5B337E'	Tecla Eliminar del teclado de edición
*REMOVEKEY	Modalidad VT220 de 8 bits	X'9B337E ¹	Tecla Eliminar del teclado de edición
*SELECTKEY	Modalidad VT220 de 7 bits	X'1B5B347E'	Tecla Seleccionar del teclado de edición
*SELECTKEY	Modalidad VT220 de 8 bits	X'9B347E ¹	Tecla Seleccionar del teclado de edición
*PREVSCN	Modalidad VT220 de 7 bits	X'1B5B357E'	Tecla Pantalla anterior del teclado de edición
*PREVSCN	Modalidad VT220 de 8 bits	X'9B357E ¹	Tecla Pantalla anterior del teclado de edición
*NEXTSCN	Modalidad VT220 de 7 bits	X'1B5B367E'	Tecla Pantalla siguiente del teclado de edición
*NEXTSCN	Modalidad VT220 de 8 bits	X'9B367E ¹	Tecla Pantalla siguiente del teclado de edición

Nota: esta secuencia es una versión abreviada de la secuencia de 7 bits. Sólo se presenta cuando opera en modalidad de 8 bits, a la que puede llamar el servidor o host VT220 remoto, o que puede especificar en el parámetro ASCOPRMOD del mandato Arrancar TCP/IP TELNET (STRTCPTELN).

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx” en la página 30
 El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

Valores de las teclas VTxxx por función 5250:

En esta tabla se describen los valores de las teclas VT VTxxx función 5250.

Tabla 15. Valores de las teclas VTxxx por función 5250

Función 5250 predeterminada	Valor especial	Teclas VTxxx	Valor hexadecimal ¹
Atención	*CTLA	<CTRL-A>	X'01'

Tabla 15. Valores de las teclas VTxxx por función 5250 (continuación)

Función 5250 predeterminada	Valor especial	Teclas VTxxx	Valor hexadecimal¹
Atención	*ESCA	<ESC><A>	X'1B41'
Retroceso	*BACKSPC	<Retroceso o Control-H>	X'08'
Borrar pantalla	*ESCC	<ESC><C>	X'1B43'
Cursor abajo	*CSRDOWN	<Flecha abajo>	X'1B5B42'
Cursor izquierda	*CSRLEFT	<Flecha a la izquierda>	X'1B5B44'
Cursor derecha	*CSRRIGHT	<Flecha a la derecha>	X'1B5B43'
Cursor arriba	*CSRUP	<Flecha arriba>	X'1B5B41'
Suprimir	*DLT	<Suprimir>	X'7F'
Suprimir	*RMV	<Eliminar>	X'1B5B337E' ²
Suprimir	*RMV	<Eliminar>	X'9B337E' ³
Duplicar	*ESCD	<ESC><D>	X'1B44'
Intro	*RETURN	<Retorno o CTRL-M>	X'0D'
Borrar entrada	*CTLE	<CTRL-E>	X'05'
Restaurar error	*CTLR	<CTRL-R>	X'12'
Restaurar error	*ESCR	<ESC><R>	X'1B52'
Avance de campo	*TAB	<Tabulador o Control-I>	X'09'
Retroceso de campo	*ESCTAB	<ESC><Tabulador o Control-I>	X'1B09'
Salida de campo	*CTLK	<Control-K>	X'0B'
Salida de campo	*CTLX	<Control-X>	X'18'
Salida de campo	*ESCX	<ESC><X>	X'1B58'
Campo menos	*ESCM	<ESC><M>	X'1B4D'
Ayuda	*CTLQST	<Control-Signo de interrogación>	X'1F'
Ayuda	*ESCH	<ESC><H>	X'1B48'
Inicio	*CTLO	<Control-O>	X'0F'
Insertar	*ESCI	<ESC><I>	X'1B49'
Insertar	*ESCDLT	<ESC><Suprimir>	X'1B7F'
Insertar	*INS	<Insertar aquí>	X'1B5B327E' ²
Insertar	*INS	<Insertar aquí>	X'9B327E' ³
Línea nueva	*ESCLF	<ESC> <Salto de línea o Control-J>	X'1B0A'
Avance Página (Giro Arriba)	*CTLD	<Control-D>	X'04'
Avance Página (Giro Arriba)	*CTLF	<Control-F>	X'06'
Avance Página (Giro Arriba)	*NXTSCR	<Pantalla siguiente>	X'1B5B367E' ²
Avance Página (Giro Arriba)	*NXTSCR	<Pantalla siguiente>	X'9B367E' ³
Giro Abajo (Retroceso Página)	*CTLB	<Control-B>	X'02'

Tabla 15. Valores de las teclas VTxxx por función 5250 (continuación)

Función 5250 predeterminada	Valor especial	Teclas VTxxx	Valor hexadecimal ¹
Giro Abajo (Retroceso Página)	*CTLU	<Control-U>	X'15'
Giro Abajo (Retroceso Página)	*PRVSCR	<Pantalla anterior>	X'1B5B357E ²
Giro Abajo (Retroceso Página)	*PRVSCR	<Pantalla anterior>	X'9B357E ³
Imprimir	*CTLP	<Control-P>	X'10'
Imprimir	*ESCP	ESC	X'1B50'
Redibujar pantalla	*CTLL	<Control-L>	X'0C'
Redibujar pantalla	*ESCL	<ESC><L>	X'1B4C'
Petición de sistema	*CTLC	<Control-C>	X'03'
Petición de sistema	*ESCS	<ESC><S>	X'1B53'
Petición de prueba	*CTLT	<Control-T>	X'14'
Conmutar indicadores luminosos	*ESCT	<ESC><T>	X'1B54'
F1	*ESC1	<ESC><1>	X'1B31'
F1	*F1	<F1> ⁵	X'1B5B31317E ²
F1	*F1	<F1> ⁵	X'9B31317E ³
F1	*PF1	<PF1>	X'1B4F50 ²
F1	*PF1	<PF1>	X'8F50 ³
F2	*ESC2	<ESC><2>	X'1B32'
F2	*F2	<F2> ⁵	X'1B5B31327E ²
F2	*F2	<F2> ⁵	X'9B31327E ³
F2	*PF2	<PF2>	X'1B4F51 ²
F2	*PF2	<PF2>	X'8F51 ³
F3	*ESC3	<ESC><3>	X'1B33'
F3	*F3	<F3> ⁵	X'1B5B31337E ²
F3	*F3	<F3> ⁵	X'9B31337E ³
F3	*PF3	<PF3>	X'1B4F52 ²
F3	*PF3	<PF3>	X'8F52 ³
F4	*ESC4	<ESC><4>	X'1B34'
F4	*F4	<F4> ⁵	X'1B5B31347E ²
F4	*F4	<F4> ⁵	X'9B31347E ³
F4	*PF4	<PF4>	X'1B4F53 ²
F4	*PF4	<PF4>	X'8F53 ³
F5	*ESC5	<ESC><5>	X'1B35'
F5	*F5	<F5> ⁵	X'1B5B31357E ²
F5	*F5	<F5> ⁵	X'9B31357E ³
F6	*ESC6	<ESC><6>	X'1B36'
F6	*F6	<F6>	X'1B5B31377E ²

Tabla 15. Valores de las teclas VTxxx por función 5250 (continuación)

Función 5250 predeterminada	Valor especial	Teclas VTxxx	Valor hexadecimal ¹
F6	*F6	<F6>	X'9B31377E ³
F7	*ESC7	<ESC><7>	X'1B37'
F7	*F7	<F7>	X'1B5B31387E ²
F7	*F7	<F7>	X'9B31387E ³
F8	*ESC8	<ESC><8>	X'1B38'
F8	*F8	<F8>	X'1B5B31397E ²
F8	*F8	<F8>	X'9B31397E ³
F9	*ESC9	<ESC><9>	X'1B39'
F9	*F9	<F9>	X'1B5B32307E ²
F9	*F9	<F9>	X'9B32307E ³
F10	*ESC0	<ESC><0>	X'1B30'
F10	*F10	<F10>	X'1B5B32317E ²
F10	*F10	<F10>	X'9B32317E ³
F11	*ESCMINUS	<ESC><Menos>	X'1B2D'
F11	*F11	<F11>	X'1B5B32337E ²
F11	*F11	<F11>	X'9B32337E ³
F12	*ESCEQ	<ESC><Igual>	X'1B3D'
F12	*F12	<F12>	X'1B5B32347E ²
F12	*F12	<F12>	X'9B32347E ³
F13	*ESCEXCL	<ESC><Exclamación>	X'1B21'
F13	*F13	<F13>	X'1B5B32357E ²
F13	*F13	<F13>	X'9B32357E ³
F14	*ESCAT	<ESC><Signo At>	X'1B40'
F14	*F14	<F14>	X'1B5B32367E ²
F14	*F14	<F14>	X'9B32367E ³
F15	*ESCPOUND	<ESC><Libra>	X'1B23'
F15	*F15	<F15>	X'1B5B32387E ²
F15	*F15	<F15>	X'9B32387E ³
F16	*ESCDOLLAR	<ESC><Dólar>	X'1B24'
F16	*F16	<F16>	X'1B5B32397E ²
F16	*F16	<F16>	X'9B32397E ³
F17	*ESCPCT	<ESC><Porcentaje>	X'1B25'
F17	*F17	<F17>	X'1B5B33317E ²
F17	*F17	<F17>	X'9B33317E ³
F18	*ESCCFX	<ESC><Acento circumflejo>	X'1B5E ¹
F18	*F18	<F18>	X'1B5B33327E ²
F18	*F18	<F18>	X'9B33327E ³
F19	*ESCAMP	<ESC><Ampersand>	X'1B26'
F19	*F19	<F19>	X'1B5B33337E ²

Tabla 15. Valores de las teclas VTxxx por función 5250 (continuación)

Función 5250 predeterminada	Valor especial	Teclas VTxxx	Valor hexadecimal¹
F19	*F19	<F19>	X'9B33337E' ³
F20	*ESCAST	<ESC><Asterisco>	X'1B2A'
F20	*F20	<F20>	X'1B5B33347E' ²
F20	*F20	<F20>	X'9B33347E' ³
F21	*ESCLPAR	<ESC><Abrir paréntesis>	X'1B50'
F22	*ESCRPAR	<ESC><Cerrar paréntesis>	X'1B51'
F23	*ESCUS	<ESC><Subrayado>	X'1B5F'
F24	*ESCPLUS	<ESC><Más>	X'1B2B'
Véase nota 4	*FIND	<Buscar>	X'1B5B317E'
Véase nota 4	*FIND	<Buscar>	X'9B317E'
Véase nota 4	*SELECT	<Seleccionar>	X'1B5B347E'
Véase nota 4	*SELECT	<Seleccionar>	X'9B347E'

Notas:

¹ - Salvo que se identifique de otro modo, el valor hexadecimal está en la modalidad VT100.

² - Modalidad de control VT220 de 7 bits.

³ - No hay ninguna tecla de función 5250 que se correlacione con esta tecla VT.

⁴ - Las teclas de F1 a F5 no están disponibles en un terminal VT220. No obstante, muchos emuladores VT220 envían estos valores hexadecimales cuando se pulsan las teclas de F1 a F5.

Conceptos relacionados

“Configuración del servidor Telnet para la modalidad de pantalla completa VTxxx” en la página 30
 El soporte de servidor VTxxx permite a los usuarios de clientes Telnet iniciar la sesión y ejecutar aplicaciones 5250 de pantalla completa, aunque el soporte de pantalla completa VTxxx se negocie.

Modalidades operativas de la estación de trabajo VT220:

Se admiten distintas modalidades operativas mientras el sistema negocia el tipo de estación de trabajo VT220.

Estas modalidades operativas son las siguientes:

- La modalidad VT200 con controles de 7 bits es la modalidad predeterminada y utiliza las funciones ANSI estándar. Esta modalidad proporciona el rango completo de prestaciones de VT220 en un entorno de comunicaciones de 8 bits con controles de 7 bits. Esta modalidad soporta el juego de caracteres multinacional DEC o juegos de caracteres de sustitución nacionales (NRC), según la modalidad de juego de caracteres seleccionada.
- La modalidad VT200 con controles de 8 bits utiliza las funciones ANSI estándar y proporciona el rango completo de prestaciones de VT220 en un entorno de comunicaciones de 8 bits con controles de 8 bits. Esta modalidad soporta el juego de caracteres multinacional DEC o juegos NRC, según la modalidad de juego de caracteres seleccionada.
- La modalidad VT100 utiliza las funciones ANSI estándar. Esta modalidad restringe el uso del teclado a las teclas VT100. Todos los datos tienen una restricción de 7 bits, y únicamente se generan caracteres ASCII, NRC o caracteres de gráficos especiales.

- La modalidad VT52 utiliza las funciones privadas de DEC (no ANSI). Esta modalidad restringe el uso del teclado a las teclas VT52.

Si se negocia la modalidad VT220, se selecciona una modalidad operativa inicial para el cliente Telnet mediante el parámetro de modalidad operativa ASCII (ASCOPRMOD) del mandato Arrancar TCP/IP Telnet (STRTCPTLN) o del mandato TELNET.

Teclas de función de la fila superior de VT220:

En la tabla se describen las teclas que transmiten los códigos de las teclas de función de la fila superior del teclado VT220 en modalidad de 7 bits.

Tabla 16. Teclas de función de la fila superior de VT220

Palabra clave	Carácter hexadecimal transmitido
*F6	X'1B5B31377E'
*F7	X'1B5B31387E'
*F8	X'1B5B31397E'
*F9	X'1B5B32307E'
*F10	X'1B5B32317E'
*F11	X'1B5B32337E'
*F12	X'1B5B32347E'
*F13	X'1B5B32357E'
*F14	X'1B5B32367E'
*F15 o *HELP	X'1B5B32387E'
*F16 o *DO	X'1B5B32397E'
*F17	X'1B5B33317E'
*F18	X'1B5B33327E'
*F19	X'1B5B33337E'
*F20	X'1B5B33347E'

En esta tabla se describen las teclas que transmiten los códigos de las teclas de función de la fila superior del teclado VT220 en modalidad de 8 bits.

Tabla 17. Teclas de función de la fila superior de VT220 en modalidad de 8 bits

Palabra clave	Carácter hexadecimal transmitido
*F6	X'9B31377E'
*F7	X'9B31387E'
*F8	X'9B31397E'
*F9	X'9B32307E'
*F10	X'9B32317E'
*F11	X'9B32337E'
*F12	X'9B32347E'
*F13	X'9B32357E'
*F14	X'9B32367E'
*F15 o *HELP	X'9B32387E'
*F16 o *DO	X'9B32397E'

Tabla 17. Teclas de función de la fila superior de VT220 en modalidad de 8 bits (continuación)

Palabra clave	Carácter hexadecimal transmitido
*F17	X'9B33317E'
*F18	X'9B33327E'
*F19	X'9B33337E'
*F20	X'9B33347E'

Palabras clave de caracteres de control de VT100 y VT220:

En esta tabla se muestran las palabras clave de caracteres de control de VT100 y VT220

Tabla 18. Palabras clave de caracteres de control de VT100 y VT220

Descripción del carácter de control	Tecla+CTRL	Palabra clave	Carácter hexadecimal transmitido
Nulo	Barra espaciadora	*NUL	X'00'
Inicio de cabecera	A	*SOH,*CTLA	X'01'
Inicio de texto	B	*STX,*CTLB	X'02'
Fin de texto	C	*ETX,*CTLC	X'03'
Fin de transmisión	D	*EOT,*CTLD	X'04'
Petición	E	*ENQ,*CTLE	X'05'
Acuse de recibo	F	*ACK,*CTLF	X'06'
Campana	G	*BEL,*CTLG	X'07'
Retroceso	H	*BS,*CTLH	X'08'
Tabulación horizontal	I	*HT,*CTLI	X'09'
Salto de línea	J	*LF,*CTLJ	X'0A'
Tabulación vertical	K	*VT,*CTLK	X'0B'
Salto de página	L	*FF,*CTLL	X'0C'
Retorno de carro	M	*CR,*CTLM	X'0D'
Desplazamiento a teclado ideográfico	N	*SO,*CTLN	X'0E'
Desplazamiento a teclado estándar	O	*SI,*CTLO	X'0F'
Escape de enlace de datos	P	*DLE,*CTLP	X'10'
Control de dispositivo 1	Q	*DC1,*CTLQ	X'11'
Control de dispositivo 2	R	*DC2,*CTLR	X'12'
Control de dispositivo 3	S	*DC3,*CTLS	X'13'
Control de dispositivo 4	T	*DC4,*CTLT	X'14'
Acuse de recibo negativo	U	*NAK,*CTLU	X'15'
Desocupado síncrono	V	*SYN,*CTLV	X'16'
Fin de bloque de transmisión	W	*ETB,*CTLW	X'17'
Cancelar palabra o carácter anterior	X	*CAN,*CTLX	X'18'
Fin de medio	Y	*EM,*CTLY	X'19'
Sustitución	Z	*SUB,*CTLZ	X'1A'

Tabla 18. Palabras clave de caracteres de control de VT100 y VT220 (continuación)

Descripción del carácter de control	Tecla+CTRL	Palabra clave	Carácter hexadecimal transmitido
Escape	[*ESC	X'1B'
Separador de archivo	\	*FS	X'1C'
Separador de grupo]	*GS	X'1D'
Separador de registro	&eqv.	*RS	X'1E'
Separador de unidad	?	*US	X'1F'
Suprimir		*DEL	X'7F'

Establecimiento de una sesión Telnet en cascada

Puede establecer otra sesión Telnet mientras está en una sesión Telnet actual. Una vez establecida una sesión en cascada, puede moverse entre los distintos sistemas.

El sistema inicial es el primer sistema cliente que se utiliza. El sistema final es el último sistema servidor Telnet al que se accede. El sistema por el que se pasa a través para ir del sistema inicial al sistema final se denomina sistema intermedio.

Inicio de una sesión en cascada

Para iniciar una sesión en cascada, inicie la sesión en el sistema inicial y, a continuación, siga los pasos correspondientes para establecer una sesión de cliente. Repita los pasos para cada sistema al que desee conectarse.

Volver al sistema

El mandato SIGNOFF finaliza la sesión y devuelve al usuario a la pantalla de inicio de sesión del sistema. Cuando ha iniciado una sesión en el sistema, el mandato SIGNOFF finaliza el trabajo de servidor actual y devuelve al usuario a la pantalla de inicio de sesión del sistema.

Puede utilizar el parámetro de finalización de conexión (ENDCNN) del mandato SIGNOFF para finalizar la sesión del sistema y finalizar la conexión TELNET. Por ejemplo, `signoff endcnn(*yes)` devuelve al usuario a la sesión original del sistema cliente, o a la sesión anterior si tiene establecida más de una sesión TELNET.

Notas:

1. No hay ningún límite en el número de sistemas con los que se puede establecer una sesión Telnet.
2. El sistema inicial intercepta las opciones 13 y 14 de Petición Sistema si se especifican en la línea de entrada de Petición Sistema. Esta función puede serle de utilidad si establece una sesión Telnet con un sistema en el que no puede iniciar la sesión. En este caso, puede finalizar una sesión con ese sistema realizando los pasos siguientes:
 - Pulse la tecla Petición de sistema.
 - Teclee 13 (Iniciar petición del sistema en sistema inicial) en la línea de entrada de Petición Sistema.
 - Teclee 2 (Finalizar petición anterior) en el menú Petición Sistema.

Conceptos relacionados

“Caso práctico de Telnet: sesiones Telnet en cascada” en la página 4

El caso práctico muestra la posibilidad de iniciar sesiones Telnet mientras todavía se está en una sesión Telnet. Una vez conectado, puede pasar de un sistema a otro utilizando los valores de petición del sistema.

“Inicio de una sesión de cliente Telnet” en la página 54

Debe conocer el nombre o la dirección Internet del sistema remoto en el que desea iniciar la sesión Telnet.

Paso de una sesión Telnet en cascada a otra

Una vez que haya iniciado una sesión Telnet en cascada, pulse la tecla Pet Sis y pulse Intro para visualizar el menú Petición Sistema.

El menú Petición Sistema proporciona las siguientes opciones.

Opción de Petición de Sistema	Acción	Descripción
10	Iniciar una petición de sistema en un sistema cliente	Visualiza el menú Petición Sistema en el sistema cliente anterior.
11	Transferir a sistema cliente	Transfiere a un trabajo alternativo del sistema cliente anterior.
13	Iniciar petición de sistema en sistema inicial	Lleva de un sistema intermedio o final al menú Petición Sistema del sistema inicial.
14	Transferir a sistema inicial	Lleva de un sistema intermedio o final al trabajo alternativo del sistema inicial.
15	Transferir a sistema final	Lleva de un sistema intermedio o inicial al sistema final

Para eludir el menú Petición Sistema, pulse la tecla Pet Sis y escriba 10 en la línea de mandatos. Este acceso directo solo es válido entre plataformas System i.

Para clientes Telnet no IBM

Podría desconectar una sesión Telnet en cascada cuando intente utilizar las opciones 10, 11, 13 o 14 del menú Petición Sistema. Para las opciones 10 y 11, el PC cliente es el sistema anterior. Para las opciones 13 y 14, el PC cliente es el sistema inicial.

El cliente Telnet es compatible si pasa estas dos pruebas:

- Tras usar las opciones 13 o 14 regresa al sistema inicial.
- No se desconecta una sesión al utilizar las opciones 10 u 11 desde el sistema inicial.

En el caso de clientes no compatibles, siga estos pasos en lugar de utilizar las opciones 10, 11, 13 o 14 de Petición Sistema:

1. Utilice la opción 11 de Petición Sistema para retroceder de un sistema a otro hasta alcanzar el sistema inicial. El sistema inicial es el primer sistema al que se conectó el cliente Telnet al principio de la sesión.
2. En el sistema inicial, utilice la opción 1 de Petición Sistema para avanzar de un sistema a otro.

Conceptos relacionados

“Caso práctico de Telnet: sesiones Telnet en cascada” en la página 4

El caso práctico muestra la posibilidad de iniciar sesiones Telnet mientras todavía se está en una sesión Telnet. Una vez conectado, puede pasar de un sistema a otro utilizando los valores de petición del sistema.

Finalización de una sesión de cliente Telnet

Cuando está conectado a una plataforma System i, al finalizar la sesión no necesariamente se finaliza la sesión del servidor Telnet. Para finalizar la sesión del servidor, debe especificar una tecla o secuencia de teclas para colocar el cliente Telnet en la modalidad de mandatos local. A continuación, puede especificar el mandato para finalizar la sesión.

- En el sistema operativo i5/OS, pulse la tecla Atención y, a continuación, seleccione la opción 99 (Finalizar sesión Telnet - QUIT).
- En la mayor parte de los demás sistemas, finalice la sesión.

Si no sabe qué tecla o secuencia de teclas hace que el cliente entre en la modalidad de mandatos, consulte con el administrador del sistema o repase la documentación del cliente Telnet.

También puede utilizar el parámetro de finalización de conexión (ENDCNN) del mandato SIGNOFF para finalizar la sesión del sistema y finalizar la conexión Telnet. Por ejemplo, SIGNOFF ENDCNN(*YES) le devuelve al sistema cliente (si solo ha establecido una sesión Telnet). Si ha establecido más de una sesión Telnet, el mandato le devuelve al sistema anterior.

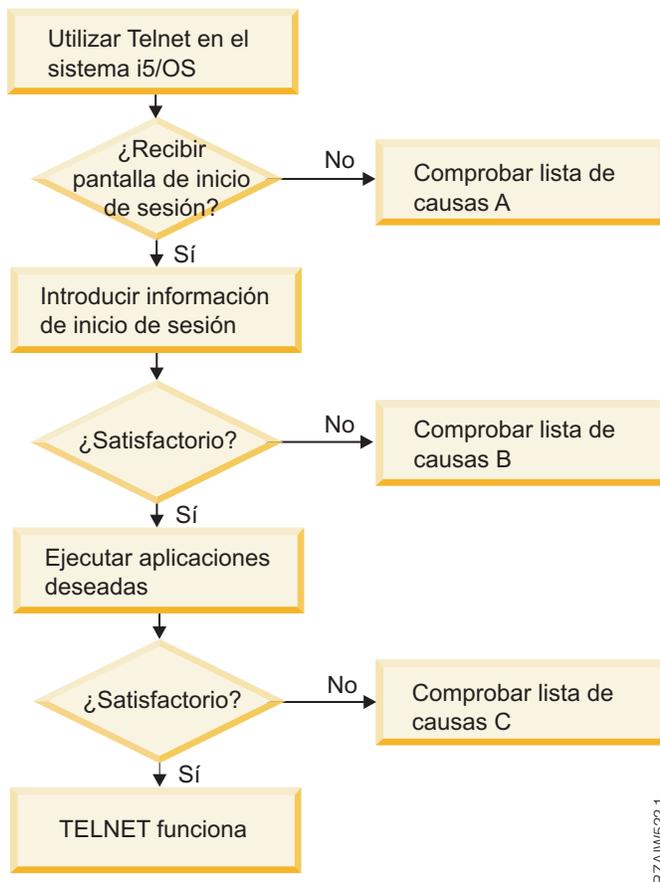
Resolución de problemas de Telnet

Este tema contiene información sobre cómo resolver y corregir los problemas relacionados con Telnet.

Determinación de problemas con Telnet

Necesita información de diagnóstico para solucionar los problemas de Telnet, que incluye un diagrama de flujo para el análisis de los problemas del sistema, y necesita una lista del material necesario para informar de problemas de Telnet.

Utilice este diagrama de flujo después de utilizar el diagrama de flujo de problemas generales de TCP/IP. Si se detecta un problema al utilizar el servidor Telnet, utilice el diagrama de flujo para identificar la causa del mismo. Las listas de causas que se muestran después del diagrama de flujo permiten identificar los posibles problemas.



Lista de causas A

1. Verifique que los trabajos del servidor Telnet están activos y que el servicio Telnet está asignado a un puerto sin restringir válido.
 - a. Para verificar que los trabajos QTVTELNET y QTVDEVICE están activos en el subsistema QSYSWRK, siga estos pasos:
 - 1) Inicie System i Navigator y expanda *su sistema* → **Gestión de trabajo**.
 - 2) Pulse **Trabajos activos** con el botón derecho del ratón y fíjese en QTVTELNET y QTVDEVICE para ver si están activos. Si lo están, continúe en el paso 1c.
 - b. Si estos trabajos no están activos, siga estos pasos para iniciar estos trabajos:
 - 1) Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - 2) Pulse **Telnet** con el botón derecho del ratón y seleccione **Iniciar**.
 - c. Para verificar que el servicio Telnet está asignado a un puerto válido, siga estos pasos:
 - 1) Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - 2) Pulse **Conexiones** con el botón derecho del ratón y seleccione **Abrir**.
 - 3) Busque Telnet.
 - d. En el caso de impresoras, asegúrese de que el subsistema QSPL está activo.
 - e. Consulte las restricciones de puerto yendo al menú CFGTCP y seleccionando la opción 4 (Trabajar con restricciones de puerto TCP/IP).
2. Verifique que el valor del sistema de dispositivos del sistema está establecido correctamente para permitir al servidor Telnet crear dispositivos virtuales automáticamente.
3. Verifique que la conexión de red entre el sistema y el cliente Telnet está activa utilizando la función Ping en System i Navigator. Si la conexión no está activa, consulte con el administrador de la red.

4. Verifique que los dispositivos virtuales del sistema que Telnet utiliza están definidos en un subsistema bajo el que deben ejecutarse los trabajos de Telnet interactivos.
 - a. Para ver las entradas de estación de trabajo que están definidas en un subsistema, siga estos pasos:
 - 1) Inicie System i Navigator y expanda *su sistema* → **Gestión de trabajo**.
 - 2) Pulse **Subsistemas** con el botón derecho del ratón y seleccione **Abrir**.
 - b. Utilice el mandato Añadir entrada de estación de trabajo (ADDWSE) para definir estaciones de trabajo a un subsistema. Por ejemplo, puede utilizar el mandato siguiente para permitir que todos los tipos de estación de trabajo se ejecuten bajo el subsistema QINTER:


```
ADDWSE SBS(QINTER) WRKSTNTYPE(*ALL)
```
5. Verifique que el subsistema interactivo (QINTER) está activo. Las conexiones Telnet no están completas si el subsistema interactivo no está activo. En estas circunstancias, el sistema no escribe mensajes de error en las anotaciones de trabajo QTVTELNET ni en las anotaciones de trabajo QTVDEVICE para mostrar el problema al usuario.

Para verificar que el subsistema está activo, siga estos pasos:

 - a. Inicie System i Navigator y expanda *su sistema* → **Gestión de trabajo**.
 - b. Pulse **Subsistemas** con el botón derecho del ratón y seleccione **Abrir**.
 - c. Verifique que el subsistema está activo.
6. Si opera en modalidad de pantalla completa VTxxx, verifique que la configuración de cliente VTxxx local específica la acomodación automática. Si la acomodación automática está activa, el sistema acomodará automáticamente las líneas en la columna 80.
7. Compruebe si hay un programa de salida de Telnet registrado en el punto de salida QIBM_QTG_DEVINIT, con el formato INIT0100, mediante el mandato para trabajar con información de registro (WRKREGINF). Si hay un programa de salida de usuario registrado, consulte las anotaciones de trabajo del servidor Telnet con el nombre de trabajo QTVDEVICE para ver si hay algún error relacionado con ese programa. Si existe algún error, corrija los errores del programa de salida o elimine el programa de salida con el mandato para eliminar programa de salida (RMVEXITPGM).
8. Asegúrese de que el cliente intenta utilizar el puerto correcto para conectarse a Telnet.

Para determinar el puerto al que está asignado el servicio Telnet, siga estos pasos:

 - a. Inicie System i Navigator y expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
 - b. Pulse **Conexiones** con el botón derecho del ratón y seleccione **Abrir**.
 - c. Busque Telnet.
9. Utilice el mandato CFGTCP para verificar que el puerto en el que el cliente intenta conectarse no está restringido. Asimismo, busque en las anotaciones de trabajo QTVTELNET si hay algún mensaje que indica que el puerto que intenta utilizar está restringido.
10. Al intentar conectarse mediante Telnet SSL, compruebe que tiene instalado el Gestor de Certificados Digitales (DCM). Este es un elemento adicional de los indicados anteriormente. Compruebe también que el servidor Telnet tiene asignado un certificado sin caducar válido (QIBM_QTV_TELNET_SERVER).

Lista de causas B

1. Verifique su autorización sobre el dispositivo virtual de pantalla. Si recibe el mensaje CPF1110 al intentar iniciar la sesión en la plataforma System i, no tiene autorización para el dispositivo virtual de pantalla. Cuando el servidor Telnet crea dispositivos virtuales, el valor del sistema QCRTAUT permite determinar la autorización concedida al usuario *PUBLIC. Este valor del sistema debe ser *CHANGE para permitir a cualquier usuario iniciar la sesión con Telnet.
2. Si es usted el responsable de seguridad o posee la autorización *SECOFR, verifique que el valor del sistema QLMTSECOFR es correcto.

Lista de causas C

1. Verifique la opción de procesador de textos que ha elegido. Si tiene problemas al utilizar el mandato Trabajar con carpetas (WRKFLR), puede que tenga que cambiar la configuración para que se emplee el editor adaptado a la oficina en lugar del editor estándar. Para ello, pida al administrador del sistema que cambie la opción de procesador de textos en la información de entorno asociada al ID de usuario de oficina.
2. Si opera en modalidad de pantalla completa VTxxx, verifique que la configuración de cliente VTxxx local especifica la acomodación automática. Si la acomodación automática está activa, el sistema acomodará automáticamente las líneas en la columna 80.
3. Si los caracteres no se visualizan correctamente en la sesión VTxxx, verifique que se utilizan las tablas de correlación correctas para la sesión.
4. Si el cliente VTxxx emite un pitido cada vez que se pulsa una tecla, el teclado podría estar bloqueado.
5. Consulte las anotaciones de trabajo QTVTELNET y QTVDEVICE para ver si hay mensajes de error en el sistema.

Conceptos relacionados

Valores del sistema: visión general de dispositivos

“Consideraciones sobre la modalidad de pantalla completa VTxxx” en la página 63

Al igual que sucede con cualquier tipo de emulación, debe tener en cuenta determinadas consideraciones antes de utilizar la modalidad de pantalla completa VTxxx con el servidor Telnet. Entre estas consideraciones se encuentran algunas cuestiones de seguridad, así como condiciones de error posibles e indicadores luminosos. Si se familiariza con estas consideraciones, aprenderá a utilizar de forma eficaz la modalidad de pantalla completa VTxxx.

Descripción: diagrama de flujo para el análisis de los problemas de Telnet

Siga estos pasos para determinar qué lista de causas debe emplearse:

1. Establezca una conexión Telnet con el sistema operativo i5/OS.
2. ¿Ha aparecido una pantalla de inicio de sesión? En caso afirmativo, continúe. En caso negativo, consulte Lista de causas A.
3. Especifique la información de inicio de sesión.
4. ¿El inicio de sesión se ha completado satisfactoriamente? En caso afirmativo, continúe. En caso negativo, consulte Lista de causas B.
5. Ejecute las aplicaciones necesarias.
6. ¿Las aplicaciones se han ejecutado satisfactoriamente? En caso afirmativo, continúe. En caso negativo, consulte Lista de causas C.
7. Telnet funciona.

Emisión de un mandato Ping al servidor de hospedaje

Puede utilizar la función Ping en System i Navigator para probar la conexión TCP/IP.

Para emitir un mandato Ping al sistema, siga estos pasos:

1. Inicie System i Navigator y expanda *su sistema* → **Red**.
2. Pulse **Configuración de TCP/IP** con el botón derecho del ratón y seleccione **Utilidades**.
3. Pulse **Ping** para visualizar el diálogo **Ping**.
4. Escriba el nombre de host en el recuadro **Ping** (por ejemplo, companyname.com).
5. Pulse **Ping ahora**.

Los mensajes se visualizan en el recuadro **Resultados** para indicarle el estado de la conexión.

Tareas relacionadas

“Comprobación del estado del sistema” en la página 98

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

Resolución de problemas relacionados con los tipos de emulación

Al desarrollar un cliente Telnet, es importante que negocie el tipo de estación de trabajo de emulación correcto. Las funciones permitidas varían según el tipo de estación de trabajo. La siguiente guía permite conocer el tipo de estación de trabajo y las funciones de esa estación de trabajo.

Negociaciones de tipo de estación de trabajo y correlaciones

La tabla de correlaciones de estación de trabajo e impresora muestra una lista de estaciones de pantalla virtuales que el servidor utiliza para hacer coincidir con las estaciones de pantalla físicas del sistema cliente.

Si no está seguro de qué paquete de emulación está ejecutando, debe determinar cuál es su dispositivo de pantalla virtual. Puede utilizar el mandato Trabajar con trabajo (WRKJOB) para averiguar cuál es. El nombre de trabajo se visualiza en la parte superior. Este es el nombre del dispositivo de pantalla virtual asociado al trabajo. De forma predeterminada, el convenio de denominación es QPADEVxxxx, donde xxxx son caracteres alfanuméricos.

Para determinar el tipo de dispositivo, escriba:

```
WRKCFGSTS *DEV QPADEVxxxx
```

Puede trabajar con la descripción del dispositivo. Escriba un 8 (Trabajar con descripción) junto al nombre del dispositivo. El sistema visualiza el tipo de dispositivo. A continuación, a partir del tipo de dispositivo puede determinar si opera en modalidad de pantalla completa para 3270, 5250, VT100 o VT220.

Tabla 19. Correlaciones de estación de trabajo e impresora

Estación de trabajo soportada (y modelo)	Tipo equivalente (y modelo)	Especificación de Internet	Descripción
5251 (11)		IBM-5251-11	Pantalla monocromática 24 x 80
5291 (1)	5291 (2)	IBM-5291-1	Pantalla monocromática 24 x 80
5292 (2)		IBM-5292-2	Pantalla de gráficos de color 24 x 80; este tipo de estación de trabajo también se emula mediante una función de estación de trabajo de gráficos.
3196 (A1)	3196 (A1) 3196(B1) 3196 (B2) 3476 (EA)	IBM-3196-A1	Pantalla monocromática 24 x 80; este tipo de estación de trabajo también se emula mediante una función de estación de trabajo monocromática.
3486 (BA)		IBM-3486-BA	Pantalla monocromática 24 x 80
3487(HA) ²	3487 (HG) ² 3487 (HW) ²	IBM-3487-HA	Pantalla monocromática 24 x 80; este tipo de estación de trabajo también se emula mediante una función de estación de trabajo monocromática.

Tabla 19. Correlaciones de estación de trabajo e impresora (continuación)

Estación de trabajo soportada (y modelo)	Tipo equivalente (y modelo)	Especificación de Internet	Descripción
3487 (HC) ²		IBM-3487-HC	Pantalla de color 24 x 80; este tipo de estación de trabajo también se emula mediante una función de estación de trabajo de color.
3179 (2)	3197 (C1) 3197 (C2) 3476 (EC)5292 (1)	IBM-3179-2	Pantalla de color 24 x 80; este tipo de estación de trabajo también se emula mediante una función de estación de trabajo de color.
3180 (2)	3197 (D1) 3197 (D2) 3197 (W1) 3197 (W2)	IBM-3180-2	Pantalla monocromática 27 x 132
5555 (B01)	5555 (E01)	IBM-5555-B01	Pantalla monocromática DBCS (juego de caracteres de doble byte) 24 x 80; este tipo de estación de trabajo se emula mediante una función de estación de trabajo con soporte para la pantalla DBCS.
5555 (C01)	5555 (F01)	IBM-5555-C01	Pantalla de color DBCS 24 x 80; este tipo de estación de trabajo se emula mediante una función de estación de trabajo con soporte para la pantalla DBCS.
5555 (G01)		IBM-5555-G01	Pantalla de gráficos monocromática DBCS (juego de caracteres de doble byte) 24 x 80; este tipo de estación de trabajo se emula mediante una función de estación de trabajo con soporte para la pantalla DBCS.
5555 (G02)		IBM-5555-G02	Pantalla de gráficos de color DBCS 24 x 80; este tipo de estación de trabajo se emula mediante una función de estación de trabajo con soporte para la pantalla DBCS.
3477 (FC)		IBM-3477-FC	Pantalla panorámica de color 27 x 132
3477 (FG)	3477 (FA) 3477 (FD) 3477 (FW)3477 (FE)	IBM-3477-FG	Pantalla panorámica monocromática 27 x 132
3277 (0) ³	3277 (DHCF)	IBM-3277-2	Pantalla monocromática 24 x 80
3277 (0) ^{3,4}	3278 (DHCF)	IBM-3278-2	Pantalla monocromática 24 x 80

Tabla 19. Correlaciones de estación de trabajo e impresora (continuación)

Estación de trabajo soportada (y modelo)	Tipo equivalente (y modelo)	Especificación de Internet	Descripción
3278 (0) ³		IBM-3278-2-E ⁵	Pantalla monocromática 24 x 80
3278 (0) ³		IBM-3278-3	Pantalla monocromática 24 x 80
3278 (0) ³		IBM-3278-4	Pantalla monocromática 24 x 80
3278 (0) ³		IBM-3278-5	Pantalla monocromática 24 x 80
3279 (0) ³	3279 (DHCF)	IBM-3279-2 IBM-3279-2-E ⁵	Pantalla monocromática 24 x 80
3279 (0) ³		IBM-3279-3	Pantalla de color 24 x 80
3812 (1)		IBM-3812-1	Impresora 3812 (SBCS)
5553 (B01)		IBM-5553-B01	Impresora 5553 (DBCS)
VT100 (*ASCII) ⁶		DEC-VT100 VT100(7) VT102 DEC-VT102 DEC-VT200 DEC-VT220 VT200(7) VT220(7)	Pantalla ASCII monocromática 24 x 80

Consideraciones:

¹ Todas las estaciones de trabajo 5250, excepto 5555 (B01) y 5555 (C01), pueden operar como estaciones de trabajo 5251-11.

² Esta estación de trabajo puede configurarse en 24 x 80 o 27 x 132. Debe determinar la modalidad de la estación de trabajo antes de establecer el valor del parámetro de tipo de estación de trabajo.

³ El sistema soporta únicamente las pantallas 24 x 80 en estaciones de trabajo 327x remotas. Las estaciones de trabajo 3277 (tanto las DHCF, Distributed Host Command Facility, como las normales) remotas se correlacionan con IBM-3277-2. Las estaciones de trabajo 3278 remotas se correlacionan con IBM-3278-2. Las estaciones de trabajo 3279 remotas se correlacionan con IBM-3279-2.

⁴ Algunos paquetes de emulador Telnet 3270 de pantalla completa (TN3270) o 3278-2 no soportan los campos estructurados de escritura correctamente. Por ello, la implementación del servidor Telnet correlaciona los dispositivos de tipo 3278-2 con los dispositivos 3277-2 para permitir que el sistema trabaje con estas implementaciones TN3270.

⁵ El atributo ampliado de resaltado está soportado. Se incluye el subrayado, el parpadeo y el contraste invertido. El proceso DBCS de 3270 también está soportado.

⁶ El dispositivo virtual VT100 soporta dispositivos VT220.

⁷ VT100, VT200 y VT220 no son nombres de tipo de terminal oficiales. Sin embargo, algunas implementaciones negocian empleando estos nombres como valor del tipo de terminal.

Referencia relacionada

“INIT0100: Formato de la información de descripción de la conexión” en la página 49

Este tema contiene información sobre la conexión del cliente que puede utilizar el programa de salida.

Resolución de problemas del servidor Telnet SSL

Aquí se describen los pasos detallados para la resolución de problemas del servidor de Capa de sockets seguros (SSL), con los códigos de retorno del sistema SSL y una lista de los problemas de SSL más habituales.

Para identificar los problemas que surjan en el servidor Telnet SSL, siga estos pasos:

1. Compruebe el estado del sistema para verificar que se ha instalado el software correcto y que los servidores se han iniciado.
2. Emita un mandato Ping al servidor de hospedaje para comprobar que se ha iniciado TCP/IP y que la red funciona correctamente.
3. Compruebe que se ha iniciado el servidor Telnet.
4. Compruebe si existe un escucha SSL activo, utilizando el mandato NETSTAT *CNN.
5. Compruebe las anotaciones de trabajo de Telnet para encontrar el código de retorno de SSL.
6. Consulte los códigos de retorno y problemas de SSL para obtener sugerencias para la resolución del problema.

Los certificados digitales incorrectos pueden ocasionar muchos problemas con SSL. El gestor de certificados digitales (DCM) le permite cambiar la autoridad certificadora o los certificados del sistema. Para confirmar que posee un certificado válido del sistema, consulte cómo iniciar el gestor de certificados digitales (DCM) y ver el certificado del sistema.

Conceptos relacionados

“Protección de Telnet con SSL” en la página 33

Con el protocolo SSL (capa de sockets seguros), puede establecer conexiones seguras entre la aplicación de servidor Telnet y los clientes Telnet que proporcionan la autenticación de uno o varios puntos finales de la sesión de comunicación. SSL también garantiza la privacidad e integridad de los datos que intercambian las aplicaciones del cliente y el servidor.

Conceptos de DCM

Inicio de Digital Certificate Manager

Tareas relacionadas

“Configuración de SSL en el servidor Telnet” en la página 33

El factor más importante que debe tenerse en cuenta al habilitar SSL en el servidor Telnet es la confidencialidad de la información que se utiliza en las sesiones de cliente. Si la información es confidencial, o privada, se recomienda proteger el servidor Telnet con SSL.

Comprobación del estado del sistema

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

1. Verifique que tiene instalado el software adecuado para soportar Telnet SSL y para gestionar certificados:
 - IBM TCP/IP Connectivity Utilities para i5/OS (5761-TC1)
 - Digital Certificate Manager
 - IBM HTTP Server para i5/OS (5761-DG1)
 - IBM Developer Kit para Java (5761-JV1)
2. Verifique que tiene un servidor Telnet seguro, asociando un certificado a la aplicación del servidor Telnet QIBM_QTV_TELNET_SERVER.
3. Emita un mandato Ping al sistema de hospedaje para verificar la conexión TCP/IP y el estado de la red.
4. Determine si se ha iniciado el servidor Telnet.
5. Determine si el servidor Telnet está configurado para permitir las conexiones SSL.

Tareas relacionadas

“Asignación de un certificado al servidor Telnet” en la página 34
Cuando habilite el uso de la Capa de sockets seguros (SSL) para el servidor Telnet en el sistema, puede establecer conexiones Telnet seguras con el sistema desde System i Access para Windows o desde cualquier otro cliente Telnet habilitado para SSL, como por ejemplo un emulador de Personal Communications.

“Emisión de un mandato Ping al servidor de hospedaje” en la página 94
Puede utilizar la función Ping en System i Navigator para probar la conexión TCP/IP.

“Inicio del servidor Telnet” en la página 21

El servidor Telnet activo tiene una o más instancias de cada uno de los siguientes trabajos en ejecución en el subsistema QSYSWRK: QTVTELNET y QTVDEVICE.

“Configuración de SSL en el servidor Telnet” en la página 33

El factor más importante que debe tenerse en cuenta al habilitar SSL en el servidor Telnet es la confidencialidad de la información que se utiliza en las sesiones de cliente. Si la información es confidencial, o privada, se recomienda proteger el servidor Telnet con SSL.

Referencia relacionada

“Códigos de retorno de SSL” en la página 100

En este tema se muestran los códigos de retorno de la capa de sockets seguros (SSL) del sistema de los problemas más habituales que pueden producirse durante la inicialización o negociación de SSL.

Comprobación de la existencia de un escucha SSL activo

Utilice este procedimiento para comprobar la existencia de un escucha de capa de sockets seguros (SSL) activo. El servidor Telnet debe estar activo y preparado para recibir intentos de conexión.

Para comprobar si existe un escucha SSL activo, siga estos pasos:

1. En la interfaz basada en caracteres, escriba NETSTAT *CNN para mostrar la pantalla Trabajar con estado de conexión TCP/IP.
2. En la columna **Puerto Local**, busque la etiqueta telnet- correspondiente a telnet-ssl. Solamente puede ver telnet- porque el campo de la pantalla no es lo suficientemente largo como para mostrarlo entero.
 - Utilice la tecla F22 para visualizar el campo Puerto Local entero.
 - Utilice la tecla F14 para ver los números de puerto. La entrada telnet-ssl tiene el puerto 992.

La inicialización de SSL sufre una anomalía si no encuentra telnet-ssl en la columna Puerto Local. Para arreglar el problema, compruebe los mensajes de diagnóstico de SSL en las anotaciones del trabajo QTVTELNET que se ejecuta en el subsistema QSYSWRK. Tras una inicialización anómala de SSL solo se estará ejecutando un trabajo QTVTELNET.

Tareas relacionadas

“Comprobación de las anotaciones de trabajo de Telnet”

Cuando la inicialización y negociación de la capa de sockets seguros (SSL) es anómala el servidor Telnet envía mensajes de diagnóstico CPDBC *nm* al trabajo QTVTELNET.

Comprobación de las anotaciones de trabajo de Telnet

Cuando la inicialización y negociación de la capa de sockets seguros (SSL) es anómala el servidor Telnet envía mensajes de diagnóstico CPDBC *nm* al trabajo QTVTELNET.

Para comprobar las anotaciones de trabajo del servidor Telnet, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Red** → **Configuración TCP/IP** → **IPv4**.
2. Pulse **Conexiones**.
3. Pulse con el botón derecho del ratón la dirección IP de la estación de trabajo cliente anómala y seleccione **Trabajos**. Anote el nombre de trabajo.
4. Expanda **Gestión de trabajos** → **Trabajos de servidor**.
5. Pulse **QTVTELNET** con el botón derecho del ratón, en la columna Nombre de trabajo.

6. Seleccione **Anotaciones de trabajo**.
7. Busque el mensaje CPDBC *mm* en la columna ID de mensaje.

Debe tener presente lo siguiente acerca de los trabajos del servidor Telnet:

- Solamente se inicia un trabajo QTVTELNET cuando la inicialización del escucha SSL es anómala.
- Los trabajos QTVDEVICE y QTVTELNET se inician cuando lo hace el servidor Telnet tras reiniciarse el sistema.
- Cuando el servidor Telnet inicia un escucha SSL, también se inicia el mismo número de trabajos QTVTELNET y QTVDEVICE.
- El mandato ENDTCPSVR *TELNET o ENDTCP finaliza los trabajos QTVTELNET.
- Cuando el subsistema QSYSWRK finaliza, los trabajos QTVDEVICE finalizan.

Conceptos relacionados

“Inicialización y negociación de SSL” en la página 38

Aquí puede encontrar información detallada sobre las interacciones entre clientes, servidores Telnet y la capa de sockets seguros (SSL).

Tareas relacionadas

“Comprobación de la existencia de un escucha SSL activo” en la página 99

Utilice este procedimiento para comprobar la existencia de un escucha de capa de sockets seguros (SSL) activo. El servidor Telnet debe estar activo y preparado para recibir intentos de conexión.

Códigos de retorno de SSL

En este tema se muestran los códigos de retorno de la capa de sockets seguros (SSL) del sistema de los problemas más habituales que pueden producirse durante la inicialización o negociación de SSL.

Debe realizar estos pasos antes de utilizar las siguientes tablas de código de retorno:

- Debe encontrar el código de retorno de SSL en las anotaciones del trabajo QTVTELNET.
- En algunos casos, deberá trabajar con el Gestor de certificados digitales (DCM) para corregir los problemas relacionados con los certificados de la autoridad certificadora (CA) o los certificados del sistema.
- Cuando copie la información del certificado de CA para el cliente Telnet SSL, no olvide incluir las líneas que contienen las palabras BEGIN CERTIFICATE y END CERTIFICATE.

Tabla 20. Códigos de retorno habituales

Código de retorno	Descripción
-2	<p>No se dispone de ningún certificado de sistema para el proceso de SSL. El servidor Telnet inicializa satisfactoriamente SSL, pero la negociación SSL es anómala. En la ventana del cliente Telnet SSL no aparece ningún panel de inicio de sesión. No se ha asignado un certificado de sistema a la aplicación QIBM_QTV_TELNET_SERVER.</p> <p>Consulte el certificado de sistema y compruebe que aparece el valor Sí en la columna Certificado asignado. Si el valor es No, cree un certificado de sistema para la aplicación QIBM_QTV_TELNET_SERVER.</p>
-4	<p>El certificado de la CA o el certificado de sistema no es correcto. El certificado de sistema no es privado o no es de confianza. Los campos Clave privada y De confianza del certificado del servidor no son correctos. La ventana del cliente Telnet SSL no presenta ningún panel de inicio de sesión.</p> <p>Añada información de la CA al cliente Telnet SSL. Si utiliza System i Access para Windows como cliente Telnet SSL, consulte la información acerca de la gestión de certificados públicos de Internet para las sesiones de comunicaciones SSL. De lo contrario, consulte cómo obtener una copia del certificado de CA privado para obtener instrucciones al respecto.</p>

Tabla 20. Códigos de retorno habituales (continuación)

Código de retorno	Descripción
-16	No se reconoce el sistema igual. Este problema es el más habitual cuando un cliente Telnet SSL intenta establecer una sesión SSL por vez primera. La ventana del cliente Telnet SSL no presenta ningún panel de inicio de sesión. Añada información de certificado de la CA al cliente Telnet SSL.
-18	El certificado de sistema es auto-firmado y el servidor lo utiliza como certificado CA. El certificado de sistema que se asigna a la aplicación QIBM_QTV_TELNET_SERVER debe ser de confianza, debe estar firmado por una autoridad certificadora y debe ser utilizado dentro del período de validez. Deberá crear un certificado CA y asociarlo al certificado de sistema. El servidor Telnet no inicializa SSL si el certificado de sistema es incorrecto. Cree un certificado CA y asícielo al certificado de sistema.
-23	El certificado de sistema no está firmado por una autoridad certificadora de confianza. El certificado de sistema que se asigna a la aplicación QIBM_QTV_TELNET_SERVER debe ser de confianza, debe estar firmado por una autoridad certificadora y debe ser utilizado dentro del período de validez. Cambie el certificado CA a De confianza. Si desea obtener instrucciones, consulte cómo gestionar las aplicaciones en el DCM.
-24	El período de tiempo de validez del certificado CA ha finalizado. Está utilizando un certificado vencido. La ventana del cliente Telnet SSL no presenta ningún panel de inicio de sesión. Renueve el certificado CA utilizado para crear el certificado de sistema.
-93	SSL no está disponible para su utilización. Los clientes Telnet SSL no pueden conectarse a un host porque no hay ningún escucha SSL activo. Instale los requisitos de software para dar soporte a Telnet SSL y gestionar certificados. Si desea obtener instrucciones, consulte el tema Comprobación del estado del sistema.

Otros códigos de retorno de SSL

Para los códigos de retorno SSL de la tabla siguiente, utilice el DCM para verificar que los certificados digitales cumplan los siguientes requisitos:

- El certificado CA es válido y no ha caducado.
- La aplicación del servidor Telnet QIBM_QTV_TELNET_SERVER tiene el valor Sí en la columna Certificado asignado.
- Una autoridad certificadora firma el certificado de sistema.
- El certificado de sistema es de confianza.
- El certificado de sistema se utiliza dentro del período de validez que se indica en el certificado.

Tabla 21. Otros códigos de retorno de SSL

Código de retorno	Descripción
-1	No se dispone de cifras o no se especifican
-6	El sistema operativo i5/OS no soporta el tipo de certificado
-10	Se ha producido un error en el proceso de SSL. En las anotaciones de trabajo, compruebe el mensaje CPExxx, donde xxx es el valor de error de los sockets
-11	SSL ha recibido un mensaje con un formato incorrecto
-12	Se ha recibido un código de autenticación incorrecto
-13	SSL no soporta la operación

Tabla 21. Otros códigos de retorno de SSL (continuación)

Código de retorno	Descripción
-14	La firma del certificado no es válida
-15	El certificado es incorrecto
-17	Se ha denegado el permiso para acceder al objeto
-20	No ha podido asignarse el almacenamiento necesario para el proceso de SSL
-21	SSL ha detectado un estado incorrecto en la sesión SSL
-22	Se ha cerrado el socket que utiliza la conexión SSL
-25	La fecha del certificado tiene un formato incorrecto
-26	La longitud de la clave es incorrecta para su exportación
-90	No es un archivo de claves
-91	La contraseña de la base de datos de claves ha caducado
-92	El certificado no es válido o el programa de salida lo ha rechazado
-94	No se ha invocado previamente SSL_Init() para el trabajo
-95	No hay ningún archivo de claves para la inicialización de SSL
-96	No se ha habilitado SSL
-97	El conjunto de cifras especificado no es válido
-98	La sesión SSL ha finalizado
-99	Se ha producido un error desconocido o inesperado durante el proceso de SSL
-1010	No se permite el cifrado doble cuando se utiliza AC2 e IP-SEC

Tareas relacionadas

Configuración de DCM

Gestión de la asignación de certificados para una aplicación

Gestión de certificados públicos de Internet para las sesiones de comunicaciones SSL

Crear y operar una CA local

Gestión de las aplicaciones en el DCM

“Comprobación del estado del sistema” en la página 98

Debe confirmar que Telnet está preparado para las sesiones de capa de sockets seguros (SSL).

Referencia relacionada

Obtención de una copia del certificado de CA privado

Salidas del programa de servicio TRCTCPAPP

Puede ejecutar un rastreo de componentes del gestor de terminales virtuales (VTM) con el campo de datos de usuario establecido en Telnet.

En el caso del mandato de rastreo de aplicación TCP/IP (TRCTCPAPP), el listado del rastreo de componentes VTM se muestra como un archivo en spool, denominado VTMTRACE con el campo de datos de usuario establecido en TELNET. El sistema coloca este archivo en la cola de salida predeterminada del perfil que ejecuta la llamada TRCTCPAPP *TELNET *OFF. Al mismo tiempo, todos los registros de incidencias de trabajos de servidor se vuelcan en archivos en spool denominados QTOCTTRC con los datos de usuario establecidos en QTVnnnnn.

A continuación figura un ejemplo de lo que verá en las anotaciones de trabajo interactivo cuando efectúe una llamada TRCTCPAPP *OFF.

```

Entrada de mandato                                SYSNAM03
Nivel de petición: 1
Todos los mensajes y mandatos anteriores:
> trctcpapp *telnet *off
Archivo de impresora en spool 1 abierto para salida.
Datos rastreo para aplic. TELNET con formato: datos us. VTMTRACE en spool 'TELNET'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017231'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017230'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017229'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017232'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017233'
Datos rastreo para apl. TELNET con formato: datos us. QTOCTTRC en spool 'TV017234'
Más...
Escriba un mandato y pulse Intro.
===>
F3=Salir F4=Solicitud F9=Recuperar F10=Excluir mensajes detallados
F11=Visualizar todo F12=Cancelar F13=Asistente de información F24=Más teclas

```

A continuación se muestra un ejemplo de lo que verá en la cola de salida predeterminada.

```

Trabajar con todos los archivos en spool
Escriba las opciones y pulse Intro.
1=Enviar 2=Cambiar 3=Retener 4=Suprimir 5=Visualizar 6=Liberar 7=Mensajes
8=Atributos 9=Trabajar con estado de impresión

Opc Archivo Usuario Cola Dispositivo o Total de
datos usuario Est páginas Página
VTMTRACE JEFF JEFFSOUTQ TELNET HLD 46 1
QTOCTTRC JEFF JEFFSOUTQ TV017231 HLD 4 1
QTOCTTRC JEFF JEFFSOUTQ TV017231 HLD 2 1

Parámetros para opciones 1, 2, 3 o mandato
===>
F3=Salir F10=Vista 4 F11=Vista 2 F12=Cancelar F22=Impresoras F24=Más teclas

```

Solo se crea un archivo denominado VTMTRACE. Si la modalidad Telnet SSL está operativa en el servidor, puede tener uno o más archivos QTOCTTRC.

A continuación se muestra un ejemplo de un archivo QTOCTTRC. Este archivo en spool es un trabajo del servidor Telnet (QTVTELNET), en oposición a un trabajo QTVDEVICE.

```

                                Visualizar archivo en spool
Archivo . . . . . : TV017231                               Página/Línea 1/6
Control . . . . . :                                         Columnas      1 - 78
Buscar . . . . . :
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
5769TC1 V4R4M0 990521 TRCTCPAPP Salida NomSis Fecha-12/11/98 Hora-14:08:32 Pág.-
Atributos TRCTCPAPP
  Aplicación.....: Servidor Telnet
  Tamaño alm. int. (KB).....: 0
                        (Valor por omis. 0 para alm. int. de 16 MB)
  Acción de rastreo completo..: *WRAP
  ID de trabajo.....: 017231/QTCP /QTVTELNET
  Fecha/hora inicial.....: Vie Dic 11 13:50:33 1998
  Fecha/hora final.....: Vie Dic 11 14:08:34 1998
  Reinicio de almac. int. rast: No
Atributos de servidor Telnet
  Servidor de inicio autom....: 'Y'
  Servidores de número.....: 2
  Tiempo espera vida sesión...: 0
  Tipo de NVT predeterminado..: >*VT100<
  Tabla EBCDIC/ASCII salida...: >*CCSID <
  Tabla ASCII/EBCDIC entrada..: >*CCSID <
  ID de juego de caracteres...: 84542
  ID versión atributos ....., >V4R4M0 <
Estructura de almacenamiento intermedio de Trace_common:
80000000 00000000 161A8753 14001074 | .....g.....| Byte 16
80000000 00000000 161A8753 14FFFFE4 | .....g....U| Byte 48
80000000 00000000 161A8753 14005820 | .....g.....| Byte 80
00FFF000 00000084 F0F1F7F2 F3F1D8E3 | ..0....d017231QT| Byte 112
C3D74040 40404040 D8E3E5E3 C5D3D5C5 | CP QTVTELNE| Byte 144
E340C699 8940C485 8340F1F1 40F1F37A | T Vie Dic 11 13:| Byte 176
F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017| Byte 208
F2F3F140 |231 | Byte 228
Registros de incidencias:
qtvtnet: Trabajo: QTVTELNET/QTCP/017231
(C) Copyright IBM Corporation, 1999
Material bajo licencia - Propiedad de programa de IBM.
Consulte Copyright Instructions Form No. G120-2083
IDProd: 5769-SS1 Rel: V4R4M0 Vers: V4R4M0 PTR: P3684767
qtvtnet: Programa QTVTELNET con fecha 04 Diciembre 1998 en ejecución
qtvtnet: Archivo de origen: qtvtnet.pIC
qtvtnet: Última modificación: Mié Dic 9 11:57:40 1998
qtvtnet: Última compilación a las 12:00:10 el 9 Dic 1998
qtvtnet: Argumentos pasados: 1
qtvtnet: Hora de inicio: Vie Dic 11 13:50:34 1998
qtvtnet: sigaction() para SIGUSR1 es EndClientSession()
qtvtnet: Establecer identidad de trabajo de servidor Telnet para OpNav
qtvtnet: Necesario configurar SSL_Init_Application()
qtvtnet: SSL_Init_Application() satisfactoria
qtvtnet: Buscar bloque de control de servidor Telnet
qtvtnet: Bloquear bloque de control de servidor Telnet
qtvtnet: Abrir controlador a secuencia
qtvtnet: Primer trabajo de servidor Telnet...

F3=Salir   F12=Cancelar F19=Izquierda F20=Derecha   F24=Más teclas

```

A continuación se muestra un ejemplo de otro archivo QTOCTTRC. Este es un archivo en spool del gestor de dispositivos, en oposición al trabajo de servidor QTVTELNET.

```

                                Visualizar archivo en spool
Archivo . . . . : TV017230                               Página/Línea  1/6
Control . . . . :                                         Columnas      1 - 78
Buscar . . . . :
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...
Atributos TRCTCPAPP
  Aplicación.....: Servidor Telnet
  Tamaño alm. int. (KB).....: 0
                        (Valor por omis. 0 para alm. int. de 16 MB)
  Acción de rastreo completo..: *WRAP
  ID de trabajo.....: 017230/QTCP /QTVDEVICE
  Fecha/hora inicial.....: Vie Dic 11 13:50:33 1998
  Fecha/hora final.....: Vie Dic 11 14:08:39 1998
  Reinicio de almac. int. rast: No
Atributos de servidor Telnet
  Servidor de inicio autom....: Y
  Servidores de número.....: 2
  Tiempo espera vida sesión...: 0
  Tipo de NVT predeterminado..: >*VT100<
  Tabla EBCDIC/ASCII salida...: >*CCSID <
5769TC1 V4R4M0 990521 TRCTCPAPP Salida NomSis Fecha-12/11/98 Hora-14:08:32 Pág.-
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...
  Tabla ASCII/EBCDIC entrada..: >*CCSID <
  ID de juego de caracteres...: 84542
  ID versión atributos .....: >V4R4M0 <
Estructura de almacenamiento intermedio de Trace_common:
80000000 00000000 3DA86C25 5F001074 | .....y...| Byte 16
80000000 00000000 3DA86C25 5FFFFFFE4 | .....y..U| Byte 48
80000000 00000000 3DA86C25 5F002F64 | .....y...| Byte 80
00FFF000 00000084 F0F1F7F2 F3F0D8E3 | ..0....d017230QT| Byte 112
C3D74040 40404040 D8E3E5C4 C5E5C9C3 | CP QTVDEVIC| Byte 144
C540C699 8940C485 8340F1F1 40F1F37A | E Vie Dic 11 13:| Byte 176
F5F07AF3 F340F1F9 F9F8D8E3 E5F0F1F7 | 50:33 1998QTV017| Byte 208
F2F3F040 |230 | Byte 228
Registros de incidencias:
qvtncsh: >>>> entrada
(C) Copyright IBM Corporation, 1999.
Material bajo licencia - Propiedad de programa de IBM.
Consulte Copyright Instructions Form No. G120-2083
IDProd: 5769-SS1 Release: V4R4M0 Versión: V4R4M0 PTR: P3684767
qvtncsh: Programa QTVTNC SH con fecha 04 Diciembre 1998 en ejecución
qvtncsh: iActiveLogLevel: 0
qvtncsh: Archivo de origen: qvtncsh.c
qvtncsh: Última modificación: Mié Dic 9 11:48:33 1998
qvtncsh: Última compilación a las 11:59:42 el 9 Dic 1998
qvtncsh: SignalHandler() registrado con signal()
qvtncsh: Argumentos pasados: 4
qvtncsh: argc: 4
qvtncsh: argv[0]: >QSYS/QTVTNC SH<
qvtncsh: argv[1]: ><
qvtncsh: argv[2]: >1p<
qvtncsh: argv[3]: >s<
SignalHandler: >>>> entrada
SignalHandler: Señal detectada SIGSEGV

F3=Salir   F12=Cancelar F19=Izquierda F20=Derecha   F24=Más teclas

```

Conceptos relacionados

“Material necesario para informar de problemas de Telnet”

Normalmente, debe proporcionar esta información al representante de servicio cuando notifique un problema de Telnet.

Material necesario para informar de problemas de Telnet

Normalmente, debe proporcionar esta información al representante de servicio cuando notifique un problema de Telnet.

- Las anotaciones de trabajo de servidor Telnet:

- Anotaciones de trabajo QTVTELNET
- Anotaciones de trabajo QTVDEVICE
- Algunos detalles sobre el problema. Por ejemplo:
 - El tipo de host remoto que utiliza con Telnet como origen o destino como, por ejemplo, System i, System z o System p. Esto es de especial utilidad si se llevan a cabo funciones Telnet en cascada.
 - El tipo de cliente que intenta conectarse al servidor Telnet como, por ejemplo, IBM Personal Communications y System i Access para Windows.
- Las anotaciones de trabajo del trabajo interactivo que ejecuta el cliente Telnet (cuando está investigándose el cliente Telnet).
- La salida del rastreo del trabajo (TRCJOB) correspondiente al trabajo interactivo anómalo (de especial importancia si ejecuta el cliente Telnet).

Nota: utilice TRCJOB *ON para iniciar este rastreo. El resultado es un archivo en spool QPSRVTRC en el trabajo interactivo.

- Un rastreo de comunicaciones de la anomalía, en formato tanto ASCII como EBCDIC, que contiene únicamente datos TCP/IP. El representante de servicio puede indicarle que incluya mensajes de difusión general en este rastreo. Además, puede que deba filtrar este rastreo en una dirección IP específica si tiene una gran cantidad de tráfico en la red y que deba saber la dirección IP del cliente anómalo.
- Todas las anotaciones de código interno bajo licencia (LIC) con el código principal 0700 y el código secundario 005x desde el momento de la anomalía. Además, puede haber algunas anotaciones LIC informativas con el código principal 0701 y el código secundario 005x que pueden resultar útiles pero no necesariamente fundamentales.
- Un rastreo del componente LIC del gestor de terminales virtuales (VTM). Puede reunir los datos de este rastreo con el mandato Rastrear aplicación TCP/IP (TRCTCPAPP) o con el mandato Arrancar herramientas de servicio del sistema (STRSST). Si desea obtener todos los detalles sobre cómo utilizar el mandato Rastrear aplicación TCP/IP (TRCTCPAPP), consulte la descripción del mandato TRCTCPAPP.

Observará que el rendimiento queda afectado cuando ejecute el rastreo de LIC de VTM. A continuación figuran algunos ejemplos de cómo utilizar este mandato:

- Para rastrear toda la actividad de VTM:
TRCTCPAPP APP(*TELNET) SET(*ON)
- Para rastrear la actividad de un dispositivo específico, si sabe el nombre del dispositivo:
TRCTCPAPP APP(*TELNET) SET(*ON) DEVD(nombredispositivo)
- Para rastrear la actividad de un dispositivo específico, si sabe la dirección IP del cliente:
TRCTCPAPP APP(*TELNET) SET(*ON) RMTNETADR(*INET'www.xxx.yyy.zzz')
- Para desactivar el rastreo y enviar a la salida el archivo en spool:
TRCTCPAPP APP(*TELNET) SET(*OFF)

Nota: antes de ejecutar este mandato, el representante de servicio debe proporcionarle detalles concretos sobre los parámetros de rastreo que debe utilizar para su problema. De esta forma se asegurará de reunir la información correcta en relación con el problema.

Conceptos relacionados

“Salidas del programa de servicio TRCTCPAPP” en la página 102

Puede ejecutar un rastreo de componentes del gestor de terminales virtuales (VTM) con el campo de datos de usuario establecido en Telnet.

Información de diagnóstico generada automáticamente

Algunos errores del servidor Telnet generan automáticamente información de diagnóstico. En este tema se describe cómo recuperar esta información.

Puede haber información de diagnóstico generada automáticamente que se obtiene cuando se producen determinados errores dentro del servidor Telnet. En ocasiones el representante de servicio necesitará esta información de diagnóstico para analizar correctamente un problema del servidor Telnet.

Si un trabajo de Telnet o del gestor de dispositivos falla con un error FFDC (captura de datos en primer error), verá los archivos en spool bajo el perfil WRKSPLF QTCP. Cuando un trabajo falla con un error FFDC, cada uno de los trabajos anómalos automáticamente tendrá dos vuelcos. Uno de los vuelcos se realiza llamando a DSPJOB *PRINT y DSPJOBLOG *PRINT efectúa el otro vuelco. De este modo, los atributos de anotaciones de trabajo y ejecución de trabajo se vuelcan y se obtiene la salida del grupo de datos de usuario junto con un identificador de número de trabajo. A continuación puede cotejarlo con cualquier salida de rastreo de componentes VTAM.

Puede ver un total de 4 archivos en spool (2 para el trabajo QTVTELNET y 2 para el trabajo QTVDEVICE). Si el sistema encuentra un error FFDC, estos archivos se generan automáticamente. Para consultar un ejemplo, vea la figura siguiente:

```

Trabajar con todos los archivos en spool

Escriba las opciones y pulse Intro.
  1=Enviar  2=Cambiar 3=Retener 4=Suprimir 5=Visualizar 6=Liberar 7=Mensajes
  8=Atributos      9=Trabajar con estado de impresión

Opc  Archivo      Usuario      Cola      Dispositivo o
      QPJOBLOG    QTCP        QEZJOBLOG TV016868  HLD  4
      QPDSPJOB    QTCP        QPRINT     TV016868  HLD  7
      QPJOBLOG    QTCP        QEZJOBLOG TV016955  HLD  3
      QPDSPJOB    QTCP        QPRINT     TV016955  HLD  7
      QPJOBLOG    QTCP        QEZJOBLOG TV017231  HLD  3
      QPJOBLOG    QTCP        QEZJOBLOG TV017232  HLD  3
      QPDSPJOB    QTCP        QPRINT     TV017232  HLD  7
      QPDSPJOB    QTCP        QPRINT     TV017231  HLD  7

Parámetros para opciones 1, 2, 3 o mandato
===>
F3=Salir F10=Vista 4 F11=Vista 2 F12=Cancelar F22=Impresoras F24=Más teclas

```

Información relacionada con Telnet

Las publicaciones IBM Redbooks y los sitios Web contienen información relacionada con la colección de temas de Telnet. Puede ver o imprimir los archivos PDF que desee.

IBM Redbooks

V4 TCP/IP for AS/400 : More Cool Things Than Ever  (10.035 KB, aproximadamente)

Esta publicación proporciona amplia información sobre TCP/IP, con casos prácticos de ejemplo que muestran soluciones habituales con configuraciones de ejemplo.

Sitios Web

- **Internet Assigned Numbers Authority (IANA)**  (www.iana.org)
Puede obtener información sobre las asignaciones de números de puerto más habituales.

- **The Internet Engineering Task Force (IETF)**  (www.ietf.org)

Lea peticiones de comentarios (RFC), como la RFC 4777 5250 Telnet Enhancements .

Referencia relacionada

Información sobre licencia de código y exención de responsabilidad

IBM le otorga una licencia de copyright no exclusiva para utilizar todos los ejemplos de código de programación, a partir de los que puede generar funciones similares adaptadas a sus necesidades específicas.

SUJETO A LAS GARANTÍAS ESTATUTARIAS QUE NO PUEDAN EXCLUIRSE, IBM Y LOS DESARROLLADORES Y SUMINISTRADORES DE PROGRAMAS DE IBM NO OFRECEN NINGUNA GARANTÍA NI CONDICIÓN, YA SEA IMPLÍCITA O EXPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS O CONDICIONES IMPLÍCITAS DE COMERCIALIZACIÓN, ADECUACIÓN A UN PROPÓSITO DETERMINADO Y NO VULNERACIÓN CON RESPECTO AL PROGRAMA O AL SOPORTE TÉCNICO, SI EXISTE.

BAJO NINGUNA CIRCUNSTANCIA, IBM Y LOS DESARROLLADORES O SUMINISTRADORES DE PROGRAMAS DE IBM SE HACEN RESPONSABLES DE NINGUNA DE LAS SIGUIENTES SITUACIONES, NI SIQUIERA EN CASO DE HABER SIDO INFORMADOS DE TAL POSIBILIDAD:

1. PÉRDIDA DE DATOS O DAÑOS CAUSADOS EN ELLOS;
2. DAÑOS ESPECIALES, ACCIDENTALES, DIRECTOS O INDIRECTOS, O DAÑOS ECONÓMICOS DERIVADOS;
3. PÉRDIDAS DE BENEFICIOS, COMERCIALES, DE INGRESOS, CLIENTELA O AHORROS ANTICIPADOS.

ALGUNAS JURISDICCIONES NO PERMITEN LA EXCLUSIÓN O LA LIMITACIÓN DE LOS DAÑOS DIRECTOS, ACCIDENTALES O DERIVADOS, POR LO QUE PARTE DE LAS LIMITACIONES O EXCLUSIONES ANTERIORES, O TODAS ELLAS, PUEDE NO SER PROCEDENTE EN SU CASO.

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en Estados Unidos de América.

Es posible que en otros países IBM no ofrezca los productos, servicios o características que se describen en este documento. El representante local de IBM le puede informar acerca de los productos y servicios que actualmente están disponibles en su localidad. Las referencias hechas a productos, programas o servicios de IBM no pretenden afirmar ni dar a entender que únicamente puedan utilizarse dichos productos, programas o servicios de IBM. Puede utilizarse en su lugar cualquier otro producto, programa o servicio funcionalmente equivalente que no vulnere ninguno de los derechos de propiedad intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes de aprobación que cubran los temas descritos en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar las consultas sobre licencias, por escrito, a la siguiente dirección:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
Estados Unidos de América

Para consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el departamento de propiedad intelectual de IBM en su país o envíe las consultas, por escrito, a:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japón

El párrafo siguiente no es de aplicación en el Reino Unido ni en ningún otro país en el que tales disposiciones sean incompatibles con la legislación local: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGUNA CLASE, EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN Y DE COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad, ni implícitas ni explícitas, en determinadas transacciones, por lo que cabe la posibilidad de que esta declaración no se aplique en su caso.

Esta información puede contener imprecisiones técnicas o errores tipográficos. La información incluida en este documento está sujeta a cambios periódicos, que se incorporarán en nuevas ediciones de la publicación. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta publicación en cualquier momento y sin previo aviso.

Las referencias hechas en esta publicación a sitios Web que no son de IBM se proporcionan únicamente por cortesía y de ningún modo deben interpretarse como promoción de dichos sitios Web. Los materiales de estos sitios Web no forman parte de los materiales de IBM para este producto, y el usuario será responsable del uso que se haga de estos sitios Web.

IBM puede utilizar o distribuir la información que usted le suministre del modo que IBM considere conveniente sin incurrir por ello en ninguna obligación para con usted.

Los licenciarios de este programa que deseen obtener información acerca del mismo con el fin de: (i) intercambiar la información entre programas creados independientemente y otros programas (incluido este) y (ii) utilizar mutuamente la información que se ha intercambiado, deben ponerse en contacto con:

IBM Corporation
Software Interoperability Coordinator, Department YBWA
3605 Highway 52 N
Rochester, MN 55901
Estados Unidos de América

Esta información puede estar disponible, sujeta a los términos y condiciones pertinentes, e incluir en algunos casos el pago de una cantidad.

- | El programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible para él, lo proporciona IBM según los términos del Acuerdo de Cliente de IBM, el Acuerdo Internacional de Programas bajo Licencia de IBM, el Acuerdo de Licencia para Código de Máquina de IBM o cualquier otro acuerdo equivalente entre ambas partes.

La información concerniente a productos que no son de IBM se ha obtenido de los suministradores de dichos productos, de sus anuncios publicados o de otras fuentes de información pública disponibles. IBM no ha comprobado dichos productos y no puede afirmar la exactitud en cuanto a rendimiento, compatibilidad u otras características relativas a productos no IBM. Las consultas acerca de las prestaciones de los productos que no son de IBM deben dirigirse a los suministradores de tales productos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlas de la forma más completa posible, los ejemplos incluyen nombres de personas, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con los nombres y direcciones utilizados por una empresa real es mera coincidencia.

| Información sobre la interfaz de programación

Esta publicación de Telnet documenta las interfaces de programación cuya finalidad es permitir al cliente escribir programas para obtener los servicios de IBM i5/OS.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

AIX
AS/400
i5/OS
IBM
IBM (logotipo)
OS/2
OS/400
Redbooks
System i
System p
System z
System/370

- | Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe
- | Systems Incorporated en los Estados Unidos o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en Estados Unidos y/o en otros países.

Java y todas las marcas basadas en Java son marcas registradas de Sun Microsystems, Inc., en Estados Unidos y/o en otros países.

Los demás nombres de compañías, productos o servicios pueden ser marcas registradas o de servicio de terceros.

Términos y condiciones

Los permisos para utilizar estas publicaciones están sujetos a los siguientes términos y condiciones.

Uso personal: puede reproducir estas publicaciones para uso personal (no comercial) siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede distribuir ni visualizar estas publicaciones ni ninguna de sus partes, como tampoco elaborar trabajos que se deriven de ellas, sin el consentimiento explícito de IBM.

Uso comercial: puede reproducir, distribuir y visualizar estas publicaciones únicamente dentro de su empresa, siempre y cuando incluya una copia de todos los avisos de derechos de autor. No puede elaborar trabajos que se deriven de estas publicaciones, ni tampoco reproducir, distribuir ni visualizar estas publicaciones ni ninguna de sus partes fuera de su empresa, sin el consentimiento explícito de IBM.

Aparte de la autorización que se concede explícitamente en este permiso, no se otorga ningún otro permiso, licencia ni derecho, ya sea explícito o implícito, sobre las publicaciones, la información, los datos, el software o cualquier otra propiedad intelectual contenida en ellas.

IBM se reserva el derecho de retirar los permisos aquí concedidos siempre que, según el parecer del fabricante, se utilicen las publicaciones en detrimento de sus intereses o cuando, también según el parecer del fabricante, no se sigan debidamente las instrucciones anteriores.

No puede bajar, exportar ni reexportar esta información si no lo hace en plena conformidad con la legislación y normativa vigente, incluidas todas las leyes y normas de exportación de Estados Unidos.

IBM NO PROPORCIONA NINGUNA GARANTÍA SOBRE EL CONTENIDO DE ESTAS PUBLICACIONES. LAS PUBLICACIONES SE PROPORCIONAN "TAL CUAL", SIN GARANTÍA DE NINGUNA CLASE, YA SEA EXPLÍCITA O IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN, NO VULNERACIÓN E IDONEIDAD PARA UN FIN DETERMINADO.



Impreso en España