System i

Seguridad
Servicio de autenticación de red

Versión 6 Release 1

System i

Seguridad
Servicio de autenticación de red

Versión 6 Release 1

Nota

Antes de utilizar esta información y el producto al que hace referencia, lea la información que figura en el apartado “Avisos”, en la página 139.

Esta edición se aplica a la versión 6, release 1, modificación 0 de IBM i5/OS (número de producto 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.

Contenido

Capítulo 1. Servicio de autenticación de red

El servicio de autenticación de red permite que el producto System i y varios servicios del System i, como el programa bajo licencia System i Access para Windows, utilicen un ticket Kerberos como sustituto opcional del nombre y la contraseña de un usuario de cara a la autenticación.

El protocolo Kerberos, desarrollado por el Massachusetts Institute of Technology, permite que un sujeto principal (un usuario o un servicio) demuestre su identidad ante otro servicio en una red no segura. La autenticación de los sujetos principales se lleva a cabo mediante un servidor centralizado conocido como servidor Kerberos o centro de distribución de claves (KDC).

Nota: A lo largo de esta documentación, se emplea el término genérico *servidor Kerberos*.

El usuario se autentica con un sujeto principal y una contraseña que se almacenan en el servidor Kerberos. Después de autenticar el sujeto principal, el servidor Kerberos emite un ticket de otorgamiento de tickets (TGT) al usuario. Cuando un usuario necesita acceder a una aplicación o a un servicio de la red, la aplicación de cliente Kerberos existente en el PC del usuario envía el TGT de nuevo al servidor Kerberos con vistas a obtener un ticket de servicio para el servicio o la aplicación destino. Luego, la aplicación de cliente Kerberos envía el ticket de servicio al servicio o a la aplicación de cara a la autenticación. Si el servicio o la aplicación acepta el ticket, se establece un contexto de seguridad y entonces la aplicación del usuario puede intercambiar datos con un servicio destino. Las aplicaciones pueden autenticar a un usuario y reenviar con seguridad su identidad a otros servicios de la red. En cuanto se conoce a un usuario, se necesitan distintas funciones para verificar la autorización del usuario para utilizar los recursos de la red.

El servicio de autenticación de red implementa las siguientes especificaciones:

- Protocolo Kerberos Versión 5 tal como se define en la petición de comentarios (RFC) 1510
- Muchas de las interfaces de programación de aplicaciones (API) del protocolo Kerberos estándar frecuentes en el sector de hoy en día
- Las API del servicio de seguridad genérico (GSS) tal como se definen en las peticiones de comentarios (RFC) 1509, 1964 y 2743

La implementación en el i5/OS del servicio de autenticación de red funciona con los servicios de autenticación, delegación y confidencialidad de datos en conformidad con estas peticiones de comentarios (RFC) y las API de la interfaz de proveedor de servicios de seguridad (SSPI) de Microsoft Windows 2000. Microsoft Active Directory utiliza Kerberos como mecanismo de seguridad predeterminado. Cuando se añaden usuarios a Microsoft Active Directory, su identificación de Windows es equivalente a un sujeto principal Kerberos. El servicio de autenticación de red proporciona interoperatividad con Microsoft Active Directory y la correspondiente implementación del protocolo Kerberos.

Novedades de la V6R1

Lea acerca de la información nueva o con cambios significativos para la colección de temas del servicio de autenticación de red.

Nuevos mandatos de lenguaje de control de Kerberos

En V6R1, se han añadido los siguientes mandatos CL de Kerberos. Puede ejecutarlos en la línea de mandatos CL de i5/OS.

- Mandato Añadir entrada de tabla de claves de Kerberos (ADDKRBKTE)
- Mandato Añadir ticket de Kerberos (ADDKRBTKT)

- Mandato Cambiar contraseña de Kerberos (CHGKRBPWD)
- Mandato Suprimir archivo de memoria caché de credenciales de Kerberos (DLTKRBCCF)
- Mandato Visualizar archivo de memoria caché de credenciales de Kerberos (DSPKRBCCF)
- Mandato Visualizar entradas de tabla de claves de Kerberos (DSPKRBKTE)
- Mandato Suprimir entrada de tabla de claves de Kerberos (RMVKRBKTE)

Si desea obtener más información sobre estos mandatos, consulte la colección de temas de lenguaje de control y los temas siguientes en el servicio de autenticación de red:
- "Cambiar las contraseñas de Kerberos" en la página 115
- "Suprimir archivos de memoria caché de credenciales caducados" en la página 117
- "Visualizar memoria caché de credenciales" en la página 111
- "Obtener o renovar tickets de otorgamiento de tickets" en la página 108
- "Gestionar archivos de tabla de claves" en la página 113

Nuevo sujeto principal de servicio para el servidor del sistema de archivos de red

El sistema de archivos de red es un protocolo que permite que un sistema acceda a archivos a través de una red como si estuvieran en discos locales. En la plataforma System i, ahora puede añadir y actualizar entradas de la tabla de claves para el servidor del sistema de archivos de red. Si desea obtener más información, consulte "Planificar nombres de sujeto principal" en la página 82.

Cómo ver las novedades o los cambios realizados

Para ayudarle a detectar los cambios técnicos que se han realizado en esta información, se utiliza:
- La imagen  , que señala dónde empieza la información nueva o cambiada.
- La imagen  , que señala dónde termina la información nueva o cambiada.

En archivos PDF, es posible que vea barras de revisión (|) en el margen izquierdo de la información nueva y cambiada.

Para buscar información adicional sobre las novedades o los cambios realizados en este release, vea el memorándum para los usuarios.

Archivo PDF para el Servicio de autenticación de red

Puede ver e imprimir un archivo PDF de esta información.

Para ver o bajar la versión en PDF de este documento, seleccione Servicio de autenticación de red (aproximadamente 1792 KB).

Los archivos PDF de temas relacionados que puede ver o bajar son:

- Inicio de sesión único  (1147 KB), que contiene estos temas:
  - Casos prácticos que enseñan cómo se puede utilizar el servicio de autenticación de red junto con la correlación de identidades de empresa (EIM) para proporcionar el inicio de sesión único (SSO) en una empresa.
  - Información conceptual que explica el inicio de sesión único (SSO) y sus ventajas.
- Correlación de identidades de empresa (EIM)  (2836 KB), que contiene estos temas:
  - Casos prácticos que muestran la implementación habitual de EIM.
  - Información conceptual y de planificación que le ayudará a comprender y planificar EIM.

Más información

Encontrará esta documentación en el CD del paquete de expansión y Bonus Pack de AIX 5L o en el CD de *Network Authentication Enablement*:

- Manuales:
  - *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
  - *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Guardar archivos PDF

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

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

Bajar Adobe Reader

Necesita tener instalado Adobe Reader en el sistema para ver o imprimir estos PDF. Puede bajar una copia gratuita del sitio Web de Adobe (www.adobe.com/products/acrobat/readstep.html) .

Conceptos del servicio de autenticación de red

El servicio de autenticación de red da soporte a los protocolos Kerberos y a las API de servicios de seguridad genéricos (GSS) que proporcionan la autenticación de los usuarios en una red.

Son muchas las fuentes de información en las que se describen los protocolos Kerberos y las API de GSS, así que en este tema se exponen los elementos básicos que atañen específicamente al entorno System i.

Conceptos de Kerberos

El servicio de autenticación de red utiliza los términos del protocolo Kerberos, entre elloos: KDC, sujeto principal, tabla de claves y tickets de Kerberos.

KDC, sujeto principal y tabla de claves

El Centro de distribución de claves (KDC), también conocido como el servidor Kerberos, está compuesto por el servidor de autenticación y el servidor de otorgamiento de tickets. El servidor de autenticación emite tickets de otorgamiento de tickets y el servidor de otorgamiento de tickets emite tickets de servicio. Es importante que la máquina que debe funcionar como servidor Kerberos sea segura. Si alguna persona obtuviese acceso al servidor Kerberos, la seguridad de todo el reino podría verse comprometida.

En un reino Kerberos, el término *sujeto principal* hace referencia al nombre de un usuario o servicio. En el sistema operativo i5/OS, se utiliza el sujeto principal de servicio krbsvr400 para identificar el servicio que prestan los servidores System i Access para Windows, QFileSrv.400 y Telnet al autenticar desde el cliente ante la plataforma System i.

La tabla de claves se compone de entradas que contiene el nombre del sujeto principal del servicio y su clave secreta. En el sistema operativo i5/OS, se crea un archivo de tabla de claves durante la configuración del servicio de autenticación de red. Cuando un servicio solicita autenticación ante un sistema que tenga configurado el servicio de autenticación de red, el sistema operativo comprueba el archivo de tabla de claves en busca de las credenciales del servicio.

Para asegurarse de que los usuarios y los servicios se autentican como es debido, debe crear los usuarios y los servicios en el servidor Kerberos y en i5/OS. Las entradas se añaden a la tabla de claves durante el proceso del asistente del servicio de autenticación de red. También puede añadir entradas a la tabla de claves utilizando el mandato keytab en la interfaz basada en caracteres del intérprete Qshell.

Nota: Este nombre de Sistema de nombres de dominio (DNS) debe coincidir con el nombre de host definido en la máquina. Hallará más información sobre cómo funcionan el DNS y Kerberos conjuntamente en el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.

Tickets de Kerberos

Un *ticket de Kerberos* es un mecanismo de aplicaciones transparente que transmite la identidad de un sujeto principal que se inicia a su destino. Un ticket sencillo contiene la identidad, una clave de sesión, una indicación de fecha y hora, así como otra información del sujeto principal, que se sella con la clave secreta del destino. Los tickets de Kerberos pueden ser renovables, reenviables o transferibles por poderes.

Los tickets reenviables le permiten transferir su identidad completa (TGT) a otra máquina, mientras que los tickets transferibles por poderes solo le permiten transferir determinados tickets. Los tickets transferibles por poderes permiten que un servicio realice una tarea en nombre de un sujeto principal. El servicio debe poder tomar la identidad del sujeto principal para una finalidad determinada. Un ticket transferible por poderes indica al servidor Kerberos que puede emitir un ticket nuevo a una dirección de red diferente, basándose en el ticket de otorgamiento de tickets original. Para los tickets transferibles por poderes no se necesitan contraseñas.

En algunos casos, podría ser interesante que una aplicación o un servicio tengan tickets cuya validez se prolongue durante largo tiempo. Sin embargo, una persona podría aprovecharse de ese tiempo prolongado para robar las credenciales que serían válidas hasta la fecha de caducidad del ticket. Los tickets renovables permiten que las aplicaciones obtengan tickets válidos durante periodos de tiempo prolongados. En los tickets renovables hay dos fechas de caducidad. La primera fecha de caducidad es válida para la instancia actual del ticket y la segunda se refiere a la fecha de caducidad más tardía permitida para el ticket.

¿Cómo funciona el servicio de autenticación de red?

El producto System i puede actuar como servidor o como cliente en la red Kerberos. Es importante entender los procesos de autenticación y el flujo de los tickets en estas dos situaciones.

El protocolo Kerberos proporciona un método de autenticación para los usuarios y los servicios de la red. Como administrador de la red, puede configurar el servicio de autenticación de red para que la plataforma System i acepte los tickets Kerberos como procedimiento de autenticación. El producto System i y varias aplicaciones específicas del sistema funcionan a modo de cliente/servidor en una red Kerberos, solicitando tickets para los usuarios y para los servicios a efectos de autenticación. El protocolo Kerberos facilita a los usuarios y servicios una manera de demostrar sus identidades (de autenticarse) ante toda la red, pero en cambio no les otorga autorización sobre los recursos de la red. La autorización específica sobre las funciones de i5/OS se mantiene por medio de perfiles de usuario que se crean en el sistema operativo i5/OS.

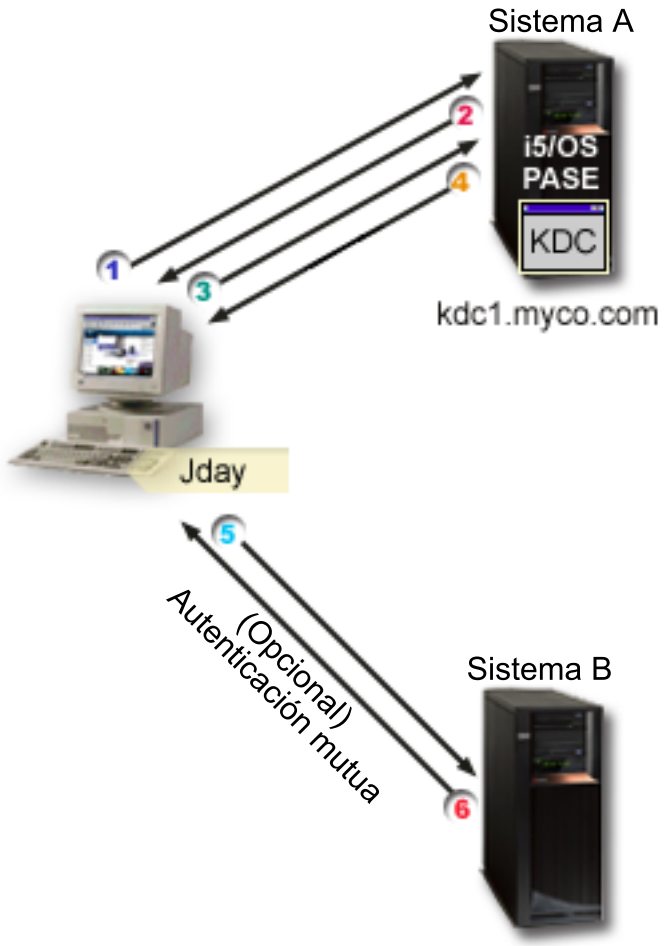
Cuando un usuario se autentica mediante Kerberos, se expide para el usuario un ticket inicial, al que llamamos ticket de otorgamiento de tickets (TGT). Luego, el usuario puede utilizar el TGT para solicitar un ticket de servicio con vistas a acceder a otros servicios y aplicaciones de la red. Para que la autenticación funcione satisfactoriamente, el administrador debe registrar en el servidor Kerberos a los usuarios, los sujetos principales de servicio de i5/OS y las aplicaciones que utilizan el protocolo Kerberos. El producto System i puede funcionar a modo de servidor, en el que los sujetos principales solicitan

autenticación ante los servicios, o puede funciona a modo de cliente, que solicita tickets para las aplicaciones y los servicios de la red. Los siguientes gráficos ilustran el flujo de los tickets en estas dos situaciones.

Producto System i como servidor

Este gráfico muestra cómo funciona la autenticación cuando un producto System i actúa como servidor en una red Kerberos. En este gráfico, el servidor Kerberos o el centro de distribución de claves (KDC) situado en i5/OS PASE expide tickets para el sujeto principal, jday.

El sujeto principal, jday, desea acceder a una aplicación del sistema A. En este caso, se utiliza la correlación de identidades de empresa (EIM) en el sistema para correlacionar el sujeto principal Kerberos con un perfil de usuario de i5/OS. Esto se lleva a cabo para cualquier función de System i que soporte la autenticación Kerberos, como puede ser System i Access para Windows.



Esta descripción muestra una visión general de cómo funciona este proceso de autenticación en una red:

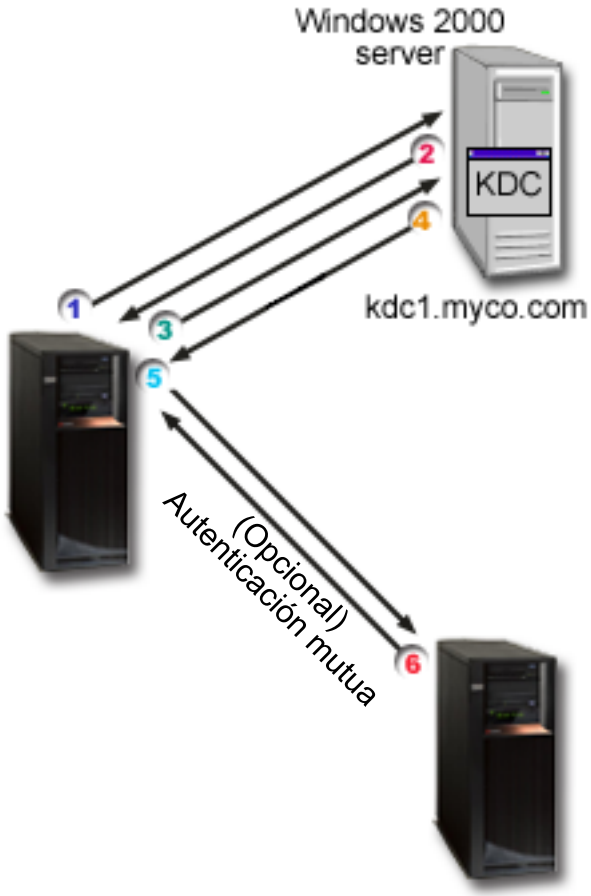
1. El usuario jday se autentica ante el servidor Kerberos proporcionando un sujeto principal y una contraseña cuando inicia sesión en el reino Kerberos. Así se envía una petición al servidor Kerberos para obtener un ticket de otorgamiento de tickets (TGT).
2. El servidor Kerberos valida el nombre de sujeto principal y la contraseña y envía un TGT a jday.
3. Jday necesita acceder a una aplicación de la plataforma System i. La aplicación cliente de Kerberos situada en el PC de jday envía el TGT al servidor Kerberos para solicitar un ticket de servicio para la aplicación o el servicio concreto, como puede ser System i Navigator. La estación

de trabajo del usuario gestiona su memoria caché de credenciales, que contiene tickets y otros datos identificativos del usuario. Estas credenciales se leen en la memoria caché a medida que se necesitan y las nuevas credenciales que se vayan obteniendo se almacenan en la memoria caché. De este modo la aplicación queda liberada de la responsabilidad de gestionar ella misma las credenciales.

4. El servidor Kerberos responde con el ticket de servicio.
5. La aplicación envía el ticket del servicio al servicio de System i para autenticar al usuario.
6. La aplicación del servidor valida el ticket llamando a las API del servicio de autenticación de red y, opcionalmente, puede remitir una respuesta al cliente de cara a una autenticación mutua.
7. Mediante una asociación EIM, el sujeto principal Kerberos se correlaciona con el perfil de usuario de i5/OS.

Producto System i como cliente

Este gráfico muestra cómo funciona la autenticación cuando un producto System i actúa como cliente en una red Kerberos. En este gráfico, el servidor Kerberos que se encuentra en el servidor Windows 2000, expide tickets para el usuario que se autenticó ante Kerberos. El sistema A se puede autenticar ante otros servicios. En este ejemplo, se utiliza EIM en el sistema B para correlacionar el sujeto principal Kerberos con un perfil de usuario. Esto se lleva a cabo para cualquier función de System i que soporte la autenticación Kerberos, como puede ser QFileSvr.400.



Esta descripción muestra una visión general de cómo funciona este proceso de autenticación en una red:

1. Un sujeto principal, jday, inicia sesión en el sistema A y luego solicita un ticket de otorgamiento de tickets (TGT) emitiendo un mandato kinit en el intérprete Qshell. El sistema envía esta petición al servidor Kerberos.
2. El servidor Kerberos valida el nombre de sujeto principal y la contraseña y envía un ticket de otorgamiento de tickets a jday.
3. Jday necesita acceder a una aplicación que se encuentra en el sistema B. Llamando a las API del servicio de autenticación de red, la aplicación envía el TGT de jday al servidor Kerberos para solicitar un ticket de servicio para la aplicación o el servicio concretos. La máquina local del sujeto principal gestiona una memoria caché de credenciales que contiene tickets, claves de sesión y otros datos identificativos del usuario. Estas credenciales se leen en la memoria caché a medida que se necesitan y las nuevas credenciales que se vayan obteniendo se almacenan en la memoria caché. De este modo la aplicación queda liberada de la responsabilidad de gestionar ella misma las credenciales.
4. El servidor Kerberos responde con el ticket de servicio.

   Nota: Hay que añadir un sujeto principal de servicio del sistema B al servidor Kerberos y además hay que configurar el servicio de autenticación de red en el sistema B.
5. La aplicación envía el ticket del servidor al servicio de System i para autenticar al usuario.
6. La aplicación del servidor valida el ticket llamando a las API del servicio de autenticación de red y, opcionalmente, puede remitir una respuesta al cliente de cara a una autenticación mutua.
7. Mediante una asociación EIM, el sujeto principal Kerberos se correlaciona con el perfil de usuario de i5/OS.

Protocolos del servicio de autenticación de red

El servicio de autenticación de red utiliza el protocolo Kerberos junto con las API de servicios de seguridad genéricos (GSS) de autenticación para prestar servicios de autenticación y seguridad.

Este tema proporciona una descripción general de los protocolos del servicio de autenticación de red y sobre cómo se utilizan en el entorno de System i. Para facilitar una información más completa sobre estos estándares, se proporcionan enlaces que llevan a las correspondientes peticiones de comentarios (RFC) y a otras fuentes de información externas.

Protocolo Kerberos

El protocolo Kerberos proporciona autenticación de tercer interlocutor, en la que los usuarios demuestran su identidad ante un servidor centralizado, llamado servidor Kerberos o centro de distribución de claves (KDC), el cual expide tickets para los usuarios. Luego, los usuarios pueden utilizar los tickets para demostrar sus identidades en la red. El ticket evita la necesidad de iniciar múltiples sesiones en los distintos sistemas. Las API del servicio de autenticación de red soportadas por el System i tienen su originen en el Massachusetts Institute of Technology y se han convertido en el estándar de hecho para utilizar el protocolo Kerberos.

Supuestos del entorno de seguridad

El protocolo Kerberos presupone todos los intercambios de datos se producen en un entorno en el que los paquetes se pueden insertar, cambiar o interceptar a voluntad. Utilice Kerberos como una capa de un plan de seguridad global. A pesar de que el protocolo Kerberos le permite autenticar a los usuarios y las aplicaciones en la red, debe tener en cuenta ciertas limitaciones al definir sus objetivos de seguridad de la red:

- El protocolo Kerberos no protege contra los ataques de denegación de servicio. Existen lugares en estos protocolos donde un intruso puede impedir que una aplicación participe en los pasos de autenticación correctos. Es preferible dejar la detección y la solución de estos ataques en manos de administradores y usuarios humanos.

- El hecho de compartir claves o el robo de las claves puede permitir ataques de imitación. Si de algún modo los intrusos logran robar la clave de un sujeto principal, podrán hacerse pasar por dicho usuario o servicio. Para minimizar esta amenaza, prohíba a los usuarios compartir sus claves e incluya esta política en sus normas de seguridad.
- El protocolo Kerberos no protege contra las vulnerabilidades típicas de las contraseñas, como la de adivinar una contraseña. Si un usuario elige una contraseña sencilla, un pirata podría montar con éxito un ataque de diccionario fuera de línea intentando repetidamente descifrar mensajes que se han cifrado bajo una clave derivada a partir de la contraseña del usuario.

Fuentes de información de Kerberos

Las peticiones de comentarios (RFC) son definiciones escritas de los estándares de protocolos y estándares propuestos que se utilizan para Internet. Las siguientes peticiones de comentarios (RFC) podrían servirle de ayuda para comprender el protocolo Kerberos:

RFC 1510
En la RFC 1510: Kerberos Network Authentication Service (V5), el equipo negociador de ingenieros de Internet (IETF) define formalmente el servicio de autenticación de red Kerberos (V5).

Para ver la RFC mencionada anteriormente, visite el motor de búsqueda del índice de RFC que se encuentra en el sitio Web del editor de RFC . Busque el número de la RFC que desea ver. Los resultados del motor de búsqueda visualizan el correspondiente título de la RFC, su autor, la fecha y el estado.

Kerberos: Network Authentication Protocol (V5)
La documentación oficial del Massachusetts Institute of Technology sobre el protocolo Kerberos proporciona información sobre programación y describe las características del protocolo.

Las API de servicios de seguridad genéricos (GSS)

Las interfaces de programación de aplicaciones (API) de los servicios de seguridad genéricos (GSS) proporcionan servicios de seguridad genéricos y están soportadas por una amplia gama de tecnologías de seguridad, como el protocolo Kerberos. Ello hace que las aplicaciones GSS sean transportables a diferentes entornos. Po este motivo, le recomendamos que utilice estas API en lugar de las API de Kerberos. Puede escribir aplicaciones que utilicen las API de GSS para comunicarse con otras aplicaciones y clientes de la misma red. Cada una de las aplicaciones que participan en la comunicación desempeña un papel en este intercambio. Con las API de GSS, las aplicaciones pueden realizar las siguientes operaciones:

- Determinar la identificación de usuario de otra aplicación.
- Delegar derechos de acceso a otra aplicación.
- Aplicar servicios de seguridad (como la confidencialidad y la integridad) por cada mensaje.

Fuentes de información de las API de GSS

Las peticiones de comentarios (RFC) son definiciones escritas de los estándares de protocolos y estándares propuestos que se utilizan para Internet. Las siguientes peticiones de comentarios (RFC) podrían servirle de ayuda para comprender las API de GSS:

RFC 2743
En la RFC 2743: Generic Security Service Application Program Interface Versión 2, Actualización 1, el equipo negociador de ingenieros de Internet (IETF) define formalmente las API de GSS.

RFC 1509
En la RFC 1509: Generic Security Service API : C-bindings, el equipo negociador de ingenieros de Internet (IETF) define formalmente las API de GSS.

RFC 1964

En la RFC 1964, The Kerberos Version 5 GSS-API Mechanism, el equipo negociador de ingenieros de Internet (IETF) define las especificaciones de Kerberos Versión 5 y de las API de GSS.

Para ver las RFC mencionadas anteriormente, visite el motor de búsqueda del índice de RFC que se encuentra en el sitio Web del editor de RFC  . Busque el número de la RFC que desea ver. Los resultados del motor de búsqueda visualizan el correspondiente título de la RFC, su autor, la fecha y el estado.

Variables de entorno del servicio de autenticación de red

Puede utilizar variables de entorno con el servicio de autenticación de red para influir en el comportamiento de las API de servicios de seguridad genéricos (GSS) y en las API del protocolo Kerberos.

Las variables de entorno le permiten cambiar la configuración y gestionar el servicio de autenticación en su red. En el sistema operativo i5/OS se puede trabajar con las variables de entorno de varias maneras.

Mandatos CL

- ADDENVVAR
- CHGENVVAR
- RMVENVVAR
- WRKENVVAR

En el tema “Herramienta de rastreo de API” en la página 129 encontrará un ejemplo de cómo utilizar las variables de entorno con el mandato CL ADDENVVAR. Este conjunto de variables de entorno le permite crear un archivo de anotaciones que rastrea cada una de las llamadas de las API de Kerberos y GSS. Con la herramienta de rastreo de API podrá resolver con métodos más avanzados los problemas que impliquen sus propias aplicaciones habilitadas para Kerberos, los problemas que pueden producirse durante la configuración del servicio de autenticación de red y los problemas que pueden producirse durante las peticiones de tickets de Kerberos.

Interfaces de programación de aplicaciones (API) C

- getenv()
- putenv()

Hallará descripciones y ejemplos de estas API en las notas de utilización de las API getenv() y putenv().

Mandatos de Qshell

- export -s nombre_var_ent=valor

Además, puede definir un archivo de variables de entorno (archivo envar) cuyas entradas tienen el **formato** variable_entorno=valor. Las variables que se hayan definido mediante el entorno Qshell o con los mandatos CL alteran temporalmente esas mismas variables del archivo envar. La variable de entorno _EUV_ENVAR_FILE permite especificar la ubicación del archivo que contiene estas entradas.

_EUV_ENVAR_FILE

Nombre del archivo que contiene definiciones de las variables de entorno. Si esta variable no está establecida, el valor predeterminado es utilizar el archivo envar situado en el directorio inicial (tal como lo especifica la variable de entorno _EUV_HOME o HOME).

Cada una de las líneas del archivo consta del nombre de la variable, un signo igual (=) y el valor de la variable, sin blancos intercalados ni otros signos de puntuación. El valor de la variable es todo lo que sigue al signo igual hasta el final de la línea (incluidos los blancos intercalados o finales). Las líneas que empiezan con un signo de almohadilla (#) se tratan como comentarios.

Para hacer que una línea continúe, se escribe una barra inclinada invertida (\) al final de la línea. Después de la barra inclinada invertida, no puede haber más blancos. La serie _EUV_ debe empezar en la columna 1.

Las variables de entorno no se establecen hasta la primera vez que se invoca una función de la unidad ejecutable de seguridad. Esto es especialmente útil para establecer las variables de entorno que se utilizarán en las funciones de la unidad ejecutable de seguridad, aunque también se puede utilizar para establecer las variables de entorno que se utilizan en las aplicaciones. En este caso, la aplicación no debe basarse en los valores de las variables de entorno hasta después que se haya inicializado la unidad ejecutable de seguridad. El perfil de usuario bajo el que se ejecuta este programa debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a este archivo, así como la autorización *R sobre el propio archivo.

_EUV_HOME y HOME
El directorio inicial (home) de la unidad ejecutable de seguridad se establece en el valor de la variable de entorno _EUV_HOME. Si esta variable no está especificada, se utiliza la variable HOME para determinar el directorio inicial de la unidad ejecutable de seguridad. Si ninguna de las dos variables de entorno está establecida, se utiliza el directorio inicial configurado en el perfil de usuario que se ejecuta en ese momento. Si el directorio inicial no existe, se utiliza el directorio de trabajo actual. El acceso público a este directorio debe estar limitado a *EXCLUDE o *R.

_EUV_SEC_KRB5CCNAME_FILE
Nombre del archivo que sirve para localizar la memoria caché de credenciales predeterminada de Kerberos. Si esta variable no está establecida, el valor predeterminado es utilizar el archivo krb5ccname situado en el directorio inicial de la unidad ejecutable de seguridad. El perfil de usuario que está ejecutando debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a este archivo. Si el archivo todavía no existe, el perfil de usuario que está ejecutando debe tener la autorización *WX sobre el directorio padre que contiene este archivo. El usuario debe asegurarse de que el acceso público al directorio padre sea limitado para impedir que un usuario con malas intenciones pueda cambiar el archivo de memoria caché de credenciales utilizado.

_EUV_SVC_MSG_LOGGING
Destino en el que se anotan los mensajes. Los valores válidos son:

NO_LOGGING
Suprimir todos los mensajes. Este es el valor predeterminado.

STDOUT_LOGGING
Escribir todos los mensajes (informativos y de error) en la salida estándar (stdout) y escribir los mensajes de error en la salida de error estándar (stderr).

STDERR_LOGGING
Escribir los mensajes informativos en la salida estándar y los mensajes de error en la salida de error estándar.

_EUV_SVC_MSG_LEVEL
Nivel de los mensajes que se anotarán. Los mensajes que no coincidan con este criterio se suprimirán. El valor predeterminado es anotar todos los mensajes. Los valores válidos son:

FATAL
Se anotan sólo los mensajes irrecuperables.

ERROR
Sólo se anotan los mensajes de error y los irrecuperables.

USER Sólo se anotan los mensajes de usuario, de error y los irrecuperables.

WARNING
Sólo se anotan los mensajes de aviso, de usuario, de error y los irrecuperables.

NOTICE
Sólo se anotan los mensajes de atención, de aviso, de usuario, de error y los irrecuperables.

VERBOSE
Se anotan todos los mensajes.

_EUV_SVC_STDOUT_FILENAME
Nombre totalmente calificado del archivo que recibirá los mensajes de salida estándar. Si esta variable de entorno no está definida, los mensajes se escriben en la salida estándar (stdout). El perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a este archivo y la autorización *WX sobre el directorio padre que contiene este archivo.

_EUV_SVC_STDERR_FILENAME
Nombre totalmente calificado del archivo que recibirá los mensajes de error estándar. Si esta variable de entorno no está definida, los mensajes se escriben en la salida de error estándar (stderr). El perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a este archivo y la autorización *WX sobre el directorio padre que contiene este archivo.

_EUV_SVC_DBG_MSG_LOGGING
Indica si se generan mensajes de depuración. El valor predeterminado es suprimir los mensajes de depuración. La anotación de mensajes de depuración no debe estar habilitada a menos que así lo solicite el personal de servicio de IBM, porque puede afectar gravemente al rendimiento. Los valores válidos son:

- 0 Suprimir mensajes de depuración
- 1 Escribir mensajes de depuración

_EUV_SVC_DBG

Subcomponentes y niveles de los mensajes de depuración. Para que los mensajes de depuración de un determinado subcomponente se anoten, el subcomponente debe estar incluido en la lista _EUV_SVC_DBG y el nivel del mensaje de depuración debe ser igual o mayor que el nivel especificado. Para especificar todos los subcomponentes, se utiliza un asterisco (*).

En la lista de subcomponentes, se escribe primero el nombre de un subcomponente, después un punto y luego el nivel de depuración. Cuando la lista consta de múltiples subcomponentes, las entradas se separan mediante comas. Por ejemplo, la lista _EUV_SVC_DBG=*.1,KRB_CCACHE.8 habilita el nivel de depuración 1 para todos los subcomponentes y el nivel de depuración 8 para el subcomponente KRB_CCACHE. Los subcomponentes que se pueden especificar son:

- KRB_API
- KRB_GENERAL
- KRB_CCACHE
- KRB_RCACHE
- KRB_CRYPTO
- KRB_GSSAPI
- KRB_KEYTAB
- KRB_LIB
- KRB_ASN1
- KRB_OS
- KRB_KDC
- KRB_KDB
- KRB_KUT

_EUV_SVC_DBG_FILENAME

Nombre totalmente calificado del archivo que recibirá los mensajes de depuración. Si esta variable de entorno no está definida, los mensajes de depuración se escriben en el archivo especificado en la variable _EUV_SVC_STDOUT_FILENAME. Si la variable _EUV_SVC_STDOUT_FILENAME no está especificada, los mensajes de depuración se escriben en la salida estándar (stdout). El perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a este archivo y la autorización *WX sobre el directorio padre que contiene este archivo.

KRB5_CONFIG

Uno o más nombres de archivos de configuración separados por dos puntos. El archivo de configuración predeterminado es /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf. El perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso que precede a estos archivos de configuración y la autorización *R sobre los archivos de configuración.

El archivo krb5.conf se divide en secciones cuyos nombres van entre corchetes. En las secciones, los valores de grupo van entre llaves. En V5R4 y en releases anteriores, puede utilizar los trígrafos correspondientes en lugar de los corchetes y las llaves, como se muestra en la tabla siguiente.

Carácter	Trígrafo
[(corchete izquierdo)	??(
] (corchete derecho)	??)
{ (llave izquierda)	??<
} (llave derecha)	??>

Sin embargo, por omisión, los sistemas que ejecutan i5/OS V6R1 están configurados para utilizar corchetes y llaves en lugar de los trígrafos. Si no utiliza un cliente de Kerberos Java, puede establecer que el sistema utilice trígrafos. Para utilizar trígrafos en el sistema, puede cambiar la primera letra del área de datos QUSRSYS/QKRBTRIGRA del valor predeterminado N a Y mediante el mandato CL Cambiar área de datos (CHGDTAARA).

KRB5CCNAME

Nombre predeterminado del archivo de memoria caché de credenciales, especificado con el formato tipo:nombre. Los tipos soportados son FILE y MEMORY. El valor predeterminado es utilizar la memoria caché de credenciales basada en FILE en el directorio /QIBM/UserData/OS400/NetworkAuthentication/creds. Si se utiliza el valor predeterminado, no hace falta configurar autorizaciones. Si se especifica un archivo de memoria caché de credenciales basada en FILE, el perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso. Debe tener la autorización *WX sobre el directorio padre la primera vez que se crea el archivo de memoria caché, además de la autorización *RW sobre el archivo de memoria caché. Si se va a suprimir el archivo de memoria caché, debe tener la autorización *OBJEXIST sobre el archivo de memoria caché.

KRB5_KTNAME

Nombre de tabla de claves predeterminado. Si no está especificada, se utiliza el archivo especificado en la entrada de configuración default_keytab_name del archivo de configuración. Si la entrada de configuración no está especificada, el archivo predeterminado es /QIBM/UserData/OS400/NetworkAuthentication/keytab/krb5.keytab. El perfil de usuario que está ejecutando actualmente debe tener la autorización *X sobre cada directorio de la vía de acceso. Si el archivo se va a crear, el perfil también debe tener la autorización *WX sobre el directorio padre. Si el archivo se va a actualizar, el perfil debe tener la autorización *RW sobre el archivo. Las autorizaciones específicas que se necesitan vienen documentadas en los mandatos de Qshell y en las API de la unidad ejecutable.

KRB5RCACHETYPE
Tipo de memoria caché de reproducción predeterminado. Toma como valor predeterminado: dfl.

KRB5RCACHENAME
Nombre de memoria caché de reproducción predeterminado. Si no está especificada, la unidad ejecutable Kerberos genera un nombre.

KRB5RCACHEDIR
Directorio de memoria caché de reproducción predeterminado. Toma como valor predeterminado: /QIBM/UserData/OS400/NetworkAuthentication/replay.

Casos prácticos: utilizar el servicio de autenticación de red en una red de Kerberos

Estos son casos prácticos habituales en los que se utiliza el servicio de autenticación de red para permitir que el sistema operativo i5/OS participe en una red de Kerberos.

Caso práctico: configurar un servidor Kerberos en i5/OS PASE

Estos son los objetivos, metas, prerrequisitos y pasos de configuración para configurar un servidor Kerberos.

Situación

Usted es un administrador que se encarga de gestionar la seguridad de la red de tamaño mediando de su empresa. Desea autenticar a los usuarios desde un sistema central. Ha decidido crear un servidor Kerberos que autentique a los usuarios ante los recursos de toda su empresa. Ha estado investigando las distintas maneras de implementar una solución Kerberos en la red. Sabe que el servidor Windows 2000 utiliza Kerberos para autenticar a los usuarios ante un dominio Windows; sin embargo, esta solución supondría costes adicionales para su pequeño presupuesto de tecnología de la información (TI). En lugar de utilizar un dominio Windows 2000 para autenticar a los usuarios, ha tomado la determinación de configurar un servidor Kerberos en el entorno System i de soluciones de aplicaciones portables (PASE) de i5/OS. i5/OS PASE proporciona un entorno de tiempo de ejecución integrado para las aplicaciones AIX. Le interesa servirse de la flexibilidad de i5/OS PASE para configurar su propio servidor Kerberos. Desea que el servidor Kerberos de i5/OS PASE autentique a los usuarios de la red que utilizan estaciones de trabajo Windows XP y Windows Vista.

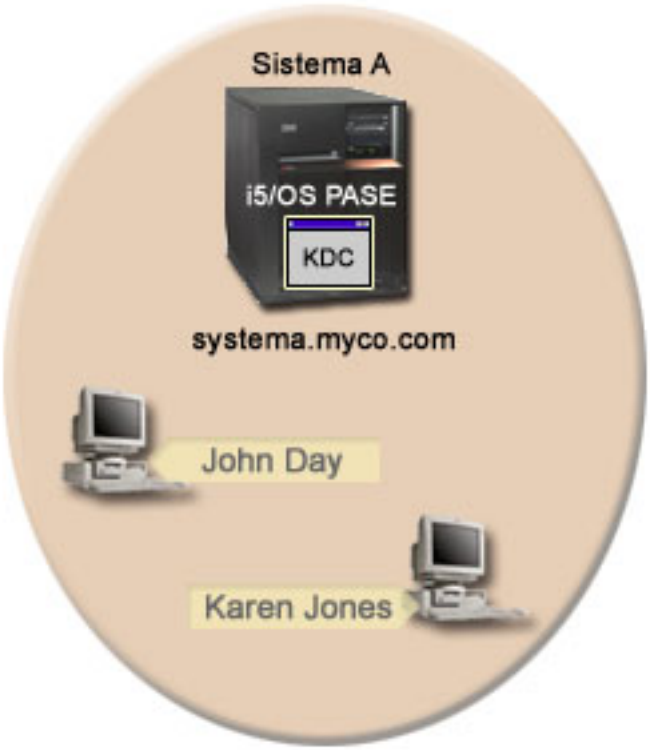
Objetivos

En este caso práctico, MyCo, Inc. se propone establecer un servidor Kerberos en i5/OS PASE para lograr los siguientes objetivos:

- Configurar un servidor Kerberos en el entorno i5/OS PASE
- Añadir los usuarios de la red a un servidor Kerberos
- Configurar las estaciones de trabajo que ejecutan los sistemas operativos Windows 2000, Windows XP y Windows Vista para que participen en el reino Kerberos configurado en i5/OS PASE
- Configurar el servicio de autenticación de red en el sistema A
- Probar la autenticación en la red

Detalles

La siguiente figura ilustra el entorno de red de este caso práctico.



Sistema A

- Funciona a modo de servidor Kerberos (kdc1.myco.com), que también se conoce como centro de distribución de claves (KDC), en la red.
- Ejecuta i5/OS Versión 5 Release 3 (V5R3) o posterior y tiene instaladas las siguientes opciones y programas bajo licencia:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - i5/OS PASE (5722-SS1 Opción 33 o 5761-SS1 Opción 33)
  - Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si ejecuta V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta V5R3
  - System i Access para Windows (5722-XE1 o 5761-XE1)
- Su nombre de host totalmente calificado es systema.myco.com.

PC clientes

- **Para todos los PC de este caso práctico:**
  - Ejecute los sistemas operativos Windows 2000, Windows XP y Windows Vista.
  - Tiene instaladas las herramientas de soporte de Windows 2000 (que proporcionan el mandato ksetup).
- **Para el PC del administrador:**
  - Tiene instalado System i Access para Windows (5722-XE1 o 5761-XE1).
  - Tiene instalado System i Navigator con los subcomponentes de seguridad y red.

Prerrequisitos y supuestos

Este caso práctico se centra en las tareas implicadas en la configuración de un servidor Kerberos en i5/OS PASE.

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado los programas bajo licencia necesarios, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.
2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. Las conexiones TCP/IP se han configurado y probado en la red.
4. Se utiliza un solo servidor DNS para la resolución de nombres de host en la red. No se utilizan tablas de hosts para la resolución de nombres de host.

   Nota: Si se utilizan tablas de hosts junto con la autenticación Kerberos, podrían producirse errores en la resolución de nombres u otros problemas. Si desea información más detallada sobre cómo funciona la resolución de nombres de host con la autenticación Kerberos, consulte el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.

Pasos de configuración

Para configurar un servidor Kerberos en i5/OS PASE y configurar asimismo el servicio de autenticación de red, lleve a cabo estos pasos.

Cumplimentar las hojas de trabajo de planificación

Para poder configurar el servidor Kerberos y el servicio de autenticación de red en i5/OS PASE, cumplimente estas hojas de trabajo de planificación.

Podrá proseguir con la configuración del servicio de autenticación de red cuando responda afirmativamente a todas las preguntas de la hoja de prerrequisitos.

Tabla 1. Hoja de trabajo de planificación de prerrequisitos

Preguntas	Respuestas
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1)?	Sí
¿Tiene instalados los siguientes programas y opciones bajo licencia en el sistema A?: • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • i5/OS PASE (5722-SS1 Opción 33 o 5761-SS1 Opción 33) • Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3 • System i Access para Windows (5722-XE1 o 5761-XE1)	Sí
¿Ha instalado Windows 2000, Windows XP o Windows Vista en todos los PC?	Sí
¿Tiene instaladas las herramientas de soporte de Windows 2000 (que proporcionan el mandato ksetup) en todos los PC?	Sí
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC del administrador?	Sí

Tabla 1. Hoja de trabajo de planificación de prerrequisitos (continuación)

Preguntas	Respuestas
¿Ha instalado System i Navigator en el PC del administrador? • ¿Está el subcomponente de seguridad de System i Navigator instalado en el PC del administrador? • ¿Está el subcomponente de red de System i Navigator instalado en el PC del administrador?	Sí Sí Sí
¿Ha instalado el último Service Pack de System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí
¿Tiene las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG? Necesitará estas autorizaciones especiales para utilizar el asistente de servicio de autenticación de red en este caso práctico.	Sí
¿Tiene configurado el DNS y tiene los nombres de host correctos para el producto System i y el servidor?	Sí
¿En qué sistema operativo desea configurar el servidor Kerberos? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 o posterior) 5. z/OS	i5/OS PASE
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

En este caso práctico, debe especificar varias contraseñas distintas. La siguiente hoja de trabajo de planificación facilita una lista de las contraseñas que deberá utilizar en este caso práctico. Consulte esta tabla cuando lleve a cabo los pasos de configuración para poner a punto el servidor Kerberos en i5/OS PASE.

Tabla 2. Hoja de trabajo de planificación de contraseñas

Entidad	Contraseña
Administrador de i5/OS PASE: admin/admin **Nota:** En i5/OS PASE se especifica `admin/admin` como nombre de usuario predeterminado para el administrador.	secret
Maestro de base de datos i5/OS PASE	pasepwd
Estaciones de trabajo Windows: • pc1.myco.com (PC de John Day) • pc2.myco.com (PC de Karen Jones)	secret1 secret2
Sujetos principales de usuario Kerberos: • day@MYCO.COM • jones@MYCO.COM	123day 123jones
Sujeto principal de servicio de i5/OS para el sistema A: krbsvr400/systema.myco.com@MYCO.COM	systema123

La siguiente hoja de trabajo de planificación ilustra el tipo de información que necesita antes de empezar a configurar el servidor Kerberos en i5/OS PASE y el servicio de autenticación de red. Podrá proseguir con la configuración del servidor Kerberos en i5/OS PASE cuando haya respondido a todas las preguntas

de la hoja de trabajo de prerrequisitos y de la hora de trabajo de planificación de contraseñas.

Tabla 3. Hoja de trabajo de planificación para configurar un servidor Kerberos en i5/OS PASE y para configurar el servicio de autenticación de red

Preguntas	Respuestas
¿Qué nombre tiene el reino Kerberos predeterminado?	MYCO.COM
¿Está este reino predeterminado situado en Microsoft Active Directory?	No
¿Qué servidor Kerberos (que también se conoce como centro de distribución de claves (KDC)) utiliza para este reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	**KDC:** kdc1.myco.com **Puerto:** 88 **Nota:** Este es el puerto predeterminado del servidor Kerberos.
¿Desea configurar un servidor de contraseñas para este reino predeterminado?	No **Nota:** Actualmente, los servidores de contraseñas no están soportados en i5/OS PASE ni en AIX.
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	Autenticación de Kerberos de i5/OS
¿Desea crear un archivo por lotes para automatizar la adición de sujetos principales de servicio a Microsoft Active Directory?	No aplicable
¿Cuál es el nombre de usuario predeterminado del administrador de i5/OS PASE? ¿Qué contraseña desea especificar para el administrador de i5/OS PASE?	Nombre de usuario: admin/admin Contraseña: secret
¿Cuál es el convenio de denominación de los sujetos principales que representan a los usuarios de la red?	Los sujetos principales que representan a los usuarios constarán del apellido escrito con minúsculas seguido del nombre del reino escrito con mayúsculas
Cuáles son los nombres de sujeto principal de usuario Kerberos de estos usuarios: • John Day • Karen Jones	day@MYCO.COM jones@MYCO.COM
Cuáles son los nombres de perfil de usuario de i5/OS de estos usuarios: • John Day • Karen Jones	JOHND KARENJ
Cuáles son los nombres de usuario de Windows 2000 de estos usuarios: • John Day • Karen Jones	johnday karenjones
Cuáles son los nombres de host de estas estaciones de trabajo Windows 2000: • PC de John Day • PC de Karen Jones	pc1.myco.com pc2.myco.com

Tabla 3. Hoja de trabajo de planificación para configurar un servidor Kerberos en i5/OS PASE y para configurar el servicio de autenticación de red (continuación)

Preguntas	Respuestas
¿Cuál es el nombre del sujeto principal de servicio i5/OS para el sistema A?	krbsvr400/systema.myco.com@MYCO.COM **Nota:** El nombre de este sujeto principal sólo tiene valor de ejemplo. En la configuración, especifique el nombre de host y el dominio de i5/OS como nombre del sujeto principal de servicio.

Configurar un servidor Kerberos en i5/OS PASE

Para configurar un servidor Kerberos en i5/OS PASE en el sistema A, utilice la información de las hojas de trabajo de planificación.

Siga estos pasos para configurar un servidor Kerberos en i5/OS PASE:

1. En una interfaz basada en caracteres, teclee `call QP2TERM`. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, especifique `config.krb5 -S -d myco.com -r MYCO.COM`, donde `-d` es el DNS de la red y `-r` es el nombre de reino. (En este ejemplo, myco.com es el nombre de DNS y MYCO.COM es el nombre de reino). Este mandato actualiza el archivo krb5.config con el nombre de dominio y el reino del servidor Kerberos, crea la base de datos Kerberos en el sistema de archivos integrado y configura el servidor Kerberos en i5/OS PASE. Se le pedirá que añada las siguientes contraseñas:
   - Contraseña maestra de base de datos: `pasepwd`
   - Contraseña del sujeto principal admin/admin: `secret`
4. Pulse F3 (Salir) para salir del entorno PASE.

Cambiar los valores de cifrado en el servidor Kerberos de i5/OS PASE

Para trabajar con las estaciones de trabajo Windows, debe cambiar los valores de cifrado predeterminados del servidor Kerberos para que los clientes se puedan autenticar ante el servidor Kerberos de i5/OS PASE.

Para cambiar los valores predeterminados de cifrado, tiene que editar el archivo kdc.conf situado en el directorio /etc/krb5 siguiendo estos pasos:

1. En una interfaz basada en caracteres, escriba `edtf '/var/krb5/krb5kdc/kdc.conf'` para acceder al archivo kdc.conf.
2. Cambie las siguientes líneas del archivo kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   para que sean

```
supported_enctypes = des-cbc-crc:normal dec-cbc-md5:normal
```

Detener y reiniciar el servidor Kerberos en i5/OS PASE

Debe detener y reiniciar el servidor Kerberos en i5/OS PASE para actualizar los valores de cifrado que acaba de cambiar.

Lleve a cabo los pasos siguientes para detener y reiniciar el servidor Kerberos:

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.

2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `stop.krb5`. Este mandato detiene el servidor Kerberos.
4. En la línea de mandatos, escriba `start.krb5`. Este mandato inicia el servidor Kerberos.

Crear sujetos principales de host para estaciones de trabajo Windows 2000, Windows XP y Windows Vista

Debe crear los sujetos principales de host que Kerberos utiliza para autenticar los usuarios de los PC.

Si ya se encuentra en i5/OS PASE, ignore los pasos 1 y 2. Para crear los sujetos principales de host para estas estaciones de trabajo, siga estos pasos:

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `kadmin -p admin/admin` y pulse Intro.
4. Inicie sesión con la contraseña de administrador. Por ejemplo, `secret`.
5. En el indicador de kadmin, escriba `addprinc -pw secret1 host/pc1.myco.com`. Así se crea un sujeto principal de host para el PC de John Day.
6. En el indicador de kadmin, escriba `addprinc -pw secret2 host/pc2.myco.com`. Así se crea un sujeto principal de host para el PC de Karen Jones.
7. Escriba `quit` para salir de la interfaz kadmin.

Crear sujetos principales de usuario en el servidor Kerberos

Para que los usuarios se autentiquen ante los servicios de la red, debe añadirlos al servidor Kerberos como sujetos principales.

Sujeto principal es en Kerberos el término que corresponde al nombre y la contraseña de un usuario. Los sujetos principales se almacenan en el servidor Kerberos y sirven para validar a los usuarios de la red. Siga estos pasos para crear sujetos principales de usuario:

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `kadmin -p admin/admin` y pulse Intro.
4. Inicie sesión con la contraseña de administrador. Por ejemplo, `secret`.
5. En el indicador de kadmin, escriba `addprinc -pw 123day day`.

Después de completar estos pasos, recibirá este mensaje:

```
Sujeto principal "day@MYCO.COM" creado.
```

Así se crea el sujeto principal de usuario para John Day.

Repita estos pasos para Karen Jones, pero ahora especifique `jones` para el nombre de sujeto principal y `123jones` para la contraseña.

Añadir el sujeto principal de servicio del sistema A al servidor Kerberos

Para que las interfaces i5/OS acepte los tickets Kerberos, debe añadirlos al servidor Kerberos como sujetos principales.

Siga estos pasos para añadir el sujeto principal de servicio. Si ya se encuentra en el entorno kadmin, ignore los pasos 1 a 4.

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `kadmin -p admin/admin` y pulse Intro.
4. Inicie sesión con la contraseña de administrador. Por ejemplo, `secret`.
5. En el indicador de kadmin, escriba `addprinc -pw systema123 krbsvr400/systema.myco.com`. Recibirá este mensaje:

   ```
   Sujeto principal "krbsvr400/systema.myco.com@MYCO.COM" creado.
   ```
6. Escriba `quit` para salir de la interfaz kadmin y pulse F3 (Salir) para salir del entorno PASE.

Configurar estaciones de trabajo Windows 2000, Windows XP y Windows Vista

Este paso es opcional cuando se configura un servidor Kerberos en i5/OS PASE. Si se propone crear un entorno de inicio de sesión único después de configurar el servidor Kerberos, tendrá que llevar a cabo este paso. En caso contrario, vaya directamente al paso 9 (Configurar el servicio de autenticación de red).

Configurar las estaciones de trabajo de cliente como parte de un grupo de trabajo estableciendo el reino Kerberos y el servidor Kerberos en la estación de trabajo. También tendrá que fijar una contraseña para que se asocie a la estación de trabajo.

Para configurar las estaciones de trabajo, siga estos pasos:

1. En un indicador de mandato de la estación de trabajo Windows 2000, escriba:

   ```
   C:> ksetup /setdomain MYCO.COM
   C:> ksetup /addkdc MYCO.COM kdc1.myco.com
   ```

2. Establezca la contraseña de la cuenta de la máquina local escribiendo lo siguiente en el indicador de mandatos de la estación de trabajo Windows 2000:

   ```
   C:> ksetup /setmachpassword secret1
   ```

3. Correlacione el sujeto principal de usuario de John Day (day@MYCO.COM) con su nombre de usuario de Windows 2000 (johnday). En el indicador de mandatos de la estación de trabajo Windows 2000, escriba:

   ```
   C:> ksetup /mapuser day@MYCO.COM johnday
   ```

4. Para verificar que el sujeto principal de usuario Kerberos de John Day se correlaciona con su nombre de usuario de Windows 2000, escriba lo siguiente en el indicador de mandatos de la estación de trabajo Windows 2000:

   ```
   C:> ksetup
   ```

   y visualice los resultados.
5. Reinicie el PC para que los cambios entren en vigor.
6. Repita estos pasos para la estación de trabajo de Karen Jones, pero ahora especifique la siguiente información:
   - Contraseña de la cuenta de la máquina local: `secret2`
   - Sujeto principal de usuario Kerberos: `jones@MYCO.COM`
   - Nombre de usuario de Windows 2000: `karenjones`

Conceptos relacionados

Caso práctico: crear un entorno de prueba de inicio de sesión único

Configurar el servicio de autenticación de red

Para configurar el servicio de autenticación de red, siga estos pasos.

1. En System i Navigator, expanda **Sistema A** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración.

   Nota: Tras configurar el servicio de autenticación de red, esta opción indicará **Reconfigurar**.
3. En la página de bienvenida encontrará información sobre los objetos que crea el asistente. Pulse **Siguiente**.
4. En la página Especificar información de reino, escriba `MYCO.COM` en el campo **Reino predeterminado**. Pulse **Siguiente**.
5. En la página Especificar información de KDC, escriba `kdc1.myco.com` para el servidor Kerberos en el campo **KDC** y teclee `88` en el campo **Puerto**. Pulse **Siguiente**.
6. En la página Especificar información de contraseña, seleccione **No**. Pulse **Siguiente**.
7. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. Pulse **Siguiente**.
8. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña, confírmela y pulse **Siguiente**, por ejemplo, `systema123`. Esta contraseña se utilizará cuando se añada el sistema A al servidor Kerberos.
9. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.

Crear un directorio inicial para los usuarios en el sistema A

Cada usuario que se conecte al sistema operativo i5/OS y a las aplicaciones del i5/OS necesitará un directorio en el directorio /home (directorio inicial). Este directorio contiene el nombre de la memoria caché de credenciales Kerberos del usuario.

Para crear un directorio inicial para los usuarios del sistema A, siga estos pasos:

1. En la línea de mandatos de i5/OS, escriba `CRTDIR '/home/perfil usuario'`, siendo `perfil usuario` el nombre del perfil i5/OS del usuario, por ejemplo, `CRTDIR '/home/JOHND'` corresponde al usuario John Day.
2. Repita este mandato para el usuario Karen Jones, pero ahora especifique su perfil de usuario i5/OS, que es `KARENJ`.

Probar el servicio de autenticación de red

Para probar la configuración del servicio de autenticación de red, solicite un ticket de otorgamiento de tickets para el sujeto principal de i5/OS y los demás sujetos principales de la red.

Nota: Antes de llevar a cabo esta prueba, asegúrese de que ha creado un directorio inicial (home) para su perfil de usuario i5/OS.

Para probar la configuración del servicio de autenticación de red, siga estos pasos:

1. En una línea de mandatos del intérprete Qshell, escriba `QSH` para iniciar el intérprete Qshell.
2. Entre `keytab list` para visualizar una lista de los sujetos principales registrados en el archivo de tabla de claves. Deben visualizarse los siguientes resultados:

```
Sujeto principal: krbsvr400/systema.myco.com@MYCO.COM
  Versión de clave: 2
  Tipo de clave: DES de 56 bits mediante derivación de clave
  Indicación de la hora de la entrada: 200X/05/29-11:02:58
```

3. Escriba `kinit -k krbsvr400/systema.myco.com@MYCO.COM` para solicitar un ticket de otorgamiento de tickets al servidor Kerberos. Este mandato verifica que el sistema está debidamente configurado y que

la contraseña del archivo de tabla de claves concuerda con la almacenada en el servidor Kerberos. Si la verificación es satisfactoria, el mandato QSH mostrará que no hay errores.

4. Escriba `klist` para verificar que el sujeto principal predeterminado es krbsvr400/systema.myco.com@MYCO.COM. Este mandato visualiza el contenido de una memoria caché de credenciales Kerberos y verifica que se ha creado un ticket válido para el sujeto principal de servicio de i5/OS y que se ha colocado en la memoria caché de credenciales del sistema.

```
 Memoria caché de tickets: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Sujeto principal predeterminado: krbsvr400/systema.myco.com@MYCO.COM

Servidor: krbtgt/MYCO.COM@MYCO.COM
  Válido del 200X/06/09-12:08:45 al 20XX/11/05-03:08:45
$
```

Ya ha terminado de realizar los pasos necesarios para configurar el sistema para que funcione a modo de servidor Kerberos y ahora puede utilizar Kerberos para autenticar a los usuarios del reino MYCO.COM.

Caso práctico: configurar el servicio de autenticación de red

Estos son los prerrequisitos y objetivos para añadir el servicio de autenticación en la red.

Situación

Usted es un administrador de red que se encarga de gestionar la red del departamento de recepción de pedidos de su empresa. Recientemente ha añadido un producto System i a su red, en el que alojará varias aplicaciones para su departamento. En su red, gestiona a los usuarios con Microsoft Active Directory en un servidor Microsoft Windows 2000. Actualmente, todos sus usuarios tienen estaciones de trabajo que ejecutan el sistema operativo Microsoft Windows 2000. Tiene sus propias aplicaciones habilitadas para Kerberos que utilizan las API de servicios de seguridad genéricos (GSS).

Las ventajas de este caso práctico son:

- Simplifica el proceso de autenticación de los usuarios
- Reduce la actividad adicional que supone gestionar el acceso a los sistemas de la red
- Minimiza la amenaza de robo de contraseñas

Objetivos

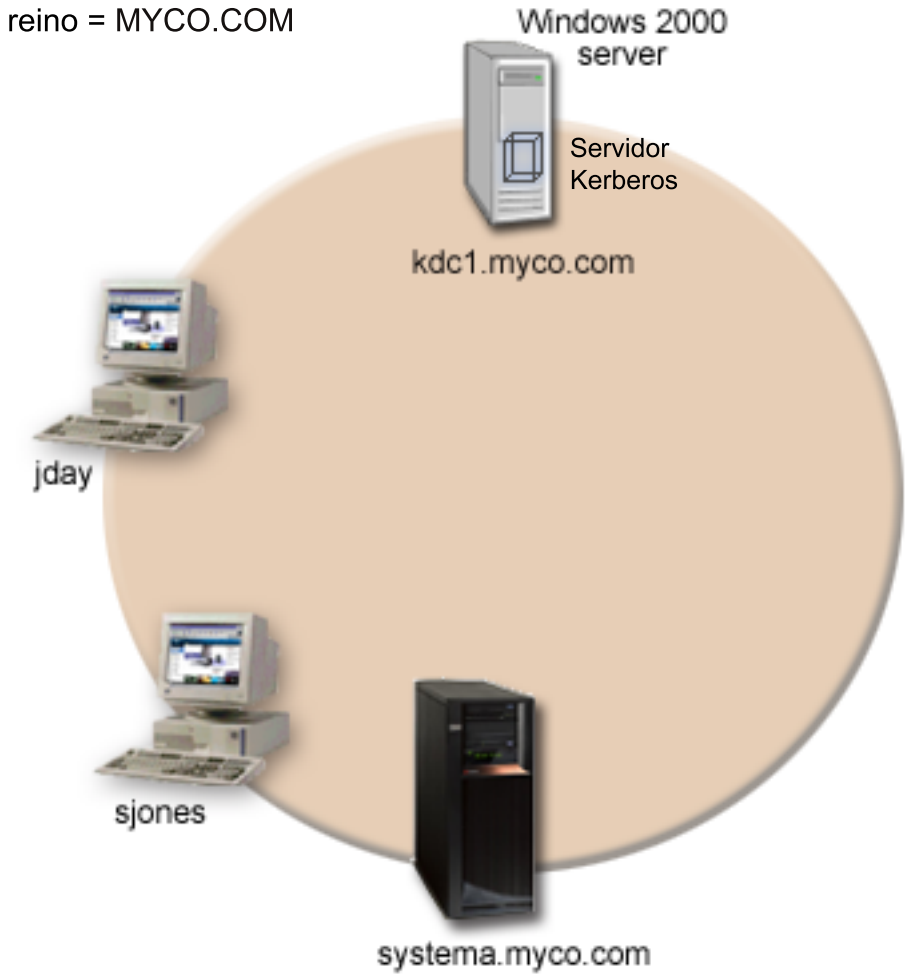
En este caso práctico, la empresa MyCo, Inc. se propone añadir un producto System i a un reino existente en el que un servidor Windows 2000 funciona como servidor Kerberos. La plataforma System i contiene varias aplicaciones críticas del negocio a las que deben acceder unos usuarios determinados. Para poder acceder a estas aplicaciones, los usuarios se tienen que autenticar ante el servidor Kerberos.

Los objetivos de este caso práctico son los siguientes:

- Permitir que la plataforma System i participe junto con un servidor Kerberos existente
- Proporcionar nombres de sujeto principal y nombres de usuario para la red
- Permitir que los usuarios de Kerberos cambien sus propias contraseñas en el servidor Kerberos

Detalles

La siguiente figura ilustra las características de MyCo en la red.



Sistema A

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta V5R3
- El nombre de sujeto principal del sistema A es krbsvr400/systema.myco.com@MYCO.COM.

Servidor **Windows 2000**

- Funciona como servidor Kerberos en el reino MYCO.COM.
- El nombre de host totalmente calificado del servidor Kerberos es kdc1.myco.com.

PC clientes

- Ejecutan Windows 2000.
- En el PC que se utiliza para administrar el servicio de autenticación de red se han instalado los siguientes productos:
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - System i Navigator y los subcomponentes de seguridad y red

Prerrequisitos y supuestos

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado los programas bajo licencia necesarios, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.

   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.
2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en cada uno de estos servidores.
4. Se utiliza un solo servidor DNS para la resolución de nombres de host en la red. No se utilizan tablas de hosts para la resolución de nombres de host.

   Nota: Si se utilizan tablas de hosts junto con la autenticación Kerberos, podrían producirse errores en la resolución de nombres u otros problemas. Si desea información más detallada sobre cómo funciona la resolución de nombres de host con la autenticación Kerberos, consulte el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.

Pasos de configuración

Para configurar el servicio de autenticación de red en el sistema, lleve a cabo los pasos siguientes.

Cumplimentar las hojas de trabajo de planificación

Para poder configurar el servicio de autenticación de red, cumplimente estas hojas de trabajo de planificación.

Podrá proseguir con la configuración del servicio de autenticación de red cuando responda afirmativamente a todas las preguntas de la hoja de trabajo de prerrequisitos.

Tabla 4. Hoja de trabajo de prerrequisitos

Preguntas	**Respuestas**
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1)?	Sí
¿Tiene instalados los siguientes programas bajo licencia en el sistema A?: • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30) • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3	Sí
¿Ha instalado Windows 2000 en los PC?	Sí
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC del administrador?	Sí

Tabla 4. Hoja de trabajo de prerrequisitos (continuación)

Preguntas	Respuestas
¿Ha instalado System i Navigator en el PC del administrador? • ¿Está el subcomponente de seguridad de System i Navigator instalado en el PC del administrador? • ¿Está el subcomponente de red de System i Navigator instalado en el PC del administrador?	Sí Sí Sí
¿Ha instalado el último Service Pack de System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí
¿Tiene las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG?	Sí
¿Ha instalado alguno de los siguientes sistemas operativos en el sistema seguro que funcionará como servidor Kerberos? Si es así, ¿cuál de ellos? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 o posterior) 5. z/OS	Sí, Windows 2000 Server
¿Están todos los PC de la red configurados en un dominio Windows 2000? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

Tabla 5. Hoja de trabajo de planificación del servicio de autenticación de red

Preguntas	Respuestas
¿Cuál es el nombre del reino Kerberos predeterminado al que pertenecerá el sistema? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	MYCO.COM
¿Está utilizando Microsoft Active Directory?	Sí
¿Cuál es el servidor Kerberos del reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	**KDC:** kdc1.myco.com **Puerto:** 88 **Nota:** Este es el puerto predeterminado del servidor Kerberos.
¿Desea configurar un servidor de contraseñas para este reino predeterminado? Si es así, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este servidor Kerberos? ¿En qué puerto está a la escucha el servidor de contraseñas?	Sí **Servidor de contraseñas:** kdc1.myco.com **Puerto:** 464 **Nota:** Este es el puerto predeterminado del servidor de contraseñas.

Tabla 5. Hoja de trabajo de planificación del servicio de autenticación de red (continuación)

Preguntas	Respuestas
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	Autenticación de Kerberos de i5/OS
¿Qué contraseña desea utilizar para los sujetos principales de servicio de i5/OS?	systema123
¿Desea crear un archivo por lotes para automatizar la adición de sujetos principales de servicio a Microsoft Active Directory?	Sí
¿Qué nombres de perfil de usuario i5/OS tienen John Day y Sharon Jones?	JOHND SHARONJ

Configurar el servicio de autenticación de red en el sistema A

Para configurar el servicio de autenticación de red, siga estos pasos.

1. En System i Navigator, expanda **Sistema A** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración.

   Nota: Tras configurar el servicio de autenticación de red, esta opción indicará **Reconfigurar**.
3. En la página de bienvenida encontrará información sobre los objetos que crea el asistente. Pulse **Siguiente**.
4. En la página Especificar información de reino, escriba `MYCO.COM` en el campo **Reino predeterminado** y seleccione **Se utiliza Microsoft Active Directory para la autenticación Kerberos**. Pulse **Siguiente**.
5. En la página Especificar información de KDC, escriba `kdc1.myco.com` para el servidor Kerberos en el campo **KDC** y teclee `88` en el campo **Puerto**. Pulse **Siguiente**.
6. En la página Especificar información de contraseña, seleccione **Sí**. Entre `kdc1.myco.com` en el campo **Servidor de contraseñas** y `464` en el campo **Puerto**. Pulse **Siguiente**.
7. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. Pulse **Siguiente**.
8. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña y confírmela, por ejemplo, `systema123`. Esta contraseña se utilizará cuando se añada el sistema A al servidor Kerberos. Pulse **Siguiente**.
9. Opcional: En la página Crear archivo por lotes, seleccione **Sí** para que se cree este archivo y especifique la siguiente información:
   - **Archivo por lotes:** añada el texto `systema` al final del nombre del archivo por lotes predeterminado, por ejemplo, `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`
   - Seleccione **Incluir contraseña**. Así se asegura de que todas las contraseñas asociadas al sujeto principal de servicio de i5/OS se incluyen en el archivo por lotes. Es importante que se fije en que las contraseñas se visualizan en texto sin cifrar y que pueden leerlas todas las personas que tengan acceso de lectura al archivo por lotes. Por ello, le recomendamos que suprima el archivo por lotes del servidor Kerberos y de su PC inmediatamente después de haberlo utilizado.

     Nota: Por otra parte, los sujetos principales de servicio generados por el asistente también se pueden añadir manualmente al servidor Kerberos. Si desea saber cómo se añade manualmente el sujeto principal de servicio de i5/OS al servidor Kerberos, consulte el tema "Añadir sujetos principales i5/OS al servidor Kerberos" en la página 101.

10. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.

Añadir el sujeto principal del sistema A al servidor Kerberos

Puede añadir manualmente el sujeto principal de servicio de i5/OS al servidor Kerberos. Tal como se ilustra en este caso práctico, también puede utilizar el archivo por lotes creado en el paso 2 para añadir el sujeto principal.

Para utilizar el archivo por lotes, debe utilizar el protocolo de transferencia de archivos (FTP) para copiarlo en el servidor Kerberos y ejecutarlo. Para añadir el sujeto principal al servidor Kerberos mediante el archivo por lotes, siga estos pasos:

1. Transmita por FTP el archivo por lotes creado por el asistente
   a. En la estación de trabajo Windows 2000 empleada por el administrador para configurar el servicio de autenticación de red, abra un indicador de mandatos y teclee `ftp kdc1.myco.com`. Así se iniciará una sesión FTP en su PC. Se le pedirá el nombre de usuario y la contraseña de administrador.
   b. En el indicador FTP, teclee `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Pulse Intro. Debe recibir el mensaje `Directorio local es ahora C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
   c. En el indicador FTP, teclee `binary`. Esto indica que el archivo que se transferirá es binario.
   d. En el indicador FTP, teclee `cd \`*`midirectorio`*, siendo *midirectorio* un directorio de kdc1.myco.com.
   e. En el indicador FTP, teclee `put NASConfigsystema.bat`. Debe recibir el mensaje: `226 Transferencia completada`.
2. Ejecute el archivo por lotes en kdc1.myco.com
   a. En el servidor Windows 2000, abra la carpeta en la que ha transferido los archivos por lotes.
   b. Localice el archivo NASConfigsystema.bat y púlselo dos veces para ejecutarlo.
   c. Una vez ejecutado el archivo, verifique que el sujeto principal de i5/OS se ha añadido al servidor Kerberos; para ello, siga estos pasos:
      1) En el servidor Windows 2000, expanda **Inicio** → **Programas** → **Herramientas administrativas** → **Usuarios y equipos de Active Directory** → **Usuarios**.
      2) Verifique que el sistema tiene una cuenta de usuario seleccionando el dominio Windows pertinente.

         Nota: Este dominio Windows debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.
      3) En la lista de usuarios visualizada, localice **systema_1_krbsvr400**. Es la cuenta de usuario generada para el nombre de sujeto principal de i5/OS.
      4) **Opcional:** acceda a las propiedades de los usuarios de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**.

         Nota: Este paso opcional permite que su sistema delegue o reenvíe las credenciales de un usuario a otros sistemas. Como resultado, el sujeto principal de servicio de i5/OS podrá acceder a los servicios en múltiples sistemas en nombre del usuario. Esto resulta útil en una red multinivel.

Crear un directorio inicial para los usuarios en el sistema A

Cada usuario que se conecte al i5/OS y a las aplicaciones del i5/OS necesitará un directorio en el directorio /home (directorio inicial). Este directorio contiene el nombre de la memoria caché de credenciales Kerberos del usuario.

Para crear un directorio inicial para un usuario, siga estos pasos:

1. En la línea de mandatos de i5/OS, escriba: `CRTDIR '/home/perfil usuario'`, siendo `perfil usuario` el nombre del perfil i5/OS del usuario. Por ejemplo, `CRTDIR '/home/JOHND'` corresponde al usuario John Day.
2. Repita este mandato para el usuario Sharon Jones, pero ahora especifique su perfil de usuario i5/OS, que es `SHARONJ`.

Probar el servicio de autenticación de red en el sistema A

Para verificar que ha configurado correctamente el servicio de autenticación de red, solicite un ticket de otorgamiento de tickets para un sujeto principal del sistema A.

Para probar el servicio de autenticación de red, siga estos pasos:

1. En una línea de mandatos del intérprete Qshell, escriba `QSH` para iniciar el intérprete Qshell.
2. Entre `keytab list` para visualizar una lista de los sujetos principales registrados en el archivo de tabla de claves. Deben visualizarse los siguientes resultados:

```
Sujeto principal: krbsvr400/systema.myc.com@MYCO.COM
  Versión de clave: 2
  Tipo de clave: DES de 56 bits mediante derivación de clave
  Indicación de la hora de la entrada: 200X/05/29-11:02:58
```

3. Escriba `kinit -k krbsvr400/systema.myco.com@MYCO.COM` para solicitar un ticket de otorgamiento de tickets al servidor Kerberos. Este mandato verifica que el sistema está debidamente configurado y que la contraseña del archivo de tabla de claves concuerda con la almacenada en el servidor Kerberos. Si la verificación es satisfactoria, el mandato QSH mostrará que no hay errores.
4. Escriba `klist` para verificar que el sujeto principal predeterminado es krbsvr400/systema.myco.com@MYCO.COM. Este mandato visualiza el contenido de una memoria caché de credenciales Kerberos y verifica que se ha creado un ticket válido para el sujeto principal de servicio de i5/OS y que se ha colocado en la memoria caché de credenciales del sistema.

```
 Memoria caché de tickets: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Sujeto principal predeterminado: krbsvr400/systema.myco.com@MYCO.COM

Servidor: krbtgt/MYCO.COM@MYCO.COM
  Válido del 200X/06/09-12:08:45 al 20XX/11/05-03:08:45
$
```

Ya ha terminado las tareas necesarias para configurar el servicio de autenticación de red en el sistema A.

Caso práctico: configurar la confianza entre distintos reinos

Estos son los prerrequisitos y objetivos para configurar la confianza entre distintos reinos en la red.

Situación

Usted es administrador de la seguridad de una gran empresa de venta al por mayor. Se encarga de gestionar la seguridad de los sistemas que utilizan los empleados del departamento de recepción de pedidos y del departamento de envíos. Ha configurado un servidor Kerberos para el departamento de recepción de pedidos. Ha configurado el servicio de autenticación de red en el entorno System i de dicho departamento para que señale hacia ese servidor Kerberos. El departamento de envíos consta de un producto System i que tiene un servidor Kerberos configurado en i5/OS PASE. También ha configurado el servicio de autenticación de red en este producto System i para que señale hacia el servidor Kerberos de i5/OS PASE.

Dado que los usuarios de ambos reinos tienen que utilizar servicios almacenados en los sistemas situados en cada departamento, le interesa que los dos servidores Kerberos de cada departamento autentiquen a los usuarios sea cual sea el reino Kerberos al que pertenecen.

Objetivos

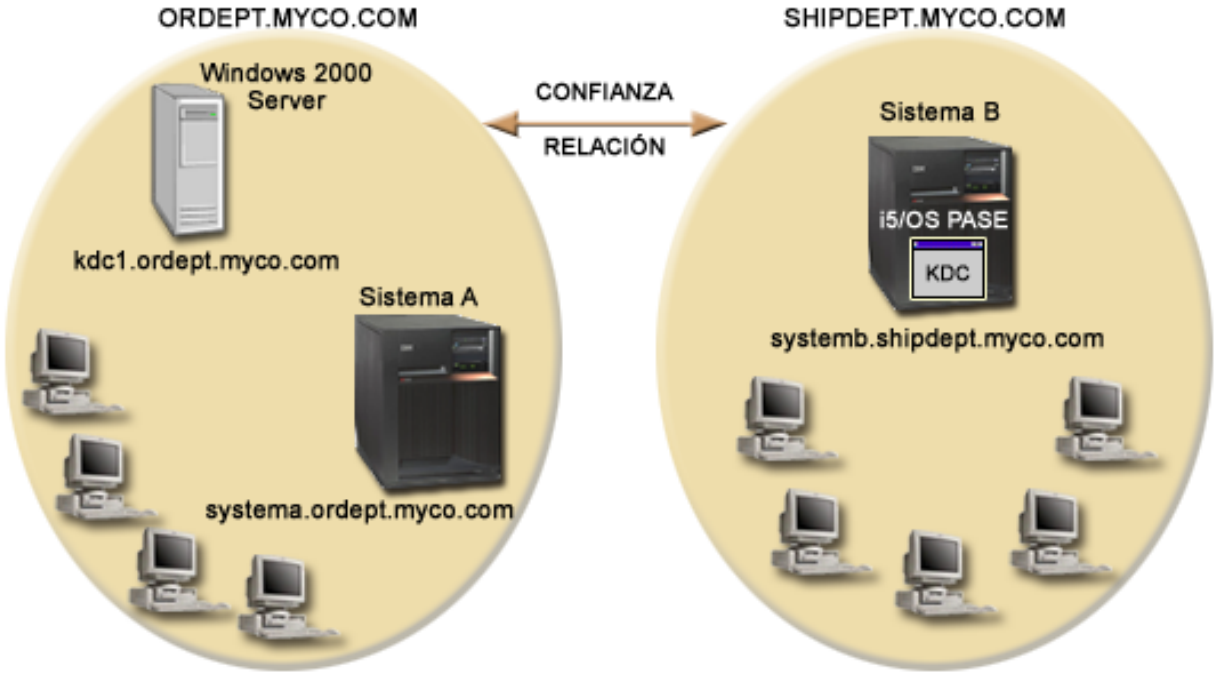
En este caso práctico, la empresa MyCo, Inc., se propone establecer una relación de confianza entre dos reinos Kerberos existentes. Uno de los reinos consta de un servidor Windows 2000 que funciona como servidor Kerberos del departamento de recepción de pedidos. Este servidor autentica a los usuarios de es departamento ante los servicios situados en una plataforma System i. El otro reino consta de un servidor Kerberos configurado en i5/OS PASE en una plataforma System i, que presta servicios a los usuarios del departamento de envíos. Los usuarios deberán autenticarse ante los servicios de los dos departamentos.

Los objetivos de este caso práctico son los siguientes:

- Facilitar a los clientes y hosts de cada red acceso a la otra red
- Simplificar el proceso de autenticación entre redes
- Permitir la delegación de tickets para los usuarios y servicios de ambas redes

Detalles

En este apartado se proporciona una descripción detallada del entorno correspondiente a este caso práctico, y se incluye una figura que muestra la topología, los elementos importantes del entorno y la relación que hay entre ellos.



Departamento de recepción de pedidos

Sistema A

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3

- Tiene configurado el servicio de autenticación de red para participar en el reino ORDEPT.MYCO.COM. El sujeto principal de i5/OS, krbsrv400/systema.ordept.myco.com@ORDEPT.MYCO.COM, se ha añadido al dominio Windows 2000.
- El nombre de host totalmente calificado del sistema A es systema.ordept.myco.com.

Servidor **Windows 2000**
- Funciona como servidor Kerberos en el reino ORDEPT.MYCO.COM.
- El nombre de host DNS es kdc1.ordept.myco.com.
- Cada usuario del departamento de pedidos se ha definido en Microsoft Active Directory en el servidor Windows 2000 con un nombre de sujeto principal y una contraseña.

PC clientes
- Ejecutan el sistema operativo Windows 2000.
- En el PC que se utiliza para administrar el servicio de autenticación de red se han instalado los siguientes productos:
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - System i Navigator y los siguientes subcomponentes:
    - Seguridad
    - Red

Departamento de envíos

Sistema B
- Ejecuta i5/OS V5R3 con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS PASE (5722-SS1 Opción 33)
  - Cryptographic Access Provider (5722-AC3)
  - System i Access para Windows (5722-XE1)
- Tiene configurado un servidor Kerberos de i5/OS PASE cuyo reino es SHIPDEPT.MYCO.COM.
- Tiene configurado el servicio de autenticación de red para participar en el reino SHIPDEPT.MYCO.COM. El sujeto principal de i5/OS, krbsrv400/systemb.shipdept.myco.com@SHIPDEPT.MYCO.COM, se ha añadido al servidor Kerberos de i5/OS PASE.
- El sistema B y el servidor Kerberos de i5/OS PASE comparten el nombre de host totalmente calificado systemb.shipdept.myco.com.
- Cada usuario del departamento de envíos se ha definido en el servidor Kerberos de i5/OS PASE con un nombre de sujeto principal y una contraseña.

PC clientes
- Ejecutan el sistema operativo Windows 2000.
- En el PC que se utiliza para administrar el servicio de autenticación de red se han instalado los siguientes productos:
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - System i Navigator y los siguientes subcomponentes:
    - Seguridad
    - Red

Prerrequisitos y supuestos

En este caso práctico, hemos hecho las siguientes suposiciones para centrarnos en las tareas que implican establecer una relación de confianza entre dos reinos Kerberos que ya existían.

Prerrequisitos del sistema A

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado los programas bajo licencia necesarios, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.
2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en el sistema A.
4. El servicio de autenticación de red se ha configurado y probado.
5. Se utiliza un solo servidor DNS para la resolución de nombres de host en la red. No se utilizan tablas de hosts para la resolución de nombres de host.

   Nota: Si se utilizan tablas de hosts junto con la autenticación Kerberos, podrían producirse errores en la resolución de nombres u otros problemas. Si desea información más detallada sobre cómo funciona la resolución de nombres de host con la autenticación Kerberos, consulte el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.

Prerrequisitos del sistema B

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado los programas bajo licencia necesarios, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.
2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en el sistema.
4. El servicio de autenticación de red se ha configurado y probado.

Prerrequisitos del servidor **Windows 2000**

1. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
2. El protocolo TCP/IP se ha configurado y probado en el servidor.
3. Microsoft Active Directory se ha configurado y probado.
4. Cada usuario del departamento de pedidos se ha definido en Microsoft Active Directory con un nombre de sujeto principal y una contraseña.

Pasos de configuración

Para establecer una relación de confianza entre dos reinos, siga estos pasos.

Cumplimentar las hojas de trabajo de planificación

Para poder configurar la confianza entre reinos, cumplimente estas hojas de trabajo de planificación.

Podrá proseguir con la configuración de la confianza entre reinos cuando responda afirmativamente a todas las preguntas de la hoja de trabajo de prerrequisitos.

Tabla 6. Hoja de trabajo de planificación de prerrequisitos

Preguntas	Respuestas
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1)?	Sí

Tabla 6. Hoja de trabajo de planificación de prerrequisitos (continuación)

Preguntas	Respuestas
¿Tiene instalados los siguientes programas y opciones bajo licencia en el sistema A?: • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3	Sí
¿Tiene instalados los siguientes programas bajo licencia en el sistema B?: • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3 • i5/OS PASE (5722-SS1 Opción 33 o 5761-SS1 Opción 33)	Sí
¿Ha instalado Windows 2000 en todos sus PC?	Sí
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC utilizado para administrar el servicio de autenticación de red?	Sí
¿Ha instalado System i Navigator y los siguientes subcomponentes en el PC utilizado para administrar el servicio de autenticación de red? • Seguridad • Red	Sí
¿Ha instalado el último Service Pack de System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí
¿Tiene la autorización especial *ALLOBJ en los sistemas?	Sí
¿Tiene autorizaciones administrativas en el servidor Windows 2000?	Sí
¿Tiene configurado el DNS y tiene los nombres de host correctos para la plataforma System i y el servidor?	Sí
¿En qué sistema operativo desea configurar el servidor Kerberos? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 o posterior) 5. z/OS	i5/OS PASE
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

La siguiente hoja de trabajo de planificación ilustra el tipo de información que necesita antes de empezar a configurar la confianza entre distintos reinos.

Tabla 7. Hoja de trabajo para planificar la confianza entre distintos reinos

Hoja de trabajo para planificar la confianza entre distintos reinos	**Respuestas**
¿Qué nombres tienen los reinos entre los que desea establecer una relación de confianza? • El reino Kerberos que utiliza el servidor Windows 2000 como servidor Kerberos • El reino Kerberos que utiliza el sistema B como servidor Kerberos (configurado en i5/OS PASE)	ORDEPT.MYCO.COM SHIPDEPT.MYCO.COM
¿Se han añadido todos los sujetos principales de usuario y todos los sujetos principales de servicio de i5/OS a sus respectivos servidores Kerberos?	Sí
¿Cuál es el nombre de usuario predeterminado del administrador de i5/OS PASE? ¿Qué contraseña desea especificar para el administrador de i5/OS PASE? **Nota:** Debe coincidir con la contraseña que utilizó al crear el servidor Kerberos en i5/OS PASE.	Nombre de usuario: admin/admin Contraseña: secret
¿Qué nombres tienen los sujetos principales que se utilizarán para configurar la confianza entre reinos? ¿Cuál es la contraseña de cada uno de estos sujetos principales?	Sujeto principal: krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM Contraseña: shipord1 Sujeto principal: krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO .COM Contraseña: shipord2
¿Cuáles son los nombres de host totalmente calificados de cada uno de los servidores Kerberos de estos reinos? • ORDEPT.MYCO.COM • SHIPDEPT.MYCO.COM	kdc1.ordept.myco.com systemb.shipdept.myco.com
Las horas de todos los sistemas, ¿difieren en menos de cinco minutos entre sí? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

Asegurarse de que el servidor Kerberos de i5/OS PASE en el sistema B se ha iniciado

Antes de configurar la confianza entre reinos, debe asegurarse de que el servidor Kerberos de i5/OS PASE se ha iniciado.

Utilice el mandato de estadísticas de proceso para determinar si el servidor Kerberos de i5/OS PASE se ha iniciado.

1. En una interfaz basada en caracteres del sistema B, escriba `call QP2TERM`. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `ps -ef | grep krb5`. Este mandato indica que desea ver todas las estadísticas de cada proceso del sistema que contenga la serie krb5. Si el servidor Kerberos está en ejecución, los resultados visualizados podrían ser similares a los de este ejemplo:

```
> ps -ef | grep krb5
     qsys   113   1   0 08:54:04      -  0:00 /usr/krb5/sbin/krb5kdc
     qsys   123   1   0 08:54:13      -  0:00 /usr/krb5/sbin/kadmind
   $
```

Si el servidor Kerberos no se ha iniciado, los resultados visualizados serían parecidos a estos:

```
> ps -ef | grep krb5
   $
```

3. Si el servidor Kerberos no se ha iniciado, siga estos pasos:
   a. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`, y pulse Intro.
   b. Escriba `start.krb5` y pulse Intro.

```
> start.krb5
  Iniciando krb5kdc...
  krb5kdc se ha iniciado satisfactoriamente.
  Iniciando kadmind...
  kadmind se ha iniciado satisfactoriamente.
  El mandato ha concluido satisfactoriamente.
  $
```

Crear un sujeto principal de confianza entre reinos en el servidor Kerberos de i5/OS PASE

Para crear un sujeto principal de confianza entre reinos en el servidor Kerberos de i5/OS PASE, siga estos pasos.

1. En una interfaz basada en caracteres, teclee `call QP2TERM`. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `kadmin -p admin/admin` y pulse Intro.
4. Inicie sesión con la contraseña de administrador. Por ejemplo, `secret`.
5. En el indicador de kadmin, escriba `addprinc krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM`. Se le pedirá que entre una contraseña para el sujeto principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM". Entre la contraseña `shipord1`. Pulse Intro. Se le pedirá que vuelva a entrar la contraseña y recibirá este mensaje:

```
Sujeto principal "krbtgt/SHIPDEPT.MYCO.COM@ORDEPT.MYCO.COM" creado.
```

6. En el indicador de kadmin, escriba `addprinc krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM`. Se le pedirá que entre una contraseña para el sujeto principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM". Entre la contraseña `shipord2`. Pulse Intro. Se le pedirá que vuelva a entrar la contraseña y recibirá este mensaje:

```
Sujeto principal "krbtgt/ORDEPT.MYCO.COM@SHIPDEPT.MYCO.COM" creado.
```

7. Escriba `quit` para salir de la interfaz kadmin y pulse F3 (Salir) para salir del entorno PASE.

Cambiar los valores de cifrado en el servidor Kerberos de i5/OS PASE

Para trabajar con las estaciones de trabajo Windows, debe cambiar los valores de cifrado predeterminados del servidor Kerberos para que los clientes se puedan autenticar ante el servidor Kerberos de i5/OS PASE.

Para cambiar los valores de cifrado predeterminados, tiene que editar el archivo kdc.conf situado en el directorio /var/krb5/krb5kdc siguiendo estos pasos:

1. En una interfaz basada en caracteres, escriba `edtf '/var/krb5/krb5kdc/kdc.conf'` para acceder al archivo kdc.conf.
2. Cambie las siguientes líneas del archivo kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

   para que sean

```
supported_enctypes = des-cbc-crc:normal des-cbc-md5:normal
```

Configurar el servidor Windows 2000 para que confíe en SHIPDEPT.MYCO.COM

Ahora que ha configurado el sistema B para que confíe en el reino ORDEPT.MYCO.COM, tendrá que configurar el servidor Windows 2000 para que confíe en el reino SHIPDEPT.MYCO.COM.

Siga estos pasos para configurar el servidor Windows 2000:

1. Inicie sesión en el servidor Windows 2000 con la cuenta de administrador.
2. En el menú Inicio, expanda **Programas** → **Herramientas administrativas** → **Dominios y confianzas de Active Directory**.
3. En la página Dominios y confianzas de Active Directory, pulse el reino **ORDEPT.MYCO.COM** con el botón derecho del ratón (el reino a veces se conoce como dominio Windows en la interfaz Windows) y seleccione **Propiedades**.
4. En la pestaña **Confianza**, pulse **Añadir** en la tabla **Dominio de confianza de este dominio**.
5. En la página Añadir dominios de confianza, escriba `SHIPDEPT.MYCO.COM` en el campo **Dominio de confianza**. Escriba `shipord1` como contraseña.
6. Se visualiza el recuadro de diálogo **Active Directory**, que indica que no se puede establecer contacto con el dominio MYCO.COM. Dado que MYCO.COM es un dominio interoperativo no de Windows y a usted le interesa configurar este lado de la confianza, pulse **Aceptar** para cerrar el recuadro de diálogo.
7. En la pestaña **Confianza**, pulse **Añadir** en la tabla **Dominio que confía en este dominio**.
8. En la página Añadir dominios de confianza, escriba `SHIPDEPT.MYCO.COM` en el campo **Dominio de confianza**. Escriba `shipord2` como contraseña.
9. Se visualiza el recuadro de diálogo **Active Directory**, que indica que no se puede establecer contacto con el dominio MYCO.COM. Dado que MYCO.COM es un dominio interoperativo no de Windows y a usted le interesa configurar este lado de la confianza, pulse **Aceptar** para cerrar el recuadro de diálogo.
10. Pulse **Aceptar**.

Añadir el reino SHIPDEPT.MYCO.COM al sistema A

Debe definir el reino SHIPDEPT.MYCO.COM en el sistema A para que este pueda determinar dónde localizar el servidor Kerberos de i5/OS PASE en el reino SHIPDEPT.MYCO.COM.

Siga estos pasos para definir el reino SHIPDEPT.MYCO.COM:

1. En System i Navigator, expanda **Sistema A** → **Seguridad** → **Servicio de autenticación de red**.
2. Pulse **Reinos** con el botón derecho del ratón y seleccione **Añadir reino**.
3. En el recuadro de diálogo **Añadir reino**, especifique la siguiente información y pulse **Aceptar**.
   a. **Reino a añadir**: `SHIPDEPT.MYCO.COM`
   b. **KDC**: `systemb.shipdept.myco.com`
   c. **Puerto**: 88
4. Pulse **Reinos** para ver la lista de reinos en el panel de la derecha. Verifique que el reino SHIPDEPT.MYCO.COM figura en la lista.

Ya ha concluido los pasos de configuración de una relación de confianza entre los reinos ORDEPT.MYCO.COM y SHIPDEPT.MYCO.COM.

Caso práctico: propagar la configuración del servicio de autenticación de red entre múltiples sistemas

Estos son los prerrequisitos y objetivos de propagar la configuración del servicio de autenticación de red entre múltiples sistemas.

Situación

Usted es administrador de sistemas de un gran fabricante de piezas de automóvil. Se encarga de gestionar cinco plataformas System i con System i Navigator. Uno de ellos funciona como sistema central, donde se almacenan los datos y desde el que se gestionan los otros sistemas. El administrador de seguridad de su compañía acaba de configurar el servicio de autenticación de red en un nuevo sistema para participar en un dominio Windows 2000, que autentica a los usuarios ante la empresa. El administrador de seguridad ha probado la configuración del servicio de autenticación de red en este sistema y ha obtenido satisfactoriamente un ticket de servicio para esta plataforma System i. Le interesa simplificar la configuración del servicio de autenticación de red entre los sistemas que gestiona.

Mediante el asistente Sincronizar funciones, desea tomar la configuración del servicio de autenticación de red del sistema modelo y aplicarla a los otros sistemas. El asistente Sincronizar funciones hará que la configuración del servicio de autenticación de red se propague de manera más rápida y sencilla a toda la red, ya que no hará falta que configure cada uno de los sistemas por separado.

Dado que uno de los sistemas ejecuta OS/400 Versión 5 Release 2 (V5R2) y que este release no soporta el asistente Sincronizar funciones, tendrá que configurar el sistema V5R2 con el asistente del servicio de autenticación de red. Deberá configurar este sistema de manera que concuerde con la configuración del servicio de autenticación de red del sistema modelo.

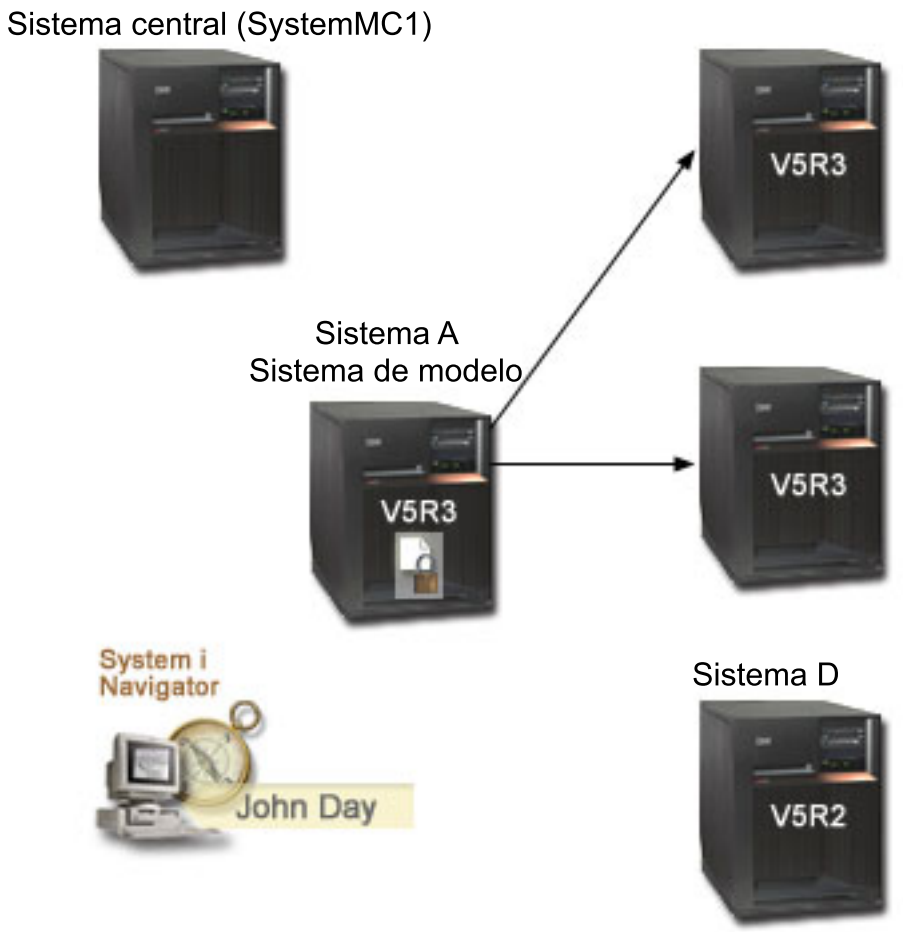
Objetivos

En este caso práctico, la empresa MyCo, Inc., tiene tres objetivos distintos:

1. Simplificar en la red la configuración del servicio de autenticación de red.
2. Hacer que todas las plataformas System i señalen hacia el mismo servidor Kerberos.
3. Configurar un sistema de la V5R2 para que también participe en el reino Kerberos.

Detalles

Los detalles de este caso práctico se muestran en el siguiente gráfico.



SystemMC1: Sistema central

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- Almacena, planifica y ejecuta tareas de sincronización de valores para cada uno de los sistemas de punto final.

Sistema A: Sistema modelo

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- Sistema que se toma como modelo para propagar la configuración del servicio de autenticación de red a los sistemas de punto final.

Sistema B: Sistema de punto final

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- Uno de los sistemas de punto final de la propagación de la configuración del servicio de autenticación de red.

Sistema C: Sistema de punto final

- Ejecuta i5/OS V5R3 con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12)
  - System i Access para Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Uno de los sistemas de punto final de la propagación de la configuración del servicio de autenticación de red.

Sistema D: Sistema de punto final

- Ejecuta OS/400 V5R2 con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12)
  - iSeries Access para Windows (5722-XE1)
  - Cryptographic Access Provider (5722-AC3)
- Se le han aplicado los siguientes arreglos temporales de programa (PTF) de la V5R2:
  - SI08977
  - SI08979
- Exige una configuración aparte del servicio de autenticación de red, utilizando para ello el asistente del servicio de autenticación de red de iSeries Navigator.

PC cliente

- Ejecuta System i Access para Windows (5722-XE1 o 5761-XE1).
- Ejecuta System i Navigator con los siguientes subcomponentes:

  Nota: Estos subcomponentes solo se necesitan en el PC que se utiliza para administrar el servicio de autenticación de red.
  - Red
  - Seguridad

Servidor Windows 2000 (no figura en el gráfico)

- Funciona como servidor Kerberos de la red (kdc1.myco.com).
- Todos los usuarios se han añadido a Microsoft Active Directory.

Nota: El nombre de servidor KDC, **kdc1.myco.com**, es un nombre ficticio que se utiliza en este caso práctico.

Prerrequisitos y supuestos

SystemMC1: Prerrequisitos del sistema central

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

Para verificar que se han instalado estos programas bajo licencia, siga estos pasos:

a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.

2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en el sistema A.
4. Nadie ha cambiado los valores predeterminados en System i Navigator para impedir que la ventana de estado de tarea se abra al iniciarse una tarea. Para verificar que el valor predeterminado no ha cambiado, siga estos pasos:

   a. En System i Navigator, pulse el ***sistema central*** con el botón derecho del ratón y seleccione **Preferencias de usuario**.
   b. En la página General, verifique que hay una marca de selección en el recuadro **Abrir automáticamente una ventana de estado de tarea al iniciarse una de mis tareas**.

5. Se ha configurado la capa de sockets segura (SSL) para proteger la transmisión de datos entre estos sistemas.

   Nota: Cuando propaga la configuración del servicio de autenticación de red entre sistemas, la información confidencial (como las contraseñas) se envía por la red. Debe utilizar SSL para proteger esta información, sobre todo si la envía fuera de la red de área local (LAN). Encontrará los detalles en el tema Caso práctico: proteger todas las conexiones al servidor de Management Central con SSL.

Sistema A: Prerrequisitos del sistema modelo

1. En este caso práctico se da por sentado que el servicio de autenticación de red está debidamente configurado en el sistema modelo (el sistema A).
2. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado estos programas bajo licencia, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.

3. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
4. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en el sistema.
5. Se ha configurado la capa de sockets segura (SSL) para proteger la transmisión de datos entre estos sistemas.

   Nota: Cuando propaga la configuración del servicio de autenticación de red entre sistemas, la información confidencial (como las contraseñas) se envía por la red. Debe utilizar SSL para proteger esta información, sobre todo si la envía fuera de la red de área local (LAN). Encontrará los detalles en el tema Caso práctico: proteger todas las conexiones al servidor de Management Central con SSL.

Sistema B, sistema C y sistema D: Prerrequisitos del sistema de punto final

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado estos programas bajo licencia, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.
   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.

2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.

3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en el sistema.
4. Se ha configurado la capa de sockets segura (SSL) para proteger la transmisión de datos entre estos sistemas.

   Nota: Cuando propaga la configuración del servicio de autenticación de red entre sistemas, la información confidencial (como las contraseñas) se envía por la red. Debe utilizar SSL para proteger esta información, sobre todo si la envía fuera de la red de área local (LAN). Encontrará los detalles en el tema Caso práctico: proteger todas las conexiones al servidor de Management Central con SSL.

Servidor Windows 2000 (no figura en el gráfico)

1. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
2. El protocolo TCP/IP se ha configurado y probado en el servidor.
3. El dominio Windows se ha configurado y probado.
4. Todos los usuarios de la red se han añadido a un dominio Windows mediante Active Directory.

Pasos de configuración

Para utilizar el asistente Sincronizar funciones para propagar la configuración del servicio de autenticación de red a los sistemas de punto final, debe llevar a cabo los pasos siguientes.

Cumplimentar las hojas de trabajo de planificación

Para poder empezar a utilizar System i Navigator para propagar la configuración de un sistema modelo a los sistemas destino, cumplimente estas hojas de trabajo de planificación.

Podrá proseguir con la propagación del servicio de autenticación de red cuando responda afirmativamente a todas las preguntas.

Tabla 8. Propagar el servicio de autenticación de red - hoja de trabajo de prerrequisitos

Hoja de trabajo de prerrequisitos	Respuestas
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1) en los sistemas siguientes? • Sistema central • Sistema A • Sistema B • Sistema C	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
En el sistema D, ¿se ejecuta OS/400 V5R2, i5/OS V5R3 o posterior?	Sí
Para el sistema D, ¿ha aplicado los arreglos temporales de programa (PTF) más recientes, incluidos los siguientes? • SI08977 • SI08979	
¿Tiene instalados los siguientes programas y opciones bajo licencia en todos los modelos de System i? • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3	Sí

Tabla 8. Propagar el servicio de autenticación de red - hoja de trabajo de prerrequisitos (continuación)

Hoja de trabajo de prerrequisitos	Respuestas
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC del administrador?	Sí
¿Está instalado System i Navigator en el PC del administrador? • ¿Está el subcomponente de red de System i Navigator instalado en el PC del administrador? • ¿Está el subcomponente de seguridad de System i Navigator instalado en el PC del administrador?	Sí
¿Ha instalado el último Service Pack de IBM System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí
¿Tiene las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG?	Sí
¿Funciona alguno de los siguientes sistemas a modo de servidor Kerberos? Si es así, indique qué sistema. 1. Microsoft Windows 2000 Server **Nota:** Microsoft Windows 2000 Server utiliza la autenticación Kerberos como mecanismo de seguridad predeterminado. 2. Windows Server 2003 3. i5/OS PASE (V5R3 o posterior) 4. Servidor AIX 5. z/OS	Sí, Windows 2000 Server
Para Windows 2000 Server y Windows Server 2003, ¿ha instalado las herramientas de soporte de Windows (que suministran la herramienta ktpass)?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte Sincronizar las horas de los sistemas.	Sí

Tabla 9. Hoja de trabajo de planificación para sincronizar funciones

Preguntas	Respuestas
¿Cuál es el nombre del grupo de sistemas?	Grupo de sistemas MyCo
¿Qué sistemas formarán parte de este grupo?	Sistema B, sistema C, sistema D
¿Qué funciones se propone propagar a este grupo de sistemas?	Servicio de autenticación de red
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	Autenticación Kerberos i5/OS
¿Qué nombres de sujeto principal de servicio tienen los sistemas a los que desea propagar la configuración?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM
¿Cuáles son las contraseñas asociadas a cada uno de estos sujetos principales?	La contraseña de los sujetos principales de los sistemas A, B y C es `systema123`. La contraseña del sujeto principal del sistema D es `systemd123`.

Tabla 9. Hoja de trabajo de planificación para sincronizar funciones (continuación)

Preguntas	Respuestas
¿Cuál es el nombre de host totalmente calificado de cada plataforma System i?	systema.myco.com systemb.myco.com systemc.myco.com systemd.myco.com
¿Qué nombre tiene el dominio Windows 2000? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	MYCO.COM

Tabla 10. Hoja de trabajo de planificación del servicio de autenticación de red para el sistema D

Preguntas	Respuestas
¿Cuál es el nombre del reino Kerberos predeterminado al que pertenece la plataforma System i? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	MYCO.COM
¿Está utilizando Microsoft Active Directory?	Sí
¿Cuál es el servidor Kerberos del reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	**KDC:** kdc1.myco.com **Puerto:** 88 **Nota:** Este es el puerto predeterminado del servidor Kerberos.
¿Desea configurar un servidor de contraseñas para este reino predeterminado? Si es así, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este servidor Kerberos? ¿En qué puerto está a la escucha el servidor de contraseñas?	Sí **Servidor de contraseñas:** kdc1.myco.com **Puerto:** 464 **Nota:** Este es el puerto predeterminado del servidor de contraseñas.
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer	Autenticación de Kerberos de i5/OS
¿Qué contraseña utilizará para los sujetos principales de servicio de i5/OS?	systemd123

Crear un grupo de sistemas

Para poder propagar la configuración del servicio de autenticación de red a un sistema destino, primero debe crear un grupo con todos los sistemas de punto final.

Grupo de sistemas es un conjunto de sistemas que se pueden gestionar y a los que se pueden aplicar valores y atributos similares, como la configuración del servicio de autenticación de red. Siga estos pasos para crear un grupo de sistemas:

1. En System i Navigator, expanda **Management Central (SystemMC1)**.
2. Pulse **Grupos de sistemas** con el botón derecho del ratón y seleccione **Grupo de sistemas nuevo** para crear un nuevo grupo de sistemas.
3. En la página General, escriba `Grupo de sistemas MyCo` en el campo nombre y especifique una descripción de este grupo de sistemas.

4. En la lista **Sistemas disponibles**, seleccione **Sistema B**, **Sistema C** y **Sistema D** y pulse **Añadir**. Así, estos sistemas se añadirán a la lista **Sistemas seleccionados**. Pulse **Aceptar**.
5. Expanda **Grupos de sistemas** para verificar que su grupo de sistemas se ha añadido.

Propagar los valores del sistema modelo (sistema A) al sistema B y al sistema C

Para propagar los valores del sistema en múltiples sistemas de punto final, utilice el asistente Sincronizar funciones en System i Navigator. El asistente puede propagar los valores del sistema, como por ejemplo, la configuración del servicio de autenticación de red.

Para propagar la configuración del servicio de autenticación de red a los sistemas destino, siga estos pasos:

1. En System i Navigator, expanda **Management Central (SystemMC1)** → **Grupos de sistemas**.
2. Pulse **Grupo de sistemas MyCo** con el botón derecho del ratón y seleccione **Valores del sistema** → **Sincronizar funciones**. Así se lanza el asistente **Sincronizar funciones**.
3. En la página Bienvenido, lea la información sobre el asistente Sincronizar funciones y pulse **Siguiente**. En la página Bienvenido figuran las funciones que puede elegir para sincronizar más adelante en el asistente.

   Nota: Cuando propaga la configuración del servicio de autenticación de red entre sistemas, la información confidencial (como las contraseñas) se envía por la red. Debe utilizar SSL para proteger esta información, sobre todo si la envía fuera de la red de área local (LAN). Encontrará los detalles en el tema Caso práctico: proteger todas las conexiones al servidor de Management Central con SSL.
4. En la página Sistema modelo, seleccione que el sistema A es el sistema modelo y pulse **Siguiente**. El sistema modelo servirá de base para sincronizar la configuración del servicio de autenticación de red con los otros sistemas.
5. En la página Sistemas y grupos destino, seleccione **Grupo de sistemas MyCo**. Pulse **Siguiente**.
6. En la página Qué actualizar, seleccione **Servicio de autenticación de red (Kerberos)**. Pulse **Verificar configuración**. Una vez verificada la configuración, pulse **Siguiente**.

   Nota: Si la verificación del servicio de autenticación de red no resulta satisfactoria, podría haberse producido un problema relacionado con la configuración del servicio de autenticación de red en el sistema modelo. Para corregir este error, debe comprobar la configuración en el sistema modelo, arreglar la configuración y después volver al paso 2 de estas instrucciones.
7. En la página Servicio de autenticación de red, seleccione **Autenticación Kerberos de i5/OS** y escriba `systema123` en los campos **Contraseña** y **Confirmar contraseña**. Pulse **Siguiente**.

   Nota: Esta contraseña se emplea para la entrada de tabla de claves en cada sistema destino. Si su política de seguridad exige que la contraseña sea distinta en cada sistema, puede saltarse este paso. En su lugar, una vez concluido el asistente, puede añadir manualmente las entradas de tabla de claves a los sistemas individuales y entrar una contraseña distinta para cada uno.
8. En la página Resumen, verifique que en ella figuran los valores pertinentes. Pulse **Finalizar**.
9. Por omisión, se visualiza un recuadro de diálogo que indica que se ha iniciado la tarea Sincronizar funciones. No obstante, si ha cambiado el valor predeterminado, este recuadro de diálogo no se visualizará. Pulse **Aceptar**.
10. Se visualiza el recuadro de diálogo **Sincronizar estado de funciones**. Verifique que la tarea se ha realizado satisfactoriamente. Asuma que la tarea se ha completado satisfactoriamente en todos los sistemas de punto final, excepto en el sistema D. Dado que el sistema D ejecuta OS/400 V5R2, no da soporte al asistente Sincronizar funciones.

    Para corregir este error, debe configurar manualmente el servicio de autenticación de red en el sistema D para que coincida con la configuración del sistema modelo (sistema A).

Configurar el servicio de autenticación de red en el sistema D

Debe configurar el servicio de autenticación de red en el sistema D para que coincida con los valores de configuración del sistema A.

Para configurar el servicio de autenticación de red, siga estos pasos:

1. En System i Navigator, expanda **Sistema D** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración.

   Nota: Tras configurar el servicio de autenticación de red, esta opción indicará **Reconfigurar**.
3. En la página de bienvenida encontrará información sobre los objetos que crea el asistente. Pulse **Siguiente**.
4. En la página Especificar información de reino, escriba `MYCO.COM` en el campo **Reino predeterminado** y seleccione **Se utiliza Microsoft Active Directory para la autenticación Kerberos**. Pulse **Siguiente**.
5. En la página Especificar información de KDC, escriba kdc1.myco.com para el nombre del servidor Kerberos de este reino en el campo **KDC** y teclee 88 en el campo **Puerto**. Pulse **Siguiente**.
6. En la página Especificar información de contraseña, seleccione **Sí** para configurar el sistema D para que señale hacia el servidor de contraseñas configurado para el reino predeterminado. El servidor de contraseñas ya se ha configurado. Permite a los sujetos principales cambiar las contraseñas en el servidor Kerberos. Entre `kdc1.myco.com` en el campo **Servidor de contraseñas**. El puerto predeterminado del servidor de contraseñas es el 464. Pulse **Siguiente**.
7. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. Pulse **Siguiente**.
8. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña y confírmela, por ejemplo, `systemd123`. Pulse **Siguiente**.
9. Opcional: En la página Crear archivo por lotes, seleccione **No**.
10. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.

Añadir los sujetos principales de los sistemas de punto final al dominio Windows 2000

Estos son los pasos para añadir sujetos principales para sistemas de punto final.

1. **Pasos para el sistema B**
   a. En el servidor Windows 2000, expanda **Herramientas administrativas** → **Usuarios y equipos de Active Directory**.
   b. Seleccione **MYCO.COM** como dominio y expanda **Acción** → **Nuevo** → **Usuario**.

      Nota: Este dominio Windows debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.
   c. En el campo **Nombre**, escriba `systemb` para identificar la plataforma System i ante este dominio Windows. Así se añadirá una cuenta de usuario nueva para el sistema B.
   d. Acceda a las propiedades del usuario systemb de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá que el sujeto principal de servicio de i5/OS acceda a otros servicios en nombre de un usuario conectado.
   e. En el servidor Windows 2000, tiene que correlacionar la cuenta de usuario que acaba de crear con el sujeto principal de servicio de i5/OS utilizando el mandato **ktpass**. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows 2000 Server. En un indicador de mandatos de Windows, escriba el mandato siguiente:

      ```
      ktpass -mapuser systemb -pass systema123 -princ krbsvr400/systemb.myco.com@MYCO.COM
      -mapop set
      ```
2. **Pasos para el sistema C**

a. En el servidor Windows 2000, expanda **Herramientas administrativas → Usuarios y equipos de Active Directory**.
b. Seleccione **MYCO.COM** como dominio y expanda **Acción → Nuevo → Usuario**.

   Nota: Este dominio Windows debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.
c. En el campo **Nombre**, escriba `systemc` para identificar la plataforma System i ante este dominio Windows. Así se añadirá una cuenta de usuario nueva para el sistema C.
d. Acceda a las propiedades del usuario systemc de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá que el sujeto principal de servicio de i5/OS acceda a otros servicios en nombre de un usuario conectado.
e. En el servidor Windows 2000, tiene que correlacionar la cuenta de usuario que acaba de crear con el sujeto principal de servicio de i5/OS utilizando el mandato ktpass. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows 2000 Server. En un indicador de mandatos de Windows, escriba el mandato siguiente:

   ```
   ktpass -mapuser systemc -pass systema123 -princ krbsvr400/systemc.myco.com@MYCO.COM
   -mapop set
   ```

3. **Pasos para el sistema D**
   a. En el servidor Windows 2000, expanda **Herramientas administrativas → Usuarios y equipos de Active Directory**.
   b. Seleccione **MYCO.COM** como dominio y expanda **Acción → Nuevo → Usuario**.

      Nota: Este dominio Windows debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.
   c. En el campo **Nombre**, escriba `systemd` para identificar la plataforma System i ante este dominio Windows. Así se añadirá una cuenta de usuario nueva para el sistema D.
   d. Acceda a las propiedades del usuario systemd de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá que el sujeto principal de servicio de i5/OS acceda a otros servicios en nombre de un usuario conectado.
   e. En el servidor Windows 2000, tiene que correlacionar la cuenta de usuario que acaba de crear con el sujeto principal de servicio de i5/OS utilizando el mandato ktpass. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows 2000 Server. En un indicador de mandatos de Windows, escriba el mandato siguiente:

      ```
      ktpass -mapuser systemd -pass systemd123 -princ krbsvr400/systemd.myco.com@MYCO.COM
      -mapop set
      ```

Ya ha terminado de propagar la configuración del servicio de autenticación de red a múltiples sistemas. Para configurar el servidor de Management Central con vistas a que saque partido del servicio de autenticación de red, tendrá que llevar a cabo algunas tareas adicionales. Encontrará los detalles en el tema “Caso práctico: utilizar la autenticación Kerberos entre servidores de Management Central”.

Caso práctico: utilizar la autenticación Kerberos entre servidores de Management Central

Estos son los prerrequisitos y objetivos de utilizar la autenticación Kerberos entre servidores de Management Central.

Situación

Usted es administrador de la red de una mediana empresa de fabricación de piezas. Se encarga de gestionar cuatro productos System i utilizando System i Navigator en un PC cliente. Le interesa que los trabajos servidores de Management Central utilicen la autenticación Kerberos en lugar de los otros

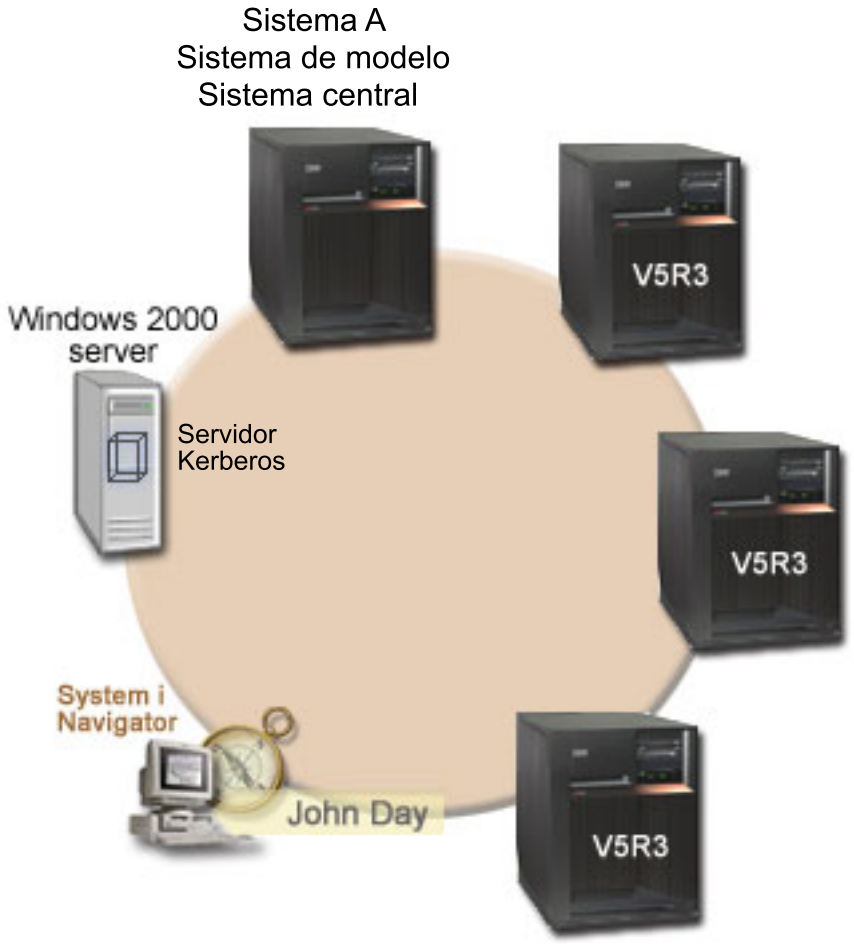
métodos de autenticación que ha venido utilizando hasta a hora, concretamente la sincronización de contraseñas.

Objetivos

En este caso práctico, el objetivo de la empresa MyCo, Inc. es utilizar la autenticación Kerberos entre los servidores de Management Central.

Detalles

Los detalles de este caso práctico se muestran en el siguiente gráfico.



Sistema A: Sistema modelo y central

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- El sujeto principal de servicio de i5/OS, krbsvr400/systema.myco.com@MYCO.COM, y la contraseña asociada se han añadido al archivo de tabla de claves.
- Almacena, planifica y ejecuta tareas de sincronización de valores para cada uno de los sistemas de punto final.

Sistema B: Sistema de punto final

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- El sujeto principal de servicio de i5/OS, krbsvr400/systemb.myco.com@MYCO.COM, y la contraseña asociada se han añadido al archivo de tabla de claves.

Sistema C: Sistema de punto final

- Ejecuta i5/OS V5R4 con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE)
- El sujeto principal de servicio de i5/OS, krbsvr400/systemc.myco.com@MYCO.COM, y la contraseña asociada se han añadido al archivo de tabla de claves.

Sistema D: Sistema de punto final

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Cryptographic Access Provider (5722-AC3)
- El sujeto principal de servicio de i5/OS, krbsvr400/systemd.myco.com@MYCO.COM, y la contraseña asociada se han añadido al archivo de tabla de claves.

Servidor **Windows 2000**

- Funciona como servidor Kerberos para estos sistemas.
- Los siguientes sujetos principales de servicio de i5/OS se han añadido al servidor Windows 2000:
  - krbsvr400/systema.myco.com@MYCO.COM
  - krbsvr400/systemb.myco.com@MYCO.COM
  - krbsvr400/systemc.myco.com@MYCO.COM
  - krbsvr400/systemd.myco.com@MYCO.COM

PC cliente

- Ejecuta System i Access para Windows (5722-XE1 o 5761-XE1).
- Ejecuta System i Navigator con los siguientes subcomponentes:

  Nota: Solo se necesitan en el PC que se utiliza para administrar el servicio de autenticación de red.
  - Red
  - Seguridad

Prerrequisitos y supuestos

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado los programas bajo licencia, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.

   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.

2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en cada uno de estos sistemas.
4. Nadie ha cambiado los valores predeterminados en System i Navigator para detener que la ventana de estado de tarea se abra al iniciarse una tarea. Para verificar que el valor predeterminado no ha cambiado, siga estos pasos:
   a. En System i Navigator, pulse el ***sistema central*** con el botón derecho del ratón y seleccione **Preferencias de usuario**.
   b. En la página General, verifique que hay una marca de selección en el recuadro **Abrir automáticamente una ventana de estado de tarea al iniciarse una de mis tareas**.
5. Este caso práctico se basa en el supuesto de que el servicio de autenticación de red se ha configurado en cada sistema utilizando el asistente Sincronizar funciones de System i Navigator. Este asistente propaga la configuración del servicio de autenticación de red de un modelo sistema a múltiples sistemas destino. En el tema "Caso práctico: propagar la configuración del servicio de autenticación de red entre múltiples sistemas" en la página 36 encontrará los detalles de cómo utilizar el asistente Sincronizar funciones.

Pasos de configuración

Para configurar la autenticación Kerberos entre servidores de Management Central, lleve a cabo los pasos siguientes.

Cumplimentar las hojas de trabajo de planificación

Estas hojas de trabajo de planificación ilustran el tipo de información que necesita antes de habilitar los sistemas para que utilicen la autenticación Kerberos.

Tabla 11. Utilizar la autenticación Kerberos entre servidores de Management Central - hoja de trabajo de prerrequisitos

Hoja de trabajo de prerrequisitos	**Respuestas**
¿Utiliza i5/OS V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1), en todas las plataformas System i?	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
¿Tiene instalados los siguientes programas y opciones bajo licencia en todos los modelos de System i? • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3	Sí
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC del administrador?	Sí
¿Está instalado System i Navigator en el PC del administrador? • ¿Está el subcomponente de red de System i Navigator instalado en el PC del administrador? • ¿Está el subcomponente de seguridad de System i Navigator instalado en el PC del administrador?	Sí
¿Ha instalado el último Service Pack de IBM System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí

Tabla 11. Utilizar la autenticación Kerberos entre servidores de Management Central - hoja de trabajo de prerrequisitos (continuación)

Hoja de trabajo de prerrequisitos	Respuestas
¿Tiene las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG?	Sí
¿Funciona alguno de los siguientes sistemas a modo de servidor Kerberos? Si es así, indique qué sistema. 1. Microsoft Windows 2000 Server **Nota:** Microsoft Windows 2000 Server utiliza la autenticación Kerberos como mecanismo de seguridad predeterminado. 2. Windows Server 2003 3. i5/OS PASE (V5R3 o posterior) 4. Servidor AIX 5. z/OS	Sí, Windows 2000 Server
Para Windows 2000 Server y Windows Server 2003, ¿ha instalado las herramientas de soporte de Windows (que suministran la herramienta ktpass)?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

Tabla 12. Utilizar la autenticación Kerberos entre servidores de Management Central - hoja de trabajo de planificación

Preguntas	Respuestas
¿Cuál es el nombre del grupo de sistemas?	Grupo de sistemas MyCo2
¿Qué sistemas formarán parte de este grupo?	Sistema A, sistema B, sistema C, sistema D
¿Qué nombres de sujeto principal de servicio tienen las plataformas System i?	krbsvr400/systema.myco.com@MYCO.COM krbsvr400/systemb.myco.com@MYCO.COM krbsvr400/systemc.myco.com@MYCO.COM krbsvr400/systemd.myco.com@MYCO.COM

Establecer el sistema central para que utilice la autenticación Kerberos

El sistema A es el sistema modelo y el sistema central de los otros sistemas destino.

Para establecer la autenticación Kerberos en el sistema central, lleve a cabo estos pasos:

1. En System i Navigator, pulse con el botón derecho del ratón en **Management Central (sistema A)** y seleccione **Propiedades**.
2. En la pestaña **Seguridad**, seleccione **Utilizar autenticación Kerberos** y establezca el nivel de autenticación en **Añadir a grupo de confianza**.
3. Seleccione **No utilizar** en el campo **Correlación de identidades** y pulse **Aceptar**. Este valor le permite habilitar o inhabilitar que los servidores de Management Central utilicen la correlación de identidades de empresa (EIM) con vistas a habilitar un entorno de inicio de sesión único (SSO) para los sistemas de punto final. Si desea habilitar el inicio de sesión único en los sistemas de punto final, vea el tema Caso práctico: Configurar el servidor de Management Central para un entorno de inicio de sesión único, donde encontrará un ejemplo relacionado con esta configuración.

   Nota: La nota situada en la parte inferior de la página Seguridad indica que los valores entrarán en vigor la próxima vez que se inicien los servidores de Management Central. No reinicie los servidores en esta ocasión. En un paso ulterior de este caso práctico, se indicará el momento apropiado para reiniciar los servidores.

4. Se visualiza un recuadro de diálogo que indica que los cambios realizados en estos valores tan solo afectan a este sistema central y que hay que configurar debidamente Kerberos para que los trabajos servidores de Management Central puedan utilizar estos valores. Pulse **Aceptar**. Ya ha habilitado la autenticación Kerberos para que la utilice el sistema central.

Crear el grupo de sistemas MyCo2

Grupo de sistemas es un conjunto de sistemas que se pueden gestionar y a los que se pueden aplicar valores y atributos similares, como la configuración del servicio de autenticación de red.

Para poder aplicar los valores pertinentes a los otros sistemas de la red, primero debe crear un grupo con todos los sistemas de punto final.

1. En System i Navigator, expanda **Management Central (sistema A)**.
2. Pulse **Grupos de sistemas** con el botón derecho del ratón y seleccione **Grupo de sistemas nuevo** para crear un nuevo grupo de sistemas.
3. En la página General, escriba `Grupo de sistemas MyCo2` en el campo del nombre. Especifique una descripción para este grupo de sistemas.
4. En la lista **Sistemas disponibles**, seleccione Sistema A, Sistema B, Sistema C y Sistema D y pulse **Añadir**. Así, estos sistemas se añadirán a la lista **Sistemas seleccionados**. Pulse **Aceptar**.
5. Expanda **Grupos de sistemas** para verificar que su grupo de sistemas se ha añadido.

Recoger el inventario de valores del sistema

Deberá utilizar la función Recoger Inventario de System i Navigator para añadir los valores de la autenticación Kerberos a un inventario de los sistemas destino del grupo de sistemas MyCo2.

Para recoger el inventario del grupo de sistemas MyCo2, lleve a cabo los pasos siguientes:

1. En System i Navigator, expanda **Management Central (sistema A)** → **Grupos de sistemas**.
2. Pulse **Grupo de sistemas MyCo2** con el botón derecho del ratón y seleccione **Inventario** → **Recoger**.
3. En la página Recoger inventario - Grupo de sistemas MyCo2, seleccione **Valores del sistema**. Pulse **Aceptar**. Por omisión, se visualiza un recuadro de diálogo que indica que se ha iniciado la tarea de recogida de inventario de sincronización de funciones. No obstante, si ha cambiado el valor predeterminado, este recuadro de diálogo no se visualizará. Pulse **Aceptar**.
4. En la página Estado de recoger inventario, lea todos los valores de estado visualizados y arregle los problemas que hayan podido surgir. Para obtener los detalles de los valores de estado concretos relacionados con la recogida de inventario que aparecen en esta página, seleccione **Ayuda** → **Ayuda de estado de tarea**. En la página de ayuda de **Estado de tarea**, seleccione **Inventario**. Esta página visualiza los posibles valores de estado, sus descripciones detalladas e información de recuperación.
5. Si la recogida de inventario se ha llevado a cabo satisfactoriamente, cierre la ventana de estado.

Comparar y actualizar los valores de Kerberos en System i Navigator

Después de recoger el inventario de valores del sistema, deberá tomar los valores de Kerberos que se seleccionaron en el sistema central y aplicarlos a cada uno de los sistemas destino del grupo de sistemas MyCo2.

Para actualizar los sistemas destino del grupo de sistemas MyCo2, lleve a cabo estos pasos:

1. En System i Navigator, expanda **Management Central (sistema A)** → **Grupos de sistemas**.
2. Pulse **Grupo de sistemas MyCo2** con el botón derecho del ratón y seleccione **Valores del sistema** → **Comparar y actualizar**.
3. Cumplimente los campos del recuadro de diálogo **Comparar y actualizar - Grupo de sistemas MyCo2**:
   a. Seleccione **Sistema A** para el campo **Sistema modelo**.
   b. Seleccione **Management Central** para el campo **Categoría**.

c. En la lista **Elementos a comparar**, seleccione **Utilizar autenticación Kerberos para verificar peticiones** y **Nivel de confianza de autenticación Kerberos**.

4. Verifique que los sistemas destino del grupo de sistemas MyCo2 se visualizan en la lista de sistemas destino y pulse **Aceptar** para dar comienzo a la actualización. Así se actualizará cada uno de los sistemas destino del grupo de sistemas MyCo2 con los valores de autenticación Kerberos que se seleccionaron en el sistema modelo.
5. Por omisión, se visualiza un diálogo que indica que se ha iniciado la tarea Comparar y actualizar. No obstante, si ha cambiado el valor predeterminado, este recuadro de diálogo no se visualizará. Pulse **Aceptar**.
6. En el recuadro de diálogo **Estado de actualización de valores**, verifique que la actualización se lleva a cabo en cada sistema y cierre el recuadro de diálogo.

Reiniciar el servidor de Management Central en el sistema central y en los sistemas destino

Una vez concluida la actualización de cada uno de los sistemas destino del grupo de sistemas MyCo2, deberá reiniciar todos los servidores de Management Central en el sistema central y en los sistemas destino.

Para reiniciar los servidores de Management Central, lleve a cabo los pasos siguientes:

1. En System i Navigator, expanda **Mis conexiones** → **Sistema A** → **Red** → **Servidores** → **TCP/IP**.
2. Pulse **Management Central** con el botón derecho del ratón y seleccione **Detener**. Espera a que se haya detenido el servidor de Management Central. Pulse F5 para renovar la pantalla y ver el estado en el panel de la derecha. El estado debe indicar **Detenido** cuando el servidor se haya detenido.
3. Pulse **Management Central** con el botón derecho del ratón y seleccione **Iniciar**. Así se reiniciarán los servidores de Management Central en el sistema central.
4. Repita los pasos 1-3 en los sistemas destino: Sistema B, Sistema C y Sistema D.

Añadir el sujeto principal de servicio Kerberos al archivo de grupos de confianza de cada punto final

Después de reiniciar todos los servidores de Management Central, debe añadir el sujeto principal de servicio Kerberos del sistema central al archivo de grupos de confianza de cada uno de los sistemas de punto final.

En el sistema central, ejecute un mandato remoto, como puede ser Visualizar lista de bibliotecas (DSPLIBL), para todos los sistemas de punto final. Cada sistema de punto final añade automáticamente el sujeto principal de servicio Kerberos del sistema central al correspondiente archivo de grupos de confianza individual, porque el nivel de autenticación seleccionado para cada sistema de punto final es **Añadir a grupo de confianza**. Puede emitir cualquier mandato remoto desde el sistema central a un sistema de punto final para hacer que el trabajo servidor de Management Central del sistema de punto final anote los sujetos principales Kerberos necesarios en el archivo de grupos de confianza. El mandato DSPLIBL tan solo se utiliza a modo de ejemplo.

Nota: Si utiliza un sistema modelo u origen para ejecutar tareas, como las de enviar arreglos, enviar usuarios o sincronizar la hora, debe ejecutarlas de tal manera que se añadan los sujetos principales de servicio Kerberos correctos a los archivos de grupos de confianza correctos.

En este caso práctico, decidirá que va a emitir un mandato remoto a todos los sistemas de punto final para añadir el sujeto principal de servicio Kerberos al archivo de grupos de confianza de cada sistema de punto final. Para ejecutar un mandato remoto, siga estos pasos:

1. En System i Navigator, expanda **Management Central (sistema A)** → **Grupos de sistemas**.
2. Pulse **Grupo de sistemas MyCo2** con el botón derecho del ratón y seleccione **Ejecutar mandato**.
3. En la página Ejecutar mandato - Grupo de sistemas MyCo2, escriba `dsplibl` en el campo **Mandatos a ejecutar** y pulse **Aceptar** para iniciar inmediatamente la tarea del mandato. También puede pulsar

Mandatos anteriores para seleccionar en una lista de los mandatos que ha ejecutado con anterioridad, o bien pulsar **Solicitud** para obtener ayuda a la hora de entrar o seleccionar un mandato de i5/OS.

4. Por omisión, se visualiza un recuadro de diálogo que indica que se ha iniciado la tarea de ejecutar mandato. No obstante, si ha cambiado el valor predeterminado, este recuadro de diálogo no se visualizará. Pulse **Aceptar**.
5. En el recuadro de diálogo **Estado de ejecución de mandato**, verifique que el mandato se lleva a cabo en cada sistema y cierre el recuadro de diálogo.

Verificar que los sujetos principales Kerberos se han añadido al archivo de grupos de confianza

Después de ejecutar el mandato remoto, puede verificar que el sujeto principal Kerberos del sistema central figura en el archivo de grupos de confianza de cada uno de los sistemas destino.

1. En System i Navigator, expanda **System B** → **Sistemas de archivos** → **Sistema de archivos integrado** → **Root** → **QIBM** → **UserData** → **OS400** → **MGTC** → **config**.
2. Pulse **McTrustedGroup.conf** con el botón derecho del ratón y seleccione **Editar** para ver el contenido del archivo.
   a. Pulse **Sistema de archivos integrado** con el botón derecho del ratón y seleccione **Propiedades**.
   b. En el recuadro de diálogo **Propiedades del sistema de archivos integrado**, seleccione **Todos los archivos** para **Habilitar opciones de edición para:** y pulse **Aceptar**.
3. Verifique que el sujeto principal de servicio Kerberos del sistema central figura en la lista de los miembros de grupos de confianza de Management Central.
4. Repita estos pasos para sistema C y sistema D con vistas a verificar que el sujeto principal de servicio Kerberos del sistema central se ha añadido a cada uno de los sistemas destinos.

Permitir conexiones de confianza para el sistema central

Una vez ejecutado satisfactoriamente el mandato remoto en los sistemas de punto final, tendrá que permitir conexiones de confianza entre los servidores de Management Central.

Siga estos pasos para permitir conexiones de confianza. Así se asegura que solo el sistema central del grupo de sistemas MyCo2 (sistema A) puede ejecutar tareas en los sistemas destino.

1. En System i Navigator, pulse con el botón derecho del ratón en **Management Central (sistema A)** y seleccione **Propiedades**.
2. En la pestaña **Seguridad**, seleccione **Utilizar autenticación Kerberos** y establezca el nivel de autenticación en **Permitir solo conexiones de confianza**.
3. Seleccione **No utilizar** en el campo **Correlación de identidades**.
4. Se visualiza un recuadro de diálogo que indica que los cambios realizados en estos valores tan solo afectan a este sistema central y que hay que configurar debidamente Kerberos para que los trabajos servidores de Management Central puedan utilizar estos valores. Pulse **Aceptar**.

Repetir los pasos del 4 al 6 para los sistemas destino

Una vez permitidas las conexiones de confianza para el sistema central, debe repetir los pasos del 4 al 6 de este caso práctico para aplicar estos cambios a los sistemas destino del grupo de sistemas MyCo2. Así se asegura de que los sistemas destino están configurados para permitir conexiones de confianza.

Le remitimos a estos pasos:

1. Paso 4: Recoger el inventario de valores del sistema
2. Paso 5: Comparar y actualizar los valores de Kerberos en System i Navigator
3. Paso 6: Reiniciar el servidor de Management Central en el sistema central y en los sistemas destino

Probar la autenticación en los sistemas de punto final

Después de reiniciar los servidores, los sistemas utilizarán Kerberos de cara a la autenticación y el grupo de confianza para la autorización. Para que un sistema acepte y lleve a cabo una petición, ese sistema

verificará no solo que el sistema peticionario tiene un sujeto principal Kerberos válido, sino también que confía en el sujeto principal Kerberos comprobando si dicho sujeto figura en la correspondiente lista de grupos de confianza.

Nota: Tendrá que repetir estos pasos en cada uno de los sistemas destino, utilizando los siguientes sujetos principales de servicio de i5/OS:

- krbsvr400/systema.myco.com@MYCO.COM
- krbsvr400/systemb.myco.com@MYCO.COM
- krbsvr400/systemc.myco.com@MYCO.COM
- krbsvr400/systemd.myco.com@MYCO.COM

Para verificar que la autenticación Kerberos funciona en los sistemas de punto final, lleve a cabo las tareas siguientes:

Nota: Antes de llevar a cabo estas tareas, asegúrese de que ha creado un directorio inicial (home) para su perfil de usuario i5/OS.

1. Cierres las sesiones de System i Navigator.
2. En una línea de mandatos del intérprete Qshell, escriba `QSH` para iniciar el intérprete Qshell.
3. Entre `keytab list` para visualizar una lista de los sujetos principales registrados en el archivo de tabla de claves. Debe ver resultados parecidos a los de esta pantalla:

```
Sujeto principal: krbsvr400/systema.myco.com@MYCO.COM
  Versión de clave: 2
  Tipo de clave: DES de 56 bits mediante derivación de clave
  Indicación de la hora de la entrada: 200X/05/29-11:02:58
```

4. Escriba `kinit -k krbsvr400/systema.myco.com@MYCO.COM` para solicitar un ticket de otorgamiento de tickets al servidor Kerberos. Este mandato verifica que el sistema está debidamente configurado y que la contraseña del archivo de tabla de claves concuerda con la almacenada en el servidor Kerberos. Si la verificación es satisfactoria, el mandato QSH mostrará que no hay errores.
5. Escriba `klist` para verificar que el sujeto principal predeterminado es krbsvr400/systema.myco.com@MYCO.COM. Este mandato visualiza el contenido de una memoria caché de credenciales Kerberos y verifica que se ha creado un ticket válido para el sujeto principal de servicio de i5/OS y que se ha colocado en la memoria caché de credenciales del sistema.

```
 Memoria caché de tickets: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Sujeto principal predeterminado: krbsvr400/systema.myco.com@MYCO.COM

Servidor: krbtgt/MYCO.COM@MYCO.COM
  Válido del 200X/06/09-12:08:45 al 20XX/11/05-03:08:45
$
```

Ya ha llevado a cabo las tareas necesarias para configurar los trabajos servidores de Management Central para que utilicen la autenticación Kerberos entre los sistemas de punto final.

Caso práctico: habilitar el inicio de sesión único para i5/OS

Estos son los prerrequisitos y objetivos para habilitar el inicio de sesión único para el sistema operativo i5/OS.

Situación

Usted es un administrador de la red de su empresa y se encarga de gestionar la red y su seguridad, incluido el departamento de recepción de pedidos. Supervisa las operaciones de tecnología de la

información (TI) de una gran cantidad de empleados que toman nota de los pedidos que los clientes cursan por teléfono. Supervisa asimismo a otros dos administradores de la red que le ayudan en las tareas de mantenimiento.

Los empleados del departamento de recepción de pedidos utilizan Windows 2000 y i5/OS, y necesitan múltiples contraseñas para las distintas aplicaciones que emplean a diario. Por lo tanto, usted invierte mucho tiempo en gestionar las contraseñas y las identidades de los usuarios, así como en resolver los problemas que plantean, como los de restablecer contraseñas olvidadas.

Como administrador de la red de su empresa, siempre está pendiente de descubrir nuevas maneras de mejorar la empresa, empezando por el departamento de recepción de pedidos. Sabe que la mayoría de sus empleados necesitan el mismo tipo de autoridad para acceder a la aplicación que les permite consultar el estado del inventario. Le parece redundante, además de una pérdida de tiempo, la necesidad de mantener los perfiles de usuarios individuales y las numerosas contraseñas que se hacen servidor en esta situación. Sabe, además, que todos sus empleados saldrían beneficiados si se emplearan menos identificadores y contraseñas. Desea:

- Simplificar la tarea de gestión de contraseñas en el departamento de recepción de pedidos. Concretamente, desea gestionar de manera eficaz el acceso de los usuarios a la aplicación que sus empleados utilizan ordinariamente para los pedidos de los clientes.
- Disminuir la utilización de múltiples identificadores y contraseñas de usuario para los empleados del departamento y también para los administradores de la red. Sin embargo, no le interesa que los identificadores de Windows 2000 coincidan con los perfiles de usuario de i5/OS ni tampoco desea utilizar la memoria caché de contraseñas ni su sincronización.

Basándose en sus investigaciones, sabe que i5/OS permite el inicio de sesión único (SSO), solución que permite a sus usuarios conectarse una vez para acceder a múltiples aplicaciones y servicios, que normalmente les exigirían conectarse con múltiples identificadores y contraseñas de usuario. Dado que sus usuarios no necesitarían proporcionar tantos identificadores y contraseñas para realizar su trabajo, usted tendría menos problemas de contraseñas que resolver. El inicio de sesión único parece una solución idónea, porque le permite simplificar la gestión de las contraseñas de varias maneras:

- Para los usuarios habituales que necesitan la misma autorización sobre una aplicación, puede crear asociaciones de política. Por ejemplo, desea que los empleados que atienden los pedidos en el departamento de recepción de pedidos puedan iniciar sesión una sola vez con el nombre de usuario y la contraseña de Windows y luego acceder a una nueva aplicación de consulta del inventario del departamento de fabricación sin tener que autenticarse de nuevo. Sin embargo, también le interesa asegurarse de que poseen el debido nivel de autorización cuando utilizan esta aplicación. Para lograr este objetivo, decide crear una asociación de política que haga que las identidades de usuario de Windows 2000 de este grupo de usuarios se correlacionen con un solo perfil de usuario de i5/OS cuyo nivel de autorización sea el que se precisa para ejecutar la aplicación de consulta de inventario. Como esta es una aplicación solo de consulta, en la que los usuarios no pueden cambiar datos, no se preocupa de establecer para ella un proceso de auditoría detallado. Por lo tanto, se siente seguro de que la utilización de una asociación de política en estas circunstancias está en conformidad con su política de seguridad.

  Creará una asociación de política para que el grupo de empleados que atienden pedidos y poseen requisitos de autorización similares se correlacionen con un solo perfil de usuario de i5/OS que tenga el debido nivel de autorización sobre la aplicación de consulta del inventario. Sus usuarios se benefician de tener que recordar una contraseña menos y de iniciar una sesión menos. Como administrador, usted se beneficia de tener que mantener tan solo un perfil de usuario para el acceso de los usuarios a la aplicación, en lugar de múltiples perfiles de usuario para cada persona del grupo.
- Para cada uno de los administradores de la red cuyos perfiles de usuario tengan autorizaciones especiales, como *ALLOBJ y *SECADM, puede crear asociaciones de identificador. Por ejemplo, le interesa que todas las identidades de usuario de un administrador de la red se correlacionen de manera precisa e individual entre sí, debido al alto nivel de autorización del administrador.

Basándose en la política de seguridad de su compañía, decide crear asociaciones de identificador que correlacionen específicamente la identidad Windows de cada administrador de la red con el perfil de usuario de i5/OS del administrador. Le resultará más fácil supervisar y rastrear la actividad del administrador debido a la correlación biunívoca que proporcionan las asociaciones de identificadores. Por ejemplo, puede supervisar los trabajos y los objetos que se ejecutan en el sistema en relación con la identidad de un usuario concreto. El administrador de la red se beneficia de tener que recordar una contraseña menos y de iniciar una sesión menos. Como administrador de la red, usted se beneficia de poder ejercer un control minucioso de las relaciones entre las identidades de usuario de todos sus administradores.

Las ventajas de este caso práctico son:

- Simplifica el proceso de autenticación de los usuarios.
- Simplifica la gestión del acceso a las aplicaciones.
- Reduce la actividad adicional que supone gestionar el acceso a los sistemas de la red.
- Minimiza la amenaza de robo de contraseñas.
- Evita la necesidad de iniciar sesión múltiples veces.
- Simplifica la gestión de las identidades de los usuarios en la red.

Objetivos

En este caso práctico, usted es el administrador de la empresa MyCo, Inc., y desea habilitar el inicio de sesión único (SSO) en el departamento de recepción de pedidos.

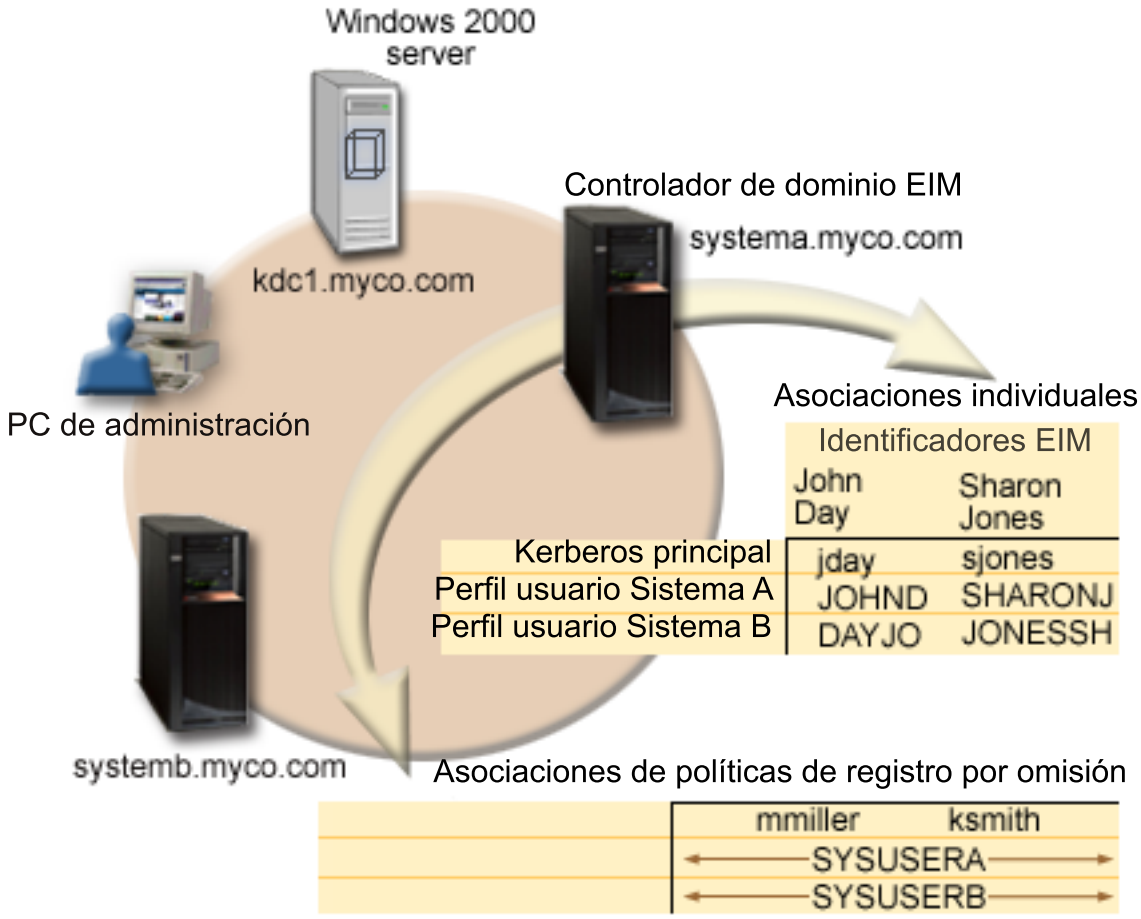
Los objetivos de este caso práctico son los siguientes:

- El sistema A y el sistema B deben participar en el reino MYCO.COM para autenticar a los usuarios y los servicios que participarán en este entorno de inicio de sesión único. Para habilitar los sistemas para que utilicen Kerberos, los sistemas A y B deben estar configurados para el servicio de autenticación de red.
- IBM Directory Server para i5/OS (LDAP) en el sistema A debe funcionar como controlador del nuevo dominio EIM.

  Nota: En el tema que trata sobre dominios se explica cómo dos tipos distintos de dominios, un dominio EIM y un dominio Windows 2000, encajan en el entorno de inicio de sesión único (SSO).
- Todas las identidades de usuario del registro Kerberos se deben correlacionar satisfactoriamente con un solo perfil de usuario de i5/OS que tenga la debida autorización de acceso de usuario a la aplicación de consulta del inventario.
- Basándose en la política de seguridad, dos administradores, John Day y Sharon Jones, que también tienen identidades de usuario en el registro Kerberos, deben tener asociaciones de identificador para correlacionar tales identidades con los correspondientes perfiles de usuario de i5/OS que tienen la autorización especial *SECADM. Estas correlaciones biunívocas le permiten supervisar minuciosamente los trabajos y los objetos que se ejecutan en el sistema en relación con esas identidades de usuario.
- Hay que utilizar un sujeto principal de servicio Kerberos para autenticar a los usuarios ante las aplicaciones de IBM System i Access para Windows, incluida la aplicación System i Navigator.

Detalles

La siguiente figura ilustra el entorno de red de este caso práctico.



En la figura se ilustran los puntos relevantes de este caso práctico que se indican a continuación.

Datos del dominio EIM definidos para la empresa

- Tres nombres de definición de registro:
  - Uno de ellos es el nombre MYCO.COM que define el registro del servidor Windows 2000. Lo definirá cuando utilice el asistente de configuración de EIM en el sistema A.
  - Un nombre de definición de registro de SYSTEMA.MYCO.COM para el registro de i5/OS en el sistema A. Lo definirá cuando utilice el asistente de configuración de EIM en el sistema A.
  - Un nombre de definición de registro de SYSTEMB.MYCO.COM para el registro de i5/OS en el sistema B. Lo definirá cuando utilice el asistente de configuración de EIM en el sistema B.
- Dos asociaciones de política de registro predeterminadas:

  Nota: El proceso de la operación de búsqueda EIM asigna la máxima prioridad a las asociaciones de identificador. Por lo tanto, cuando una identidad de usuario está definida como origen en una asociación de política y en una asociación de identificador, tan solo la asociación de identificador correlaciona la identidad de usuario. En este caso práctico, los dos administradores de la red, John Day y Sharon Jones, tienen sus identidades de usuario en el registro MYCO.COM, que es el origen de las asociaciones de política de registro predeterminadas. Sin embargo, tal como se

muestra a continuación, estos administradores también tienen definidas asociaciones de identificador para sus identidades de usuario en el registro MYCO.COM. Las asociaciones de identificador garantizan que las identidades de usuario de MYCO.COM no se correlacionen mediante las asociaciones de política. Por el contrario, las asociaciones de identificador garantizan que las identidades de usuario del registro MYCO.COM se correlacionen individualmente con otras identidades de usuario individuales concretas.

  - Una asociación de política de registro predeterminada hace que todas las identidades de usuario del registro de servidor Windows 2000, que se llama MYCO.COM, se correlacionen con un so lo perfil de usuario de i5/OS, que se llama SYSUSERA, en el registro SYSTEMA.MYCO.COM del sistema A. En este caso práctico, mmiller y ksmith representan dos de estas identidades de usuario.
  - Una asociación de política de registro predeterminada hace que todas las identidades de usuario del registro de servidor Windows 2000, que se llama MYCO.COM, se correlacionen con un so lo perfil de usuario de i5/OS, que se llama SYSUSERB, en el registro SYSTEMB.MYCO.COM del sistema B. En este caso práctico, mmiller y ksmith representan dos de estas identidades de usuario.
- Dos identificadores EIM, que son John Day y Sharon Jones, para representar a los dos administradores de la red de la compañía que tienen esos nombres.
- Para el identificador EIM de John Day, se definen estas asociaciones de identificador:
  - Una asociación origen para la identidad de usuario jday, que es un sujeto principal Kerberos del registro del servidor Windows 2000.
  - Una asociación destino para la identidad de usuario JOHND, que es un perfil de usuario del registro i5/OS en el sistema A.
  - Una asociación destino para la identidad de usuario DAYJO, que es un perfil de usuario del registro i5/OS en el sistema B.
- Para el identificador EIM de Sharon Jones, se definen estas asociaciones de identificador:
  - Una asociación origen para la identidad de usuario sjones, que es un sujeto principal Kerberos del registro del servidor Windows 2000.
  - Una asociación destino para la identidad de usuario SHARONJ, que es un perfil de usuario del registro i5/OS en el sistema A.
  - Una asociación destino para la identidad de usuario JONESSH, que es un perfil de usuario del registro i5/OS en el sistema B.

Servidor **Windows 2000**

- Funciona a modo de servidor Kerberos (`kdc1.myco.com`), que también se conoce como centro de distribución de claves (KDC), en la red.
- El reino predeterminado del servidor Kerberos es `MYCO.COM`.
- Todos los usuarios de Microsoft Active Directory que no tienen asociaciones de identificador se correlacionan con un solo perfil de usuario i5/OS en cada uno de las plataformas System i.

Sistema A

- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3

Nota: Puede implementar este caso práctico con un sistema que ejecute OS/400 V5R2. No obstante, algunos de los pasos de configuración son algo distintos. Además, este caso práctico hace una demostración de algunas funciones del inicio de sesión único (SSO) que sólo están disponibles en i5/OS V5R3 y posteriores, como por ejemplo las asociaciones de política.

- El servidor de directorio del sistema A se configurará para que funcione como controlador de dominio EIM del nuevo dominio EIM, MyCoEimDomain.
- Participa en el dominio EIM, MyCoEimDomain.
- Su nombre de sujeto principal de servicio es `krbsvr400/systema.myco.com@MYCO.COM`.
- Su nombre de host totalmente calificado es `systema.myco.com`. Este nombre se registra en un sistema de nombres de dominio (DNS) individual hacia el que señalan todos los PC y servidores de la red.
- En los directorios iniciales del sistema A se almacenan la memoria caché de credenciales Kerberos de los perfiles de usuario de i5/OS.

Sistema B
- Ejecuta i5/OS V5R3 o posterior con los siguientes programas y opciones bajo licencia instalados:
  - i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12)
  - Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30)
  - System i Access para Windows (5722-XE1 o 5761-XE1)
  - Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior
  - Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3
- Su nombre de host totalmente calificado es `systemb.myco.com`. Este nombre se registra en un sistema de nombres de dominio (DNS) individual hacia el que señalan todos los PC y servidores de la red.
- El nombre de sujeto principal del sistema B es `krbsvr400/systemb.myco.com@MYCO.COM`.
- Participa en el dominio EIM, MyCoEimDomain.
- En los directorios iniciales del sistema B se almacenan la memoria caché de credenciales Kerberos de los perfiles de usuario de i5/OS.

PC administrativo
- Ejecuta el sistema operativo Microsoft Windows 2000.
- Ejecuta System i Access para Windows (5722-XE1 o 5761-XE1).
- Ejecuta System i Navigator y tiene instalados los siguientes subcomponentes:
  - Red
  - Seguridad
  - Usuarios y grupos
- Funciona como sistema de inicio de sesión primario para el administrador.
- Está configurado para formar parte del reino MYCO.COM (dominio Windows.

Prerrequisitos y supuestos

Para la implementación satisfactoria de este caso práctico, deben satisfacerse los siguientes prerrequisitos y supuestos:

1. Se han verificado todos los requisitos del sistema, incluida la instalación del sistema operativo y el software.

   Para verificar que se han instalado estos programas bajo licencia, siga estos pasos:

   a. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Software** → **Productos instalados**.

   b. Ahora puede asegurarse de que se han instalado todos los programas bajo licencia necesarios.

   Nota: Las API del servicio de autenticación de red soportan entornos de trabajos para la mayor parte de los EBCDIC CCSID. Sin embargo, los CCSID 290 y 5026 no están soportados debido a la variación de letras minúsculas de la ″a″ a la ″z″.
2. Se ha llevado a cabo todo el proceso de planificación e instalación del hardware necesario.
3. El protocolo TCP/IP y la seguridad básica del sistema se han configurado y probado en cada sistema.

4. El servidor de directorio y EIM no deben haberse configurado con anterioridad en el sistema A.

   Nota: Las instrucciones de este caso práctico se basan en el supuesto de que el servidor de directorios todavía no está configurado en el sistema A. Sin embargo, en el caso de que ya haya configurado el servidor de directorio, todavía podrá seguir estas instrucciones con algunas diferencias. Las diferencias se indican en los lugares pertinentes de los pasos de configuración.
5. Se utiliza un solo servidor DNS para la resolución de nombres de host en la red. No se utilizan tablas de hosts para la resolución de nombres de host.

   Nota: Si se utilizan tablas de hosts junto con la autenticación Kerberos, podrían producirse errores en la resolución de nombres u otros problemas. Si desea información más detallada sobre cómo funciona la resolución de nombres de host con la autenticación Kerberos, consulte el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.

Pasos de configuración

Antes de implementar este escenario, es necesario que conozca los conceptos relacionados con el inicio de sesión único, entre ellos, el servicio de autenticación de red y la correlación de identidades de empresa (EIM). Para obtener información sobre los términos y conceptos relacionados con el inicio de sesión único (SSO), consulte estos temas:

- Conceptos de la correlación de identidades de empresa (EIM)
- Conceptos del servicio de autenticación de red

Para configurar el inicio de sesión único (SSO), lleve a cabo los pasos siguientes.

Conceptos relacionados

Visión general de inicio de sesión único

Dominios

Cumplimentar las hojas de trabajo de planificación

Estas hojas de trabajo pretenden hacer una demostración de la información que tendrá que reunir y de las decisiones que deberá tomar cuando se disponga a configurar la función del inicio de sesión único descrita en este caso práctico.

Las siguientes hojas de trabajo de planificación se han elaborado de acuerdo con este caso práctico tomando como base las hojas de trabajo de planificación del inicio de sesión único (SSO) en general. Para garantizar una implementación satisfactoria, deberá poder responder afirmativamente a todas las preguntas relacionadas con los prerrequisitos de la hoja de trabajo y reunir toda la información necesaria para cumplimentar las hojas de trabajo antes de realizar las tareas de configuración.

Nota: Las API del servicio de autenticación de red soportan entornos de trabajos para la mayor parte de los EBCDIC CCSID. Sin embargo, los CCSID 290 y 5026 no están soportados debido a la variación de letras minúsculas de la ″a″ a la ″z″.

Tabla 13. Hoja de trabajo de prerrequisitos para el inicio de sesión único (SSO)

Hoja de trabajo de prerrequisitos	Respuestas
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1)?	Sí

Tabla 13. Hoja de trabajo de prerrequisitos para el inicio de sesión único (SSO) (continuación)

Hoja de trabajo de prerrequisitos	Respuestas
¿Tiene instalados los siguientes programas y opciones bajo licencia en los sistemas A y B? • i5/OS Host Servers (5722-SS1 Opción 12 o 5761-SS1 Opción 12) • Qshell Interpreter (5722-SS1 Opción 30 o 5761-SS1 Opción 30) • System i Access para Windows (5722-XE1 o 5761-XE1) • Network Authentication Enablement (5722-NAE o 5761-NAE) si utiliza i5/OS V5R4 o posterior • Cryptographic Access Provider (5722-AC3) si ejecuta i5/OS V5R3	Sí
¿Ha instalado una aplicación habilitada para el inicio de sesión único en cada uno de los PC que participarán en el entorno de inicio de sesión único? **Nota:** En este caso práctico, todos los PC participantes tienen instalado System i Access para Windows (5722-XE1 o 5761-XE1).	Sí
¿Está instalado System i Navigator en el PC del administrador? • ¿Esta el subcomponente de red de System i Navigator instalado en el PC que servirá para administrar el inicio de sesión único? • ¿Esta el subcomponente de seguridad de System i Navigator instalado en el PC que servirá para administrar el inicio de sesión único? • ¿Esta el subcomponente de usuarios y grupos de System i Navigator instalado en el PC que servirá para administrar el inicio de sesión único?	Sí
¿Ha instalado el último Service Pack de System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	Sí
¿Tiene el administrador del inicio de sesión único las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG?	Sí
¿Funciona alguno de los siguientes sistemas a modo de servidor Kerberos (que también se conoce como KDC)? Si es así, indique qué sistema. 1. Microsoft Windows 2000 Server **Nota:** Microsoft Windows 2000 Server utiliza la autenticación Kerberos como mecanismo de seguridad predeterminado. 2. Windows Server 2003 3. i5/OS PASE (V5R3 o posterior) 4. Servidor AIX 5. z/OS	Sí, Windows 2000 Server
¿Están todos los PC de la red configurados en un dominio Windows 2000?	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	Sí

Necesita esta información para configurar EIM y el servicio de autenticación de red en el sistema A.

Tabla 14. Hoja de trabajo para planificar la configuración del inicio de sesión único en el sistema A

Hoja de trabajo del plan de configuración en el sistema A	**Respuestas**
Utilice la siguiente información para cumplimentar las páginas del asistente de configuración de EIM. La información de esta hoja de trabajo se correlaciona con la que necesitará suministrar en cada página del asistente:	
¿Cómo desea configure EIM en su sistema? • Unirse a un dominio existente • Crear un dominio nuevo para unirse a él	Crear un dominio nuevo para unirse a él
¿Dónde desea configurar el dominio EIM?	En el servidor de directorio local **Nota:** Esto hará que el servidor de directorio se configure en el sistema en el que está configurando EIM.
¿Desea configurar el servicio de autenticación de red? **Nota:** Para configurar el inicio de sesión único, debe configurar el servicio de autenticación de red.	Sí
El asistente del servicio de autenticación de red se inicia desde el asistente de configuración de EIM. Utilice la siguiente información para cumplimentar las páginas del asistente del servicio de autenticación de red.	
¿Cuál es el nombre del reino Kerberos predeterminado al que pertenecerá el producto System i? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	`MYCO.COM`
¿Está utilizando Microsoft Active Directory?	Sí
¿Qué servidor Kerberos (que también se conoce como centro de distribución de claves (KDC)) utiliza para este reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	**KDC:** `kdc1.myco.com` **Puerto:** `88` **Nota:** Este es el puerto predeterminado del servidor Kerberos.
¿Desea configurar un servidor de contraseñas para este reino predeterminado? Si es así, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este servidor Kerberos? ¿En qué puerto está a la escucha el servidor de contraseñas?	Sí **Servidor de contraseñas:** `kdc1.myco.com` **Puerto:** `464` **Nota:** Este es el puerto predeterminado del servidor de contraseñas.
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	Autenticación Kerberos i5/OS
¿Qué contraseña utilizará para los sujetos principales de servicio (uno o varios)?	`systema123`
Desea crear un archivo por lotes para automatizar la adición de sujetos principales de servicio del sistema A al registro Kerberos?	Sí
¿Desea incluir las contraseñas con los sujetos principales de servicio de i5/OS en el archivo por lotes?	Sí
Cuando salga del asistente del servicio de autenticación de red, volverá al asistente de configuración de EIM. Utilice la siguiente información para cumplimentar las páginas del asistente de configuración de EIM:	

Tabla 14. Hoja de trabajo para planificar la configuración del inicio de sesión único en el sistema A (continuación)

Hoja de trabajo del plan de configuración en el sistema A	Respuestas
Especifique la información de usuario que el asistente debe utilizar al configurar el servidor de directorio. Se trata del usuario de conexión. Debe especificar el número de puerto, el nombre distinguido del administrador y una contraseña para el administrador. **Nota:** Especifique el nombre distinguido (DN) del administrador de LDAP y su contraseña para asegurar que el asistente tiene autorización suficiente para administrar el dominio EIM y los objetos que hay en él.	**Puerto:** `389` **Nombre distinguido:** `cn=administrator` **Contraseña:** `mycopwd`
¿Cuál es el nombre del dominio EIM que desea crear?	`MyCoEimDomain`
¿Desea especificar un DN padre para el dominio EIM?	No
¿Qué registros de usuarios desea añadir al dominio EIM?	i5/OS local--SYSTEMA.MYCO.COM Kerberos--KDC1.MYCO.COM **Nota:** Cuando el asistente le presente la opción **Las identidades de usuario Kerberos distinguen entre mayúsculas/minúsculas**, no debe seleccionarla.
¿Qué usuario de EIM desea que utilice el sistema A al realizar operaciones de EIM? Este es el usuario del sistema. **Nota:** Si no ha configurado el servidor de directorio antes de configurar el inicio de sesión único, el único nombre distinguido (DN) que puede proporcionar para el usuario del sistema es el DN del administrador de LDAP y su contraseña.	**Tipo de usuario:** `Nombre distinguido` **Nombre distinguido:** `cn=administrator` **Contraseña:** `mycopwd`

Necesita esta información para permitir que el sistema B participe en el dominio EIM y para configurar el servicio de autenticación de red en el sistema B.

Tabla 15. Hoja de trabajo para planificar la configuración del inicio de sesión único en el sistema B

Hoja de trabajo del plan de configuración en el sistema B	Respuestas
Utilice la siguiente información para cumplimentar las páginas del asistente de configuración de EIM para el sistema B:	
¿Cómo desea configurar EIM en su sistema?	Unirse a un dominio existente
¿Desea configurar el servicio de autenticación de red? **Nota:** Para configurar el inicio de sesión único, debe configurar el servicio de autenticación de red.	Sí
El asistente del servicio de autenticación de red se inicia desde el asistente de configuración de EIM. Utilice la siguiente información para cumplimentar las páginas del asistente del servicio de autenticación de red: **Nota:** Puede iniciar el asistente del servicio de autenticación de red con independencia del asistente de configuración de EIM.	
¿Cuál es el nombre del reino Kerberos predeterminado al que pertenecerá el producto System i? **Nota:** Los dominios en Windows 2000 equivalen a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	`MYCO.COM`
¿Está utilizando Microsoft Active Directory?	Sí
¿Cuál es el servidor Kerberos del reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	**KDC:** `kdc1.myco.com` **Puerto:** `88` **Nota:** Este es el puerto predeterminado del servidor Kerberos.

Tabla 15. Hoja de trabajo para planificar la configuración del inicio de sesión único en el sistema B (continuación)

Hoja de trabajo del plan de configuración en el sistema B	Respuestas
¿Desea configurar un servidor de contraseñas para este reino predeterminado? Si es así, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este servidor Kerberos? ¿En qué puerto está a la escucha el servidor de contraseñas?	Sí **Servidor de contraseñas:** `kdc1.myco.com` **Puerto:** `464` **Nota:** Este es el puerto predeterminado del servidor de contraseñas.
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	Autenticación de Kerberos de i5/OS
¿Qué contraseña utilizará para los sujetos principales de servicio de i5/OS?	systemb123
Desea crear un archivo por lotes para automatizar la adición de sujetos principales de servicio del sistema B al registro Kerberos?	Sí
¿Desea incluir las contraseñas con los sujetos principales de servicio de i5/OS en el archivo por lotes?	Sí
Cuando salga del asistente del servicio de autenticación de red, volverá al asistente de configuración de EIM. Utilice la siguiente información para cumplimentar las páginas del asistente de configuración de EIM para el sistema B:	
¿Cuál es el nombre del controlador de dominio EIM del dominio EIM al que desea unirse?	systema.myco.com
¿Piensa proteger la conexión con SSL o TLS?	No
¿En qué puerto está a la escucha el controlador de dominio EIM?	389
¿Qué usuario desea utilizar para conectarse al controlador de dominio? Se trata del usuario de conexión. **Nota:** Especifique el nombre distinguido (DN) del administrador de LDAP y su contraseña para asegurar que el asistente tiene autorización suficiente para administrar el dominio EIM y los objetos que hay en él.	**Tipo de usuario:** `Nombre distinguido y contraseña` **Nombre distinguido:** `cn=administrator` **Contraseña:** `mycopwd`
¿Cuál es el nombre del dominio EIM al que desea unirse?	`MyCoEimDomain`
¿Desea especificar un DN padre para el dominio EIM?	No
¿Cuál es el nombre del registro de usuarios que desea añadir al dominio EIM?	i5/OS local--SYSTEMB.MYCO.COM
¿Qué usuario de EIM desea que utilice el sistema B al realizar operaciones de EIM? Este es el usuario del sistema. **Nota:** Anteriormente, en este caso práctico ha utilizado el asistente de configuración de EIM para configurar el servidor de directorios en el sistema A. Al hacerlo, ha creado un nombre distinguido (DN) y una contraseña para el administrador de LDAP. Ese es actualmente el único DN definido para el servidor de directorio. Por lo tanto, esos son el DN y la contraseña que debe suministrar aquí.	**Tipo de usuario:** `Nombre distinguido y contraseña` **Nombre distinguido:** `cn=administrator` **Contraseña:** `mycopwd`

Tabla 16. Hoja de trabajo para planificar la configuración del inicio de sesión único - perfiles de usuario

Nombre de perfil de usuario de i5/OS	Se especifica contraseña	Autorización especial (clase de privilegio)	Sistema
SYSUSERA	No	Usuario	Sistema A

Tabla 16. Hoja de trabajo para planificar la configuración del inicio de sesión único - perfiles de usuario (continuación)

Nombre de perfil de usuario de i5/OS	Se especifica contraseña	Autorización especial (clase de privilegio)	Sistema
SYSUSERB	No	Usuario	Sistema B

Tabla 17. Hoja de trabajo para planificar la configuración del inicio de sesión único - datos de dominio EIM

Nombre de identificador	Registro de usuarios	Identidad de usuario	Tipo de asociación	Descripción de identificador
John Day	MYCO.COM	jday	Origen	Identidad de usuario de inicio de sesión Kerberos (Windows 2000)
John Day	SYSTEMA.MYCO.COM	JOHND	Destino	Perfil de usuario de i5/OS en el sistema A
John Day	SYSTEMB.MYCO.COM	DAYJO	Destino	Perfil de usuario de i5/OS en el sistema B
Sharon Jones	MYCO.COM	sjones	Origen	Identidad de usuario de inicio de sesión Kerberos (Windows 2000)
Sharon Jones	SYSTEMA.MYCO.COM	SHARONJ	Destino	Perfil de usuario de i5/OS en el sistema A
Sharon Jones	SYSTEMB.MYCO.COM	JONESSH	Destino	Perfil de usuario de i5/OS en el sistema B

Tabla 18. Hoja de trabajo para planificar la configuración del inicio de sesión único - datos de dominio EIM - asociaciones de política

Tipo de asociación de política	Registro de usuarios origen	Registro de usuarios destino	Identidad de usuario	Descripción
Registro predeterminado	MYCO.COM	SYSTEMA.MYCO.COM	SYSUSERA	Correlaciona un usuario de Kerberos autenticado con el perfil de usuario i5/OS pertinente
Registro predeterminado	MYCO.COM	SYSTEMB.MYCO.COM	SYSUSERB	Correlaciona un usuario de Kerberos autenticado con el perfil de usuario i5/OS pertinente

Crear una configuración básica de inicio de sesión único para el sistema A

El asistente de configuración de EIM le ayudará a crear la configuración básica de EIM. También abrirá el asistente del servicio de autenticación de red para permitirle crear una configuración básica del servicio de autenticación de red.

Nota: Las instrucciones de este caso práctico se basan en el supuesto de que el servidor de directorio todavía no está configurado en el sistema A. Sin embargo, en el caso de que ya haya configurado el servidor de directorio, todavía podrá seguir estas instrucciones con algunas diferencias. Las diferencias se indican en los lugares pertinentes de los pasos de configuración.

Utilice la información de las hojas de trabajo para configurar EIM y el servicio de autenticación de red en el sistema A. Cuando haya completado este paso, habrá realizado las siguientes tareas:

- Crear un dominio EIM nuevo.
- Configurar el servidor de directorio en el sistema A para que funcione como controlador de dominio EIM.
- Configurar el servicio de autenticación de red.
- Crear definiciones de registro EIM para el registro de i5/OS y el registro de Kerberos en el sistema A.
- Configurar el sistema A para que participe en el dominio EIM.

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)**.
2. Pulse **Configuración** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración de EIM.
3. En la página de bienvenida, seleccione **Crear y unirse a un dominio nuevo**. Pulse **Siguiente**.
4. En la página Especificar ubicación de dominio EIM, seleccione **En el servidor de directorio local**. Pulse **Siguiente**.
5. Lleve a cabo estas tareas para configurar el servicio de autenticación de red:
   a. En la página Configurar servicio de autenticación de red, seleccione **Sí**.

      Nota: Se iniciará el asistente del servicio de autenticación de red. Con este asistente, podrá configurar varias interfaces y servicios de i5/OS para participar en el reino Kerberos.

   b. En la página Especificar información de reino, escriba `MYCO.COM` en el campo **Reino predeterminado** y seleccione **Se utiliza Microsoft Active Directory para la autenticación Kerberos**. Pulse **Siguiente**.
   c. En la página Especificar información de KDC, escriba `kdc1.myco.com` para el nombre del servidor Kerberos en el campo **KDC** y teclee `88` en el campo **Puerto**. Pulse **Siguiente**.
   d. En el campo Especificar información de servidor de contraseñas, seleccione **Sí**. Entre `kdc1.myco.com` en el campo **Servidor de contraseñas** y `464` en el campo **Puerto**. Pulse **Siguiente**.
   e. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. Pulse **Siguiente**.
   f. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña, confírmela y pulse **Siguiente**. Por ejemplo, `systema123`. Esta contraseña se utilizará cuando se añada el sujeto principal de servicio del sistema A al servidor Kerberos.
   g. En la página Crear archivo por lotes, seleccione **Sí**, especifique la siguiente información y pulse **Siguiente**:
      - **Archivo por lotes:** añada el texto `systema` al final del nombre del archivo por lotes predeterminado, por ejemplo, `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystema.bat`.
      - Seleccione **Incluir contraseña**. Así se asegura de que todas las contraseñas asociadas al sujeto principal de servicio de i5/OS se incluyen en el archivo por lotes. Es importante que se fije en que las contraseñas se visualizan en texto sin cifrar y que pueden leerlas todas las personas que tengan acceso de lectura al archivo por lotes. Por ello, le recomendamos que suprima el archivo por lotes del servidor Kerberos y de su PC inmediatamente después de haberlo utilizado.

        Nota: Si no la incluye ahora, se le solicitará la contraseña cuando se ejecute el archivo por lotes.

   h. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.
6. En la página Configurar servidor de directorio, escriba la siguiente información y pulse **Siguiente**:

   Notas:

- Si configuró el servidor de directorio antes de empezar este caso práctico, verá la página Especificar usuario para conexión en lugar de la página Configurar servidor de directorio. En ese caso, debe especificar el nombre distinguido y la contraseña del administrador de LDAP.
- Si ha configurado varios servidores de directorio en sistemas en los que se ejecuta i5/OS V6R1, verá las páginas Especificar instancias de servidor de directorio y Especificar usuario para conexión. En este caso, debe especificar los nombres distinguidos y las contraseñas del administrador de LDAP.

- **Puerto**: `389`
- **Nombre distinguido**: `cn=administrator`
- **Contraseña:** `mycopwd`

7. En la página Especificar dominio, escriba el nombre del dominio en el campo **Dominio**. Por ejemplo, `MyCoEimDomain`.
8. En la página Especificar DN padre para dominio, seleccione **No**. Pulse **Siguiente**.

   Nota: Si el servidor de directorio está activo, se visualiza un mensaje que indica que debe finalizar el servidor de directorio y reiniciarlo para que los cambios entren en vigor. Pulse **Sí** para reiniciar el servidor de directorio.
9. En la página Información de registro, seleccione **i5/OS local** y **Kerberos**. Pulse **Siguiente**. Anote los nombres del registro. Los necesitará cuando cree asociaciones para los identificadores EIM.

   Notas:
   - Los nombres de registro deben ser exclusivos en el dominio.
   - Puede escribir un nombre de definición de registro específico para el registro de usuarios si desea utilizar un plan de denominación de definición de registro específico. Sin embargo, en lo que se refiere a este caso práctico, puede aceptar los valores predeterminados.
10. En la página Especificar usuario del sistema EIM, seleccione el usuario que el sistema operativo utiliza al efectuar operaciones EIM en nombre de las funciones del sistema operativo; después pulse **Siguiente**:

    Nota: Dado que no configuró el servidor de directorio antes de seguir los pasos de este caso práctico, el único nombre distinguido (DN) que puede elegir es el DN del administrador de LDAP.
    - **Tipo de usuario**: `Nombre distinguido y contraseña`
    - **Nombre distinguido**: `cn=administrator`
    - **Contraseña**: `mycopwd`
11. En la página **Resumen**, confirme la información de configuración de EIM. Pulse **Finalizar**.

Configurar el sistema B para que participe en el dominio EIM y configurar el sistema B para el servicio de autenticación de red

Después de crear un dominio nuevo y configurar el servicio de autenticación de red en el sistema A, es necesario configurar el sistema B para que participe en el dominio EIM y configurar el servicio de autenticación de red en el sistema B.

Utilice la información de las hojas de trabajo para llevar a cabo este paso.

1. En System i Navigator, expanda **Sistema B** → **Red** → **Correlación de identidades de empresa (EIM)**.
2. Pulse **Configuración** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración.
3. En la página de bienvenida, seleccione **Unirse a un dominio existente**. Pulse **Siguiente**.
4. Lleve a cabo las tareas de configuración del servicio de autenticación de red.

a. En la página Configurar servicio de autenticación de red, seleccione **Sí**.

   Nota: Se iniciará el asistente del servicio de autenticación de red. Con este asistente podrá configurar varias interfaces y servicios de i5/OS para participar en una red Kerberos.

b. En la página Especificar información de reino, escriba `MYCO.COM` en el campo **Reino predeterminado** y seleccione **Se utiliza Microsoft Active Directory para la autenticación Kerberos**. Pulse **Siguiente**.

c. En la página Especificar información de KDC, escriba `kdc1.myco.com` para el nombre del servidor Kerberos en el campo **KDC** y teclee `88` en el campo **Puerto**. Pulse **Siguiente**.

d. En el campo Especificar información de servidor de contraseñas, seleccione **Sí**. Entre `kdc1.myco.com` en el campo **Servidor de contraseñas** y `464` en el campo **Puerto**. Pulse **Siguiente**.

e. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. Pulse **Siguiente**.

f. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña, confírmela y pulse **Siguiente**, por ejemplo, escriba `systema123`. Esta contraseña se utilizará cuando se añada el sujeto principal de servicio del sistema A al servidor Kerberos.

g. Opcional: En la página Crear archivo por lotes, seleccione **Sí**, especifique la siguiente información y pulse **Siguiente**:

   - **Archivo por lotes:** añada el texto `systemb` al final del nombre del archivo por lotes predeterminado. Por ejemplo, escriba `C:\Documents and Settings\All Users\Documents\IBM\Client Access\NASConfigsystemb.bat`.
   - Seleccione **Incluir contraseña**. Así se asegura de que todas las contraseñas asociadas al sujeto principal de servicio de i5/OS se incluyen en el archivo por lotes. Es importante que se fije en que las contraseñas se visualizan en texto sin cifrar y que pueden leerlas todas las personas que tengan acceso de lectura al archivo por lotes. Por ello, le recomendamos que suprima el archivo por lotes del servidor Kerberos y de su PC inmediatamente después de haberlo utilizado.

     Nota: Si no la incluye ahora, se le solicitará la contraseña cuando se ejecute el archivo por lotes.

h. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.

5. En la página Especificar controlador de dominio, especifique la siguiente información y pulse **Siguiente**:
   - **Nombre de controlador de dominio**: `systema.myco.com`
   - **Puerto**: `389`
6. En la página Especificar usuario para conexión, especifique la siguiente información y pulse **Siguiente**:

   Nota: Especifique el DN del administrador de LDAP y la contraseña que creó anteriormente en este caso práctico en el sistema A.

   a. **Tipo de usuario**: `Nombre distinguido y contraseña`
   b. **Nombre distinguido**: `cn=administrator`
   c. **Contraseña**: `mycopwd`
7. En la página Especificar dominio, seleccione el nombre del dominio al que desea unirse. Pulse **Siguiente**. Por ejemplo, `MyCoEimDomain`.
8. En la página Información de registro, seleccione **i5/OS local** y deseleccione **Registro Kerberos** (el registro Kerberos se creó al crear el dominio MyCoEimDomain). Pulse **Siguiente**. Anote los nombres del registro. Los necesitará cuando cree asociaciones para los identificadores EIM.

   Notas:

- Los nombres de registro deben ser exclusivos en el dominio.
- Puede escribir un nombre de definición de registro específico para el registro de usuarios si desea utilizar un plan de denominación de definición de registro específico. Sin embargo, en lo que se refiere a este caso práctico, puede aceptar los valores predeterminados.

9. En la página Especificar usuario del sistema EIM, seleccione el usuario que el sistema operativo utiliza al efectuar operaciones EIM en nombre de las funciones del sistema operativo; después pulse **Siguiente**:

   Nota: Especifique el DN del administrador de LDAP y la contraseña que creó anteriormente en este caso práctico en el sistema A.

   a. **Tipo de usuario**: `Nombre distinguido y contraseña`
   b. **Nombre distinguido**: `cn=administrator`
   c. **Contraseña**: `mycopwd`
10. En la página Resumen, confirme la configuración de EIM. Pulse **Finalizar**.

Añadir ambos sujetos principales de servicio de i5/OS al servidor Kerberos

Puede añadir manualmente los sujetos principales de servicio de i5/OS necesarios al servidor Kerberos. Tal como se ilustra en este caso práctico, también puede utilizar un archivo por lotes para añadirlos.

Este archivo por lotes se creó en el paso 2. Para utilizar el archivo, puede servirse del protocolo de transferencia de archivos (FTP) para copiar el archivo en el servidor Kerberos y ejecutarlo.

Para utilizar el archivo por lotes para añadir nombres de sujeto principal al servidor Kerberos, siga estos pasos:

1. Crear archivos por lotes FTP
   a. En la estación de trabajo Windows 2000 empleada por el administrador para configurar el servicio de autenticación de red, abra un indicador de mandatos y teclee `ftp kdc1.myco.com`. Así se iniciará una sesión FTP en su PC. Se le pedirá el nombre de usuario y la contraseña de administrador.
   b. En el indicador FTP, teclee `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Pulse Intro. Debe recibir el mensaje `Directorio local es ahora C:\Documents and Settings\All Users\Documents\IBM\Client Access`.
   c. En el indicador FTP, teclee `cd \`*`midirectorio`*, siendo *midirectorio* un directorio de kdc1.myco.com.
   d. En el indicador FTP, teclee `put NASConfigsystema.bat`. Debe recibir el mensaje: `226 Transferencia completada`.
   e. Teclee `quit` para salir de la sesión FTP.
2. Ejecute ambos archivos por lotes en kdc1.myco.com
   a. En el servidor Windows 2000, abra el directorio al que ha transferido los archivos por lotes.
   b. Localice el archivo `NASConfigsystema.bat` y púlselo dos veces para ejecutarlo.
   c. Repita los pasos comprendidos entre 1a y 2b para `NASConfigsystemb.bat`.
   d. Una vez ejecutado cada archivo, verifique que el sujeto principal de i5/OS se ha añadido al servidor Kerberos; para ello, siga estos pasos:
      1) En el servidor Windows 2000, expanda **Herramientas administrativas** → **Usuarios y equipos de Active Directory** → **Usuarios**.
      2) Verifique que la plataforma System i tiene una cuenta de usuario seleccionando el dominio Windows 2000 pertinente.

         Nota: Este dominio de Windows 2000 debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.
      3) En la lista de usuarios visualizada, localice **systema_1_krbsvr400** e **systemb_1_krbsvr400**. Se trata de las cuentas de usuario generadas para el nombre de sujeto principal de i5/OS.

4) Acceda a las propiedades de los usuarios de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**.

   Nota: Este paso opcional permite que su sistema delegue, o reenvíe, las credenciales de un usuario a otros sistemas. Como resultado, el sujeto principal de servicio de i5/OS podrá acceder a los servicios en múltiples sistemas en nombre del usuario. Esto resulta útil en una red multinivel.

Crear los perfiles de usuario en los sistemas A y B

Le interesa que todos los usuarios del registro Kerberos MYCO.COM se correlacionen con un solo perfil de usuario i5/OS en cada uno de las plataformas System i. Por lo tanto, tendrá que crear un perfil de usuario i5/OS en los sistemas A y B.

Para crear un perfil para estos usuarios, utilice la información de las hojas de trabajo:

1. En System i Navigator, expanda **Sistema A** → **Usuarios y grupos**.
2. Pulse **Todos los usuarios** con el botón derecho del ratón y seleccione **Usuario nuevo**.
3. En el recuadro de diálogo **Usuario nuevo**, escriba `SYSUSERA` en el campo **Nombre de usuario**.
4. En el campo **Contraseña**, seleccione **Sin contraseña (inicio de sesión no permitido)**.
5. Pulse **Posibilidades**.
6. En la página Privilegios, seleccione **Usuario** en el campo **Clase de privilegio**. Pulse **Aceptar** y después **Añadir**.
7. Repita los pasos comprendidos entre 1 y 6 en el sistema B, pero ahora escriba `SYSUSERB` en el campo **Nombre de usuario**.

Crear los directorios iniciales en los sistemas A y B

Cada usuario que se conecte al i5/OS y a las aplicaciones del i5/OS necesitará un directorio en el directorio /home (directorio inicial). En este directorio se almacena la memoria caché de credenciales Kerberos del usuario.

Para crear un directorio inicial para un usuario, siga estos pasos:

1. En la línea de mandatos del sistema A, escriba `CRTDIR '/home/perfil usuario'`, siendo `perfil usuario` el nombre del perfil i5/OS del usuario. Por ejemplo: `CRTDIR '/home/SYSUSERA'`.
2. Repita este mandato en el sistema B, pero ahora especifique `SYSUSERB` con vistas a crear un directorio inicial para el perfil de usuario en el sistema B.

Probar el servicio de autenticación de red en los sistemas A y B

Una vez concluidas las tareas de configuración del servicio de autenticación de red en ambos sistemas, tendrá que verificar que las configuraciones funcionan correctamente en los sistemas A y B.

Para probar las configuraciones, puede seguir los pasos que se indican a continuación, donde se solicita un ticket de otorgamiento de tickets para los sujetos principales de los sistemas A y B:

Nota: Antes de llevar a cabo este procedimiento, asegúrese de que ha creado un directorio inicial para su perfil de usuario i5/OS.

1. En una línea de mandatos del intérprete Qshell, escriba `QSH` para iniciar el intérprete Qshell.
2. Entre `keytab list` para visualizar una lista de los sujetos principales registrados en el archivo de tabla de claves. En este caso práctico, se debe visualizar krbsvr400/systema.myco.com@MYCO.COM como nombre de sujeto principal del sistema A.
3. Escriba `kinit -k krbsvr400/systema.myco.com@MYCO.COM` para solicitar un ticket de otorgamiento de tickets al servidor Kerberos. La ejecución de este mandato le permite verificar que el sistema está debidamente configurado y que la contraseña del archivo de tabla de claves concuerda con la almacenada en el servidor Kerberos. Si la verificación es satisfactoria, el mandato kinit mostrará que no hay errores.

4. Escriba `klist` para verificar que el sujeto principal predeterminado es krbsvr400/systema.myco.com@MYCO.COM. Este mandato visualiza el contenido de una memoria caché de credenciales Kerberos y verifica que se ha creado un ticket válido para el sujeto principal de servicio de i5/OS y que se ha colocado en la memoria caché de credenciales del sistema.

```
 Memoria caché de tickets: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Sujeto principal predeterminado: krbsvr400/systema.myco.com@MYCO.COM

Servidor: krbtgt/MYCO.COM@MYCO.COM
  Válido del 200X/06/09-12:08:45 al 20XX/11/05-03:08:45
$
```

Crear identificadores EIM para los dos administradores, John Day y Sharon Jones

Como parte de la configuración del entorno de prueba del inicio de sesión único, necesita crear identificadores EIM para dos de los administradores, de modo que los dos puedan iniciar sesión en i5/OS utilizando las correspondientes identidades de usuario de Windows.

En este caso práctico, creará dos identificadores EIM, uno que se llama John Day y el otro, Sharon Jones. Para crear los identificadores EIM, siga estos pasos:

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain**.

   Nota: Podría pedírsele que se conecte al controlador de dominio. En tal caso, se visualizaría el recuadro de diálogo **Conectar al controlador de dominio EIM**. Para poder llevar a cabo acciones en el dominio, primero debe conectarse a él. Para conectarse al controlador de dominio, facilite la siguiente información y pulse **Aceptar**:

   a. **Tipo de usuario**: `Nombre distinguido`
   b. **Nombre distinguido**: `cn=administrator`
   c. **Contraseña**: `mycopwd`
2. Pulse **Identificadores** con el botón derecho del ratón y seleccione **Identificador nuevo**.
3. En el recuadro de diálogo **Identificador EIM nuevo**, escriba `John Day` en el campo **Identificador**. Pulse **Aceptar**.
4. Repita los pasos del 2 al 4, pero ahora escriba `Sharon Jones` en el campo **Identificador**.

Crear asociaciones para el identificador John Day

Debe crear las asociaciones pertinentes entre el identificador EIM John Day y las identidades de usuario que utiliza la persona representada por el identificador. Estas asociaciones del identificador, cuando están debidamente configuradas, permiten al usuario participar en un entorno de inicio de sesión único.

En este caso práctico, tendrá que crear una asociación origen y dos asociaciones destino para el identificador John Day:

- Una asociación origen para el sujeto principal Kerberos jday, que es la identidad de usuario que John Day utiliza para iniciar sesión en Windows y en la red. La asociación origen permite que el sujeto principal Kerberos se correlacione con otra identidad de usuario tal como se define en una correspondiente asociación destino.
- Una asociación destino para el perfil de usuario i5/OS JOHND, que es la identidad de usuario que John Day utiliza para iniciar sesión en System i Navigator y en otras aplicaciones de i5/OS en el sistema A. La asociación destino especifica que una operación de búsqueda de correlaciones se puede correlacionar con esta identidad de usuario desde otra, tal como se define en una asociación origen del mismo identificador.
- Una asociación destino para el perfil de usuario i5/OS DAYJO, que es la identidad de usuario que John Day utiliza para iniciar sesión en System i Navigator y en otras aplicaciones de i5/OS en el sistema B.

La asociación destino especifica que una operación de búsqueda de correlaciones se puede correlacionar con esta identidad de usuario desde otra, tal como se define en una asociación origen del mismo identificador.

Para crear las asociaciones, utilice la información de las hojas de trabajo de planificación.

Para crear la asociación origen correspondiente al sujeto principal Kerberos de John Day, siga estos pasos:

1. En el sistema A, expanda **Red → Correlación de identidades de empresa (EIM) → Gestión de dominios → MyCoEimDomain → Identificadores**.
2. Pulse **John Day** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Asociaciones, pulse **Añadir**.
4. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro**: `MYCO.COM`
   b. **Usuario**: `jday`
   c. **Tipo de asociación**: `Origen`
5. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.

   Para crear una asociación destino correspondiente al perfil de usuario i5/OS de John Day en el sistema A, siga estos pasos:
6. En la página Asociaciones, pulse **Añadir**.
7. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro**: `SYSTEMA.MYCO.COM`
   b. **Usuario**: `JOHND`
   c. **Tipo de asociación**: `Destino`
8. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.

   Para crear una asociación destino correspondiente al perfil de usuario i5/OS de John Day en el sistema B, siga estos pasos:
9. En la página Asociaciones, pulse **Añadir**.
10. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
    a. **Registro**: `SYSTEMB.MYCO.COM`
    b. **Usuario**: `DAYJO`
    c. **Tipo de asociación**: `Destino`
11. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.
12. Pulse **Aceptar** para cerrar el recuadro de diálogo **Propiedades**.

Crear asociaciones para el identificador Sharon Jones

Debe crear las asociaciones pertinentes entre el identificador EIM Sharon Jones y las identidades de usuario que utiliza la persona representada por el identificador. Estas asociaciones, cuando están debidamente configuradas, permiten al usuario participar en un entorno de inicio de sesión único.

En este caso práctico, tendrá que crear una asociación origen y dos asociaciones destino para el identificador Sharon Jones:

- Una asociación origen para el sujeto principal Kerberos sjones, que es la identidad de usuario que Sharon Jones utiliza para iniciar sesión en Windows y en la red. La asociación origen permite que el sujeto principal Kerberos se correlacione con otra identidad de usuario tal como se define en una correspondiente asociación destino.
- Una asociación destino para el perfil de usuario i5/OS SHARONJ, que es la identidad de usuario que Sharon Jones utiliza para iniciar sesión en System i Navigator y en otras aplicaciones de i5/OS en el

sistema A. La asociación destino especifica que una operación de búsqueda de correlaciones se puede correlacionar con esta identidad de usuario desde otra, tal como se define en una asociación origen del mismo identificador.

- Una asociación destino para el perfil de usuario i5/OS SHARONJ, que es la identidad de usuario que Sharon Jones utiliza para iniciar sesión en System i Navigator y en otras aplicaciones de i5/OS en el sistema B. La asociación destino especifica que una operación de búsqueda de correlaciones se puede correlacionar con esta identidad de usuario desde otra, tal como se define en una asociación origen del mismo identificador.

Para crear las asociaciones, utilice la información de las hojas de trabajo de planificación:

Para crear la asociación origen correspondiente al sujeto principal Kerberos de Sharon Jones, siga estos pasos:

1. En el sistema A, expanda **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain** → **Identificadores**.
2. Pulse **Sharon Jones** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Asociaciones, pulse **Añadir**.
4. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro**: `MYCO.COM`
   b. **Usuario**: `sjones`
   c. **Tipo de asociación**: `Origen`
5. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.

   Para crear una asociación destino correspondiente al perfil de usuario i5/OS de Sharon Jones en el sistema A, siga estos pasos:
6. En la página Asociaciones, pulse **Añadir**.
7. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro**: `SYSTEMA.MYCO.COM`
   b. **Usuario**: `SHARONJ`
   c. **Tipo de asociación**: `Destino`
8. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.

   Para crear una asociación destino correspondiente al perfil de usuario i5/OS de Sharon Jones en el sistema B, siga estos pasos:
9. En la página Asociaciones, pulse **Añadir**.
10. En el recuadro de diálogo **Añadir asociación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
    a. **Registro**: `SYSTEMB.MYCO.COM`
    b. **Usuario**: `JONESSH`
    c. **Tipo de asociación**: `Destino`
11. Pulse **Aceptar** para cerrar el recuadro de diálogo **Añadir asociaciones**.
12. Pulse **Aceptar** para cerrar el recuadro de diálogo **Propiedades**.

Crear asociaciones predeterminadas de política de registro

Puede utilizar las asociaciones de política para crear directamente correlaciones entre un grupo de usuarios y una única identidad de usuario destino.

Le interesa que todos los usuarios de Microsoft Active Directory en el servidor Windows 2000 se correlacionen con el perfil de usuario SYSUSERA en el sistema A y con el perfil de usuario SYSUSERB en el sistema B. En este caso, puede crear una asociación de política de registro predeterminada que haga

que todas las identidades de usuario (que no tengan asociaciones de identificador) del registro Kerberos MYCO.COM se correlacionen con un único perfil de usuario i5/OS en el sistema A.

Para lograr este objetivo, necesitará dos asociaciones de política. Cada una de ellas utilizará la definición de registro de usuarios MYCO.COM como origen de la asociación. Sin embargo, cada asociación de política hará que las identidades de usuario de este registro se correlacionen con distintas identidades de usuario destino, en función de la plataforma System i a la que acceda el usuario de Kerberos:

- Una de las asociaciones de política hará que los sujetos principales Kerberos del registro de usuarios MYCO.COM se correlacionen con un usuario destino SYSUSERA del registro destino SYSTEMA.MYCO.COM.
- La otra asociación de política hará que los sujetos principales Kerberos del registro de usuarios MYCO.COM se correlacionen con un usuario destino SYSUSERB del registro destino SYSTEMB.MYCO.COM.

Para crear las dos asociaciones de política de registro predeterminadas, utilice la información de las hojas de trabajo de planificación.

Para poder utilizar asociaciones de política, primero debe habilitar el dominio de cara a la utilización de asociaciones de política para las operaciones de búsqueda de correlaciones.

Para habilitar el dominio de cara a la utilización de asociaciones de política para las operaciones de búsqueda de correlaciones, siga los pasos siguientes:

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios**.
2. Pulse **MyCoEimDomain** con el botón derecho del ratón y seleccione **Política de correlación**.
3. En la página General, marque el recuadro **Habilitar búsquedas de correlaciones utilizando asociaciones de política para el dominio MyCoEimDomain**.

Para crear la asociación predeterminada de política de registro para que los usuarios se correlacionen con el perfil de usuario SYSUSERA en el sistema A, siga estos pasos:

1. En la página Registro, pulse **Añadir**.
2. En el recuadro de diálogo **Añadir asociación predeterminada de política de registro**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro origen**: `MYCO.COM`
   b. **Registro destino**: `SYSTEMA.MYCO.COM`
   c. **Usuario destino**: `SYSUSERB`
3. Pulse **Aceptar** para cerrar el recuadro de diálogo **Política de correlación**.

Para crear la asociación predeterminada de política de registro para que los usuarios se correlacionen con el perfil de usuario SYSUSERB en el sistema B, siga estos pasos:

1. En la página Registro, pulse **Añadir**.
2. En el recuadro de diálogo **Añadir asociación predeterminada de política de registro**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Aceptar**:
   a. **Registro origen**: `MYCO.COM`
   b. **Registro destino**: `SYSTEMB.MYCO.COM`
   c. **Usuario destino**: `SYSUSERB`
3. Pulse **Aceptar** para cerrar el recuadro de diálogo **Política de correlación**.

Habilitar los registros para que participen en las operaciones de búsqueda y utilicen las asociaciones de política

Para utilizar las asociaciones de política de un registro, debe habilitar su utilización para ese registro y también habilitar el registro para que participe en las operaciones de búsqueda.

EIM le permite controlar cómo participa cada registro en EIM. Dado que una asociación de política puede tener un efecto a gran escala dentro de una empresa, se puede controlar si un registro puede quedar afectado por las asociaciones de política. Asimismo, se puede controlar si es que un registro puede participar en las operaciones de búsqueda de correlaciones.

Para habilitar los registros para que utilicen asociaciones de política y participen en las operaciones de búsqueda, lleve a cabo los procedimientos siguientes:

Para habilitar el registro MYCO.COM para que participe en las operaciones de búsqueda de correlaciones, siga estos pasos:

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain** → **Registros de usuarios**.
2. Pulse el registro **MYCO.COM** con el botón derecho del ratón y seleccione **Política de correlación**.
3. En la página General, seleccione **Habilitar búsquedas de correlaciones para el registro MYCO.COM** y pulse **Aceptar**.

   Para habilitar el registro SYSTEMA.MYCO.COM para que participe en las operaciones de búsqueda de correlaciones y utilice las asociaciones de política, siga estos pasos:
4. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain** → **Registros de usuarios**.
5. Pulse el registro **SYSTEMA.MYCO.COM** con el botón derecho del ratón y seleccione **Política de correlación**.
6. En la página General, seleccione **Habilitar búsquedas de correlaciones para el registro SYSTEMA.MYCO.COM**, seleccione **Utiliza asociaciones de política** y pulse **Aceptar**.
7. Repita los pasos comprendidos entres 1 y 6 para habilitar el registro SYSTEMB.MYCO.COM para que participe en las operaciones de búsqueda de correlaciones y utilice las asociaciones de política, pero ahora, en la página General, seleccione **Habilitar búsquedas de correlaciones para el registro SYSTEMB.MYCO.COM**, seleccione **Utilizar asociaciones de política** y pulse **Aceptar**.

Probar las correlaciones de identidades de EIM

Ahora que ya ha creado todas las asociaciones que necesita, debe verificar que las operaciones de búsqueda de correlaciones de EIM devuelven los resultados correctos en función de las asociaciones configuradas.

En este caso práctico, debe probar las correlaciones que se emplean para las asociaciones de identificador de cada uno de los administradores, así como las correlaciones que se emplean para las asociaciones predeterminadas de política de registro. Para probar las correlaciones de EIM, siga estos pasos:

Probar las correlaciones de John Day

Para comprobar que las correlaciones de identificador funcionan según lo previsto para John Day, siga estos pasos:

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain**.

   Nota: Podría pedírsele que se conecte al controlador de dominio. En tal caso, se visualizaría el recuadro de diálogo **Conectar al controlador de dominio EIM**. Para poder llevar a cabo acciones en el dominio, primero debe conectarse a él. Para conectarse al controlador de dominio, facilite la siguiente información y pulse **Aceptar**:

   a. **Tipo de usuario**: `Nombre distinguido`
   b. **Nombre distinguido**: `cn=administrator`
   c. **Contraseña**: `mycopwd`
2. Pulse **MyCoEimDomain** con el botón derecho del ratón y seleccione **Probar una correlación**.

3. En el recuadro de diálogo **Probar una correlación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Probar**:
   a. **Registro origen**: `MYCO.COM`
   b. **Usuario origen**: `jday`
   c. **Registro destino**: `SYSTEMA.MYCO.COM`

   Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	JOHND
Origen	Identificador EIM: John Day

4. Pulse **Cerrar**.
5. Repita estos pasos seleccionando ahora `SYSTEMB.MYCO.COM` para el campo **Registro destino**. Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	DAYJO
Origen	Identificador EIM: John Day

Probar las correlaciones de Sharon Jones

Para probar las correlaciones empleadas para las asociaciones individuales de Sharon Jones,siga estos pasos:

6. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain**.

   Nota: Podría pedírsele que se conecte al controlador de dominio. En tal caso, se visualizaría el recuadro de diálogo **Conectar al controlador de dominio EIM**. Para poder llevar a cabo acciones en el dominio, primero debe conectarse a él. Para conectarse al controlador de dominio, facilite la siguiente información y pulse **Aceptar**:
   a. **Tipo de usuario**: `Nombre distinguido`
   b. **Nombre distinguido**: `cn=administrator`
   c. **Contraseña**: `mycopwd`
7. Pulse **MyCoEimDomain** con el botón derecho del ratón y seleccione **Probar una correlación**.
8. En el recuadro de diálogo **Probar una correlación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Probar**:
   a. **Registro origen**: `MYCO.COM`
   b. **Usuario origen**: `sjones`
   c. **Registro destino**: `SYSTEMA.MYCO.COM`

   Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	SHARONJ
Origen	Identificador EIM: Sharon Jones

9. Pulse **Cerrar**.

10. Repita los pasos comprendidos entre 1 en la página 74 y 9 en la página 75, pero seleccionando ahora SYSTEMB.MYCO.COM para el campo **Registro destino**. Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	JONESSH
Origen	Identificador EIM: Sharon Jones

Probar las correlaciones utilizadas para las asociaciones predeterminadas de política de registro

Para comprobar que las correlaciones funcionen según lo previsto para los usuarios del departamento de recepción de pedidos, en función de las asociaciones de política definidas, siga estos pasos:

11. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain**.

    Nota: Podría pedírsele que se conecte al controlador de dominio. En tal caso, se visualizaría el recuadro de diálogo **Conectar al controlador de dominio EIM**. Para poder llevar a cabo acciones en el dominio, primero debe conectarse a él. Para conectarse al controlador de dominio, facilite la siguiente información y pulse **Aceptar**:

    a. **Tipo de usuario**: Nombre distinguido
    b. **Nombre distinguido**: cn=administrator
    c. **Contraseña**: mycopwd

12. Pulse **MyCoEimDomain** con el botón derecho del ratón y seleccione **Probar una correlación**.
13. En el recuadro de diálogo **Probar una correlación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Probar**:
    a. **Registro origen**: MYCO.COM
    b. **Usuario origen**: mmiller
    c. **Registro destino**: SYSTEMA.MYCO.COM

    Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	SYSUSERA
Origen	Asociación de política de registro

14. Pulse **Cerrar**.

Para probar las correlaciones empleadas para la asociación predeterminada de política de registro que correlaciona los usuarios con el perfil SYSUSERB en el sistema B, siga estos pasos:

1. En System i Navigator, expanda **Sistema A** → **Red** → **Correlación de identidades de empresa (EIM)** → **Gestión de dominios** → **MyCoEimDomain**.

   Nota: Podría pedírsele que se conecte al controlador de dominio. En tal caso, se visualizaría el recuadro de diálogo **Conectar al controlador de dominio EIM**. Para poder llevar a cabo acciones en el dominio, primero debe conectarse a él. Para conectarse al controlador de dominio, facilite la siguiente información y pulse **Aceptar**:

   a. **Tipo de usuario**: Nombre distinguido
   b. **Nombre distinguido**: cn=administrator
   c. **Contraseña**: mycopwd

2. Pulse **MyCoEimDomain** con el botón derecho del ratón y seleccione **Probar una correlación**.

3. En el recuadro de diálogo **Probar una correlación**, especifique la siguiente información o pulse **Examinar** para seleccionarla y después pulse **Probar**:
   a. **Registro origen**: `MYCO.COM`
   b. **Usuario origen**: `ksmith`
   c. **Registro destino**: `SYSTEMB.MYCO.COM`

   Los resultados se visualizarán en la parte **Correlación encontrada** de la página, como se indica a continuación:

Para estos campos	Vea estos resultados
Usuario destino	SYSUSERB
Origen	Asociación de política de registro

4. Pulse **Cerrar**. Si recibe los mensajes o errores que indican problemas relacionados con las correlaciones o con las comunicaciones, vea el tema Resolución de problemas de EIM, donde hallará procedimientos para solucionar los problemas.

Configurar las aplicaciones de System i Access para Windows para que utilicen la autenticación de Kerberos

Tomando como base los objetivos del inicio de sesión único, todos los usuarios del departamento de recepción de pedidos deben autenticarse mediante Kerberos para poder utilizar System i Navigator para acceder a los sistemas A y B. Por tanto, deberá configurar System i Access para Windows para utilizar la autenticación de Kerberos.

Para configurar las aplicaciones de System i Access para Windows, siga estos pasos:

Nota: Todos los usuarios deben seguir todos estos pasos en sus propios PC.

1. Conéctese al dominio de Windows 2000 iniciando sesión en el PC.
2. En System i Navigator en el PC, pulse **Sistema A** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Conexión, seleccione **Utilizar nombre de sujeto principal Kerberos, sin solicitud**. Ello permitirá que las conexiones de System i Access para Windows utilicen el nombre de sujeto principal Kerberos y la contraseña para la autenticación.
4. Se visualiza un mensaje que indica que es necesario cerrar y reiniciar todas las aplicaciones que se estén ejecutando en ese momento para que entren en vigor los cambios realizados en los valores de la conexión. Pulse **Aceptar**. Después, finalice System i Navigator y vuelva a iniciarlo.
5. Repita estos pasos para el sistema B.

Verificar la configuración del servicio de autenticación de red y EIM

Ahora que ya ha verificado las partes individuales de la configuración del inicio de sesión único y se ha asegurado de que la configuración está completa, debe verificar que ha configurado la Correlación de identidades de empresa (EIM) y el servicio de autenticación de red como es debido y que el inicio de sesión único funciona según lo previsto.

Para verificar que el entorno de inicio de sesión único funciona correctamente, haga que John Day siga estos pasos:

1. En System i Navigator, expanda **Sistema A** para abrir una conexión con el sistema A.
2. Pulse F5 para renovar la pantalla.
3. En el panel de la derecha, localice el `Sistema A` en la columna **Nombre** y verifique que el perfil de usuario i5/OS, `JOHND`, se visualiza como entrada correspondiente en la columna **Usuario conectado**. System i Navigator ha utilizado satisfactoriamente EIM para correlacionar el sujeto principal Kerberos jday con el perfil de usuario JOHND del sistema A debido a las asociaciones definidas para el identificador EIM John Day. La sesión de System i Navigator del sistema A está ahora conectada como JOHND.

4. Repita estos pasos para Sharon Jones y para, como mínimo, una de las identidades de usuario que se correlaciona con el perfil de usuario SYSUSERA o SYSUSERB.

Consideraciones de postconfiguración

El número de usuarios de EIM adicionales que defina depende del énfasis que pone su política de seguridad en la separación de loe deberes y responsabilidades relacionados con la seguridad.

Ahora que ya ha terminado este caso práctico, el único usuario de EIM que ha definido y que EIM puede utilizar es el DN del administrador de LDAP. El DN del administrador de LDAP que ha especificado para el usuario del sistema en los sistemas A y B tiene un alto nivel de autorización sobre todos los datos del servidor de directorios. Por lo tanto, podría plantearse la posibilidad de crear uno o más nombres distinguidos (DN) como usuarios adicionales que tengan un control de acceso más adecuado y limitado sobre los datos de EIM. Por lo general, podría crear como mínimo los siguientes tipos de nombres distinguidos (DN):

- **Un usuario que tenga control de acceso de administrador de EIM**

  Este DN de administrador de EIM proporciona el nivel de autoridad adecuado de un administrador que se encargue de gestionar el dominio EIM. Este DN de administrador de EIM puede utilizarse para conectar con el controlador de dominio al gestionar todos los aspectos del dominio EIM por medio de System i Navigator.
- **Un usuario como mínimo que tenga todos los controles de acceso siguientes**:
  - Administrador de identificadores
  - Administrador del registro
  - Operaciones de correlaciones de EIM

  Este usuario proporciona el nivel de control de acceso apropiado necesario para el usuario del sistema que realiza operaciones EIM en nombre del sistema operativo.

Nota: Para utilizar este nuevo DN para el usuario del sistema en lugar del DN del administrador de LDAP, tendrá que cambiar las propiedades de configuración de EIM para cada sistema. Para este caso práctico, es necesario cambiar las propiedades de configuración de EIM para los sistemas A y B.

Conceptos relacionados

Control de acceso EIM

IBM Directory Server para i5/OS (LDAP)

Tareas relacionadas

Gestionar propiedades de configuración EIM

Planificar el servicio de autenticación de red

Antes de implementar el servicio de autenticación de red o una solución Kerberos en la red, es fundamental llevar a cabo las tareas de planificación necesarias.

Para planificar el servicio de autenticación de red y una implementación Kerberos, deberá reunir la información pertinente sobre los sistemas y usuarios de la red. Se han facilitado varias hojas de trabajo de planificación que pretenden ayudarle a configurar el servicio de autenticación en su red.

Nota: Son muchas y variadas las soluciones de autenticación Kerberos que se pueden utilizar en una empresa. Esta información se centrará en planificar una implementación para el i5/OS y en las consideraciones que conviene tener en cuenta al utilizar el servicio de autenticación de red con un servidor Kerberos configurado en Microsoft Active Directory o en i5/OS PASE.

Para obtener información sobre cómo configurar un servidor Kerberos en Microsoft Active Directory, consulte Windows 2000 Server .

Los siguientes sistemas IBM soportan la autenticación de Kerberos. Si desea información sobre la implementación Kerberos específica de cada plataforma, vea las siguientes fuentes de información:

- **System p**
  - *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
  - *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

    Nota: Encontrará esta documentación en el CD del paquete de ampliación y Bonus Pack de AIX 5L .
- **System z**
  - z/OS Security Server Network Authentication Service Administration

Como ayuda para planificar el servicio de autenticación de red, utilice estas tareas.

Planificar un servidor Kerberos

Planificar un servidor Kerberos en función del sistema operativo.

Un servidor Kerberos o centro de distribución de claves (KDC) mantiene una base de datos de sujetos principales y las contraseñas asociadas a ellos. Está compuesto por el servidor de autenticación y el servidor de otorgamiento de tickets. Cuando un sujeto principal inicia sesión en una red Kerberos, el servidor de autenticación valida el sujeto principal y le envía un ticket de otorgamiento de tickets (TGT). Cuando planifique el uso de la autenticación Kerberos, tendrá que decidir qué sistema desea configurar como servidor Kerberos.

Nota: La información del servicio de autenticación de red se centra en servidores Kerberos que ejecutan i5/OS PASE o Windows 2000 Server. En la mayoría de los casos prácticos y ejemplos se da por sentado que se ha configurado un servidor Windows 2000 como servidor Kerberos, a menos que se indique explícitamente lo contrario. Si se propone utilizar otros sistemas operativos o aplicaciones de terceros para la autenticación Kerberos, consulte la documentación que corresponda.

La siguiente lista facilita detalles sobre el soporte de servidor Kerberos en tres sistemas operativos clave:

Microsoft Windows 2000 y Windows Server 2003
Ambos sistemas operativos, Microsoft Windows 2000 y Windows Server 2003, soportan la autenticación Kerberos como mecanismo de seguridad predeterminado. Cuando los administradores añaden usuario y servicios mediante Microsoft Active Directory, lo que hacen en realidad es crear sujetos principales Kerberos para los usuarios y servicios. Si tiene un servidor Windows 2000 ó 2003 en su red, tiene un servidor Kerberos incorporado en dichos sistemas operativos. Para obtener información sobre cómo se utiliza la autenticación Kerberos en los servidores Microsoft Windows, consulte Windows 2000 Server .

AIX y i5/OS PASE
Tanto AIX como i5/OS PASE soportan un servidor Kerberos mediante el mandato kadmin. Los administradores deben entrar en el entorno PASE (escribiendo `call QP2TERM`) para configurar y gestionar el servidor Kerberos de PASE. i5/OS PASE suministra un entorno de ejecución para aplicaciones AIX, como por ejemplo un servidor Kerberos. En la siguiente documentación encontrará instrucciones que le ayudarán a configurar y gestionar un servidor Kerberos en AIX.

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

  Nota: Encontrará esta documentación en el CD del paquete de ampliación y Bonus Pack de AIX 5L .

z/OS Security Server Network Authentication Service para z/OS es el programa IBM z/OS basado en Kerberos Versión 5. Network Authentication Service para z/OS proporciona servicios de

seguridad Kerberos sin que haga falta adquirir o utilizar un programa de middleware. Estos servicios soportan un servidor Kerberos nativo. En z/OS Security Server Network Authentication Service Administration  encontrará detalles sobre cómo configurar y gestionar un servidor Kerberos de z/OS.

Sea cual sea el sistema operativo que proporcione el servidor Kerberos, tendrá que determinar los puertos del servidor Kerberos, asegurar el acceso al servidor Kerberos y asegurarse de que la hora de los clientes está sincronizada con la hora del servidor Kerberos.

Determinar los puertos del servidor

El servicio de autenticación de red utiliza como valor predeterminado el puerto 88 para el servidor Kerberos. Sin embargo, puede haber otros puertos especificados en los archivos de configuración del servidor Kerberos. Debe verificar el número de puerto de los archivos de configuración Kerberos situados en el servidor Kerberos.

Asegurar el acceso al servidor Kerberos

El servidor Kerberos debe estar situado en un sistema dedicado y seguro para que la seguridad de la base de datos de sujetos principales y contraseñas no se vea comprometida. Los usuarios deben tener un acceso limitado al servidor Kerberos. Si el sistema en el que reside el servidor Kerberos también se utiliza para alguna otra finalidad (por ejemplo, para un servidor Web o un servidor FTP), alguna persona podría aprovecharse de las grietas de seguridad de tales aplicaciones y obtener acceso a la base de datos almacenada en el servidor Kerberos. En el caso de un servidor Kerberos de Microsoft Active Directory, puede configurar opcionalmente un servidor de contraseñas que permita a los sujetos principales gestionar y actualizar sus propias contraseñas almacenadas en el servidor Kerberos. Si ha configurado un servidor Kerberos en i5/OS PASE y le resulta imposible dedicar la plataforma System i a la autenticación Kerberos, debe asegurarse de que sólo el administrador tenga acceso a la configuración de Kerberos.

Sincronizar las horas de los sistemas

La autenticación Kerberos exige que la hora de los sistemas esté sincronizada. Kerberos rechazará las peticiones de autenticación procedentes de un sistema o un cliente cuya hora no esté dentro del desvío horario máximo especificado del servidor Kerberos. Dado que en cada ticket se intercala la hora de su envío al sujeto principal, los piratas no pueden reenviar el mismo ticket en un momento posterior para autenticarse ante la red. La plataforma System i también rechazará los tickets procedentes de un servidor Kerberos si su hora no está dentro del desvío horario máximo fijado durante la configuración del servicio de autenticación de red. El valor predeterminado del desvío horario máximo es de 300 segundos (cinco minutos). Durante la configuración del servicio de autenticación de red, el desvío horario máximo se fija en este valor predeterminado; pero es posible cambiar este valor en caso necesario. Es recomendable que este valor no sea mayor de 300 segundos. En el tema “Sincronizar las horas de los sistemas” en la página 105 encontrará los detalles sobre cómo trabajar con las horas de los sistemas.

Tabla 19. Hoja de trabajo de planificación de ejemplo para el servidor Kerberos. En esta hoja de trabajo se muestra un ejemplo de un administrador que ha planificado el servidor Kerberos para una red.

Preguntas	Respuestas
¿En qué sistema operativo se propone configurar el servidor Kerberos? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (V5R3 o posterior) • z/OS	Entorno de soluciones de aplicaciones portables (PASE) de i5/OS
¿Cuál es el nombre de dominio totalmente calificado del servidor Kerberos?	systema.myco.com

Tabla 19. Hoja de trabajo de planificación de ejemplo para el servidor Kerberos (continuación). En esta hoja de trabajo se muestra un ejemplo de un administrador que ha planificado el servidor Kerberos para una red.

Preguntas	Respuestas
¿Están sincronizadas las horas entre los PC y los sistemas que se conectan al servidor Kerberos? ¿Cuál es el desvío horario máximo?	Sí, 300 segundos
¿Debo instalar el producto Network Authentication Enablement (5722-NAE o 5761-NAE)?	Sí, si desea configurar un servidor Kerberos en i5/OS PASE en un sistema V5R4. En V5R4 o posterior, el servidor de autenticación de red se suministra como un producto aparte, *Network Authentication Enablement* (5722-NAE o 5761-NAE). En cambio, si utiliza i5/OS V5R3, debe instalar el producto Cryptographic Access Provider (5722-AC3) para configurar un servidor Kerberos en i5/OS PASE.

Planificar reinos

Descripción de cómo su empresa puede ayudarle a planificar reinos en su entorno.

En el protocolo Kerberos, los reinos están formados por un conjunto de máquinas y servicios que utilizan un solo servidor de autenticación, llamado servidor Kerberos o centro de distribución de claves (KDC). Los reinos se gestionan individualmente. Las aplicaciones y los servicios del reino suelen compartir alguna utilización o finalidad común. Las siguientes preguntas generales pretenden ayudarle a planificar los reinos de su empresa:

¿Qué tamaño tiene mi entorno actual?
Del tamaño de su entorno depende el número de reinos que necesite. En una gran empresa, podría plantearse la posibilidad de tener varios reinos que estén relacionados con los límites organizativos o con la función que desempeñan determinados sistemas en la empresa. Por ejemplo, podría establecer reinos que representen las distintas organizaciones de su compañía, como un reino para el departamento de recursos humanos, otro reino para el departamento de servicio al cliente o para el departamento de envíos. También puede crear reinos para los distintos conjuntos de sistemas o servicios que desempeñen funciones similares. Por lo general, para las empresas más pequeñas tan solo serían necesarios uno o dos reinos.

¿Qué ritmo de crecimiento pronostico para mi entorno?
Si piensa que su empresa crecerá rápidamente, podría interesarle configurar varios reinos que representen unidades organización más reducidas en su empresa. Si cree que su empresa crecerá más despacio, puede configurar tan solo uno o dos reinos basándose en su organización actual.

¿Cuántos administradores necesitaré para gestionar los reinos?
Sea cual sea el tamaño de su empresa, debe asegurarse de que dispone de personal cualificado para configurar y administrar los reinos que necesita.

Nombres de los reinos

Teniendo en cuenta los convenios del protocolo Kerberos, los nombres de los reinos se componen en general de una versión del nombre del dominio escrita con mayúsculas; por ejemplo, MYCO.COM. En las redes que constan de múltiples reinos, puede crear un nombre de reino que incluya un nombre descriptivo y un nombre de dominio, escritos con mayúsculas. Por ejemplo, podría tener dos reinos, uno llamado HR.MYCO.COM y el otro, SHIPPING.MYCO.COM, cada uno de los cuales representaría un departamento concreto de su organización.

No es necesario utilizar siempre letras mayúsculas; no obstante, algunas implementaciones de Kerberos ponen en vigor este convenio. Por ejemplo, los nombres de los reinos tienen que estar escritos con mayúsculas en Microsoft Active Directory. Si se propone configurar el servicio de autenticación de red en

la plataforma System i para que participe en un reino Kerberos configurado en Microsoft Active Directory, deberá escribir el nombre del reino con mayúsculas.

En el caso de un servidor Kerberos que esté configurado en i5/OS PASE, podrá crear nombres de reino escritos con minúsculas o mayúsculas. Sin embargo, si piensa crear relaciones de confianza entre un servidor Kerberos configurado con Microsoft Active Directory y un servidor Kerberos configurado en i5/OS PASE, los nombres de los reinos deberán escribirse con mayúsculas.

Tabla 20. Hoja de trabajo de planificación de ejemplo para los reinos Kerberos

Preguntas	**Respuestas**
¿Cuántos reinos necesita?	Dos
¿Cómo se propone organizar los reinos?	Actualmente, nuestra compañía tiene un servidor Windows 2000 que autentica a los usuarios del departamento de recepción de pedidos. Para nuestro departamento de envíos se utiliza un servidor Kerberos de i5/OS PASE. Habrá un reino para cada departamento.
¿Qué convenio de denominación utilizará para los reinos?	Utilizaremos un nombre corto escrito con mayúsculas que indique el departamento seguido de una versión en mayúsculas del nombre de dominio Windows 2000. Por ejemplo, ORDEPT.MYCO.COM representará el departamento de recepción de pedidos y SHIPDEPT.MYCO.COM, el departamento de envíos.

Planificar nombres de sujeto principal

Llamamos sujetos principales a los nombres de los usuarios o de los servicios de una red Kerberos. El nombre de un sujeto principal consta del nombre del usuario o del servicio y del nombre del reino al que pertenece el usuario o el servicio.

Si Mary Jones utiliza el reino MYCO.COM, su nombre de sujeto principal podría ser jonesm@MYCO.COM. Mary Jones utilice este nombre de sujeto principal y la contraseña asociada para autenticarse ante un servidor Kerberos centralizado. Todos los sujetos principales se añaden al servidor Kerberos, en el que se mantiene una base de datos de todos los usuarios y servicio de un reino.

Cuando desarrolle un sistema para denominar sujetos principales, deberá asignar los nombres siguiendo un convenio de denominación coherente que se ajuste a los usuarios actuales y futuros. A la hora de establecer un convenio de denominación para los sujetos principales, tenga en cuenta las siguientes sugerencias:

- Utilizar el apellido y la letra inicial del nombre
- Utilizar la letra inicial del nombre y el apellido completo
- Utilizar el nombre y la letra inicial del apellido
- Utilizar los nombres de las aplicaciones o servicios con números identificativos; por ejemplo, basedatos1.

Nombres de sujetos principales de i5/OS

Cuando configure el servicio de autenticación de red en plataformas System i, podrá crear opcionalmente nombres para sujetos principales. Cada uno de estos sujetos principales representan servicios que se encuentran en el sistema operativo i5/OS. Durante la configuración del servicio de autenticación de red, se crea una entrada de tabla de claves en el sistema para cada uno de los sujetos principales de servicio que haya elegido crear. La entrada de tabla de claves almacena el nombre de sujeto principal de servicio y la contraseña cifrada que especificó durante la configuración. Es importante tener en cuenta que todos los sujetos principales de servicio de i5/OS deben añadirse al servidor Kerberos una vez configurado el servicio de autenticación de red. Los procedimientos para añadir el sujeto principal de i5/OS al servidor

Kerberos varían en función del servidor Kerberos que haya configurado en su empresa. Las instrucciones para añadir el nombre de sujeto principal de i5/OS a un dominio Windows 2000 o a un servidor Kerberos de i5/OS PASE están en el tema "Añadir sujetos principales i5/OS al servidor Kerberos" en la página 101. La siguiente información describe cada uno de los sujetos principales de servicio de i5/OS que se crean durante el proceso de configuración del servicio de autenticación de red:

Autenticación de Kerberos de i5/OS

Cuando elige crear una entrada de tabla de claves para la autenticación Kerberos de i5/OS, se genera el sujeto principal de servicio en el archivo de tabla de claves con uno de estos formatos: krbsvr400/nombre de dominio totalmente calificado de *System i@NOMBRE REINO* o krbsvr400/nombre de host *System i@NOMBRE REINO*. Por ejemplo, un sujeto principal de servicio válido para la autenticación Kerberos de i5/OS podría ser krbsvr400/systema.myco.com@MYCO.COM o krbsvr400/systema@MYCO.COM. i5/OS genera el sujeto principal basándose en el nombre de host que encuentra en el servidor DNS o en la plataforma System i, dependiendo de cómo esté configurada la plataforma System i para resolver los nombres de host.

El sujeto principal de servicio se utiliza para varias interfaces de i5/OS, como por ejemplo QFileSrv.400, Telnet, Distributed Relational Database Architecture (DRDA), i5/OS NetServer e IBM System i Access para Windows incluido System i Navigator. Cada una de estas aplicaciones podría exigir una configuración adicional para habilitar la autenticación Kerberos.

LDAP Además del nombre de sujeto principal de servicio de i5/OS, puede configurar opcionalmente sujetos principales de servicio adicionales para IBM Directory Server para i5/OS (LDAP) durante el proceso de configuración del servicio de autenticación de red. El nombre de sujeto principal de LDAP es ldap/nombre de dominio totalmente calificado de *System i@NOMBRE REINO*. Por ejemplo, un nombre de sujeto principal de LDAP válido sería ldap/systema.myco.com@MYCO.COM. Este nombre de sujeto principal identifica el servidor de directorio situado en esa plataforma System i.

Nota: En los releases anteriores, el asistente del servicio de autenticación de red creaba una entrada de tabla de claves en mayúsculas para el servicio LDAP. Si configuró anteriormente el sujeto principal de LDAP, cuando reconfigure el servicio de autenticación de red o acceda al asistente mediante la interfaz de correlación de identidades de empresa (EIM), se le pedirá que cambie este nombre de sujeto principal para obtener la versión en minúsculas.

Si se propone utilizar la autenticación Kerberos con el servidor de directorio, no solo tendrá que configurar el servicio de autenticación de red, sino también cambiar las propiedades del servicio de directorio para que acepte la autenticación Kerberos. Cuando se utiliza la autenticación Kerberos, el servidor de directorio asocia el nombre distinguido (DN) del servidor al nombre de sujeto principal Kerberos. Para asociar el DN del servidor, puede elegir uno de los siguientes métodos:

- El servidor puede crear un DN basándose en el nombre de sujeto principal Kerberos. Si elige esta opción, una identidad Kerberos cuyo formato sea **sujeto_principal@reino** genera un DN con el formato **ibm-kn=sujeto_principal@reino**. **ibm-kn=** es equivalente a **ibm-kerberosName=**.
- El servidor puede buscar en el directorio un nombre distinguido (DN) que contenga una entrada correspondiente al sujeto principal Kerberos y al reino. Si elige esta opción, el servidor busca en el directorio una entrada que especifique esta identidad Kerberos.

En IBM Tivoli Directory Server para i5/OS (LDAP) encontrará los detalles sobre la configuración de la autenticación Kerberos en relación con el servidor de directorio.

Servidor HTTP

Además del nombre de sujeto principal de servicio de i5/OS, puede configurar opcionalmente sujetos principales de servicio adicionales para HTTP Server powered by Apache (HTTP) durante el proceso de configuración del servicio de autenticación de red. El nombre de sujeto principal de

HTTP es HTTP/nombre de dominio totalmente calificado de *System i@NOMBRE REINO*. Este nombre de sujeto principal identifica las instancias del servidor HTTP en la plataforma System i que utilizará Kerberos para autenticar a los usuarios de la Web. Para utilizar la autenticación Kerberos con una instancia del servidor HTTP, también tendrá que llevar a cabo algunos pasos de configuración adicionales en relación con el servidor HTTP.

En la página de presentación de HTTP Server para i5/OS: documentación hallará información sobre cómo utilizar la autenticación Kerberos con el servidor HTTP.

i5/OS NetServer

Para i5/OS NetServer, también puede optar por crear varios sujetos principales NetServer que se añaden automáticamente al archivo de tabla de claves de la plataforma System i. Cada uno de los sujetos principales NetServer representa todos los clientes potenciales que se podrían utilizar para conectar con NetServer. La siguiente tabla muestra el nombre de sujeto principal de NetServer y los clientes que representa cada uno de ellos.

Tabla 21. Nombres de sujetos principales de i5/OS NetServer

Conexión de cliente	Nombre de sujeto principal de i5/OS NetServer
Windows XP y Windows Vista	cifs/nombre de dominio totalmente calificado de System i cifs/nombre de host de System i cifs/nombre de host de QSystem i cifs/nombre de host de qSystem i cifs/dirección IP
Windows 2000	HOST/nombre de dominio totalmente calificado de System i HOST/nombre de host de System i HOST/nombre de host de QSystem i HOST/nombre de host de qSystem i HOST/dirección IP

En i5/OS NetServer hallará más información sobre cómo utilizar la autenticación Kerberos con esta aplicación.

Servidor del sistema de archivos de red

Además del nombre de sujeto principal de i5/OS, puede configurar opcionalmente el servidor del sistema de archivos de red (NFS) durante el proceso de configuración del servicio de autenticación de red. El nombre de sujeto principal de NFS es nfs/nombre de dominio totalmente calificado de *System i@NOMBRE REINO*. Por ejemplo, un nombre de sujeto principal válido para el servidor NFS sería nfs/systema.myco.com@MYCO.COM.

Hoja de trabajo de planificación de ejemplo

Tabla 22. Hoja de trabajo de planificación de sujetos principales de ejemplo

Preguntas	Respuestas
¿Qué convenio de denominación se propone utilizar para los sujetos principales Kerberos que representan a los usuarios de la red?	Letra inicial del nombre seguida de las cinco primeras letras del apellido en minúscula, por ejemplo: mjones
¿Qué convenio de denominación utilizará para las aplicaciones de la red?	Nombre descriptivo seguido de un número, por ejemplo: basedatos123
¿Para qué servicios de i5/OS piensa utilizar la autenticación Kerberos?	La autenticación Kerberos de i5/OS se utiliza para los siguientes servicios: 1. System i Access para Windows, System i Navigator, i5/OS NetServer y Telnet 2. HTTP Server powered by Apache 3. LDAP 4. Servidor del sistema de archivos de red (NFS)

Tabla 22. Hoja de trabajo de planificación de sujetos principales de ejemplo (continuación)

Preguntas	Respuestas
¿Qué nombres de sujeto principal de i5/OS tiene cada uno de dichos servicios de i5/OS?	1. krbsvr400/systema.myco.com@MYCO.COM 2. HTTP/systema.myco.com@MYCO.COM 3. ldap/systema.myco.com@MYCO.COM 4. nfs/systema.myco.com/MYCO.COM

Consideraciones sobre la resolución de nombres de host

Para garantizar el debido funcionamiento de la autenticación Kerberos y de la resolución de nombres de host en lo que se refiere a las aplicaciones habilitadas para Kerberos, verifique que los PC y las plataformas System i resuelvan el mismo nombre de host para el sistema en el que reside la aplicación de servicio.

En un entorno Kerberos, tanto el cliente como el servidor utilizan algún método de resolución de nombres de host para determinar el nombre de host del sistema en el que reside una aplicación o un servicio en concreto. Si las plataformas System i y los PC utilizan un servidor de nombres de dominio (DNS), es importante que utilicen el mismo servidor DNS para la resolución de nombres de host o, si utilizan más de un servidor DNS, los nombres de host deben ser iguales en ambos servidores DNS. Si la plataforma System i o el PC resuelven los nombres de host localmente (desde una tabla o un archivo de hosts locales), podrían obtener un nombre de host distinto del anotado en el servidor DNS. Esto podría hacer que fallara el servicio de autenticación de red.

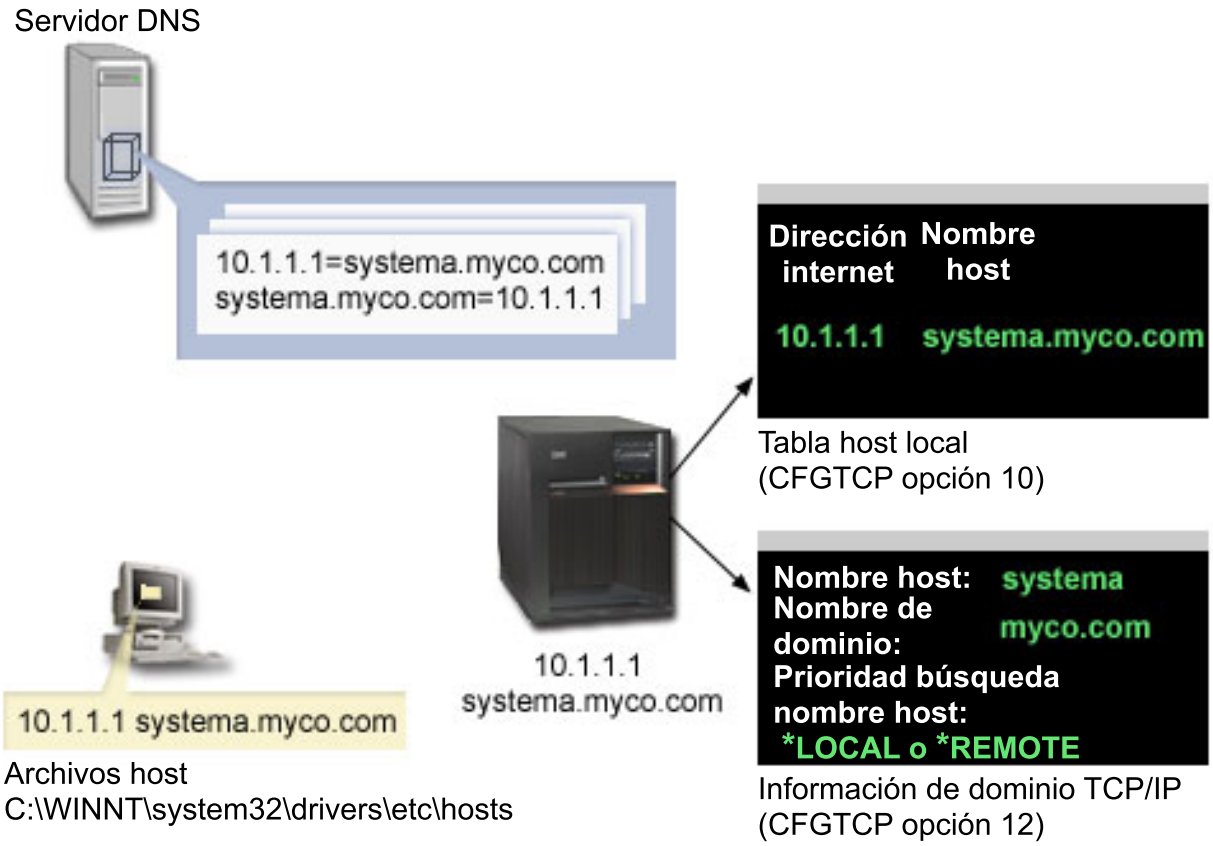
Para garantizar el debido funcionamiento de la autenticación Kerberos y de la resolución de nombres de host en lo que se refiere a las aplicaciones habilitadas para Kerberos, debe verificar que los PC y las plataformas System i resuelvan el mismo nombre de host para el sistema en el que reside la aplicación de servicio. En el siguiente ejemplo, el sistema en cuestión se llama sistema A.

Las siguientes instrucciones muestran cómo determinar si los PC y las plataformas System i resuelven el mismo nombre para el sistema A. Consulte las hojas de trabajo de ejemplo a medida que sigue las instrucciones.

Puede entrar su propia información en las hojas de trabajo en blanco mientras sigue estos pasos para el reino Kerberos.

Este gráfico ilustra los archivos y registros del sistema que contienen información de nombres de host en el ejemplo que sigue.

Nota: La dirección IP 10.1.1.1 representa la dirección IP pública. Es una dirección propuesta solo a modo de ejemplo.



Detalles

Servidor DNS

- Contiene registros de recursos de datos que indican que la dirección IP `10.1.1.1` se correlaciona con el nombre de host `systema.myco.com`, que son la dirección IP y el nombre de host del sistema A.
- Podría utilizarlo el PC, el sistema A o ambos para la resolución de hosts.

Nota: En la demostración que se hace en este ejemplo tan solo se utiliza un servidor DNS. Aunque en la práctica se pueden utilizar varios servidores DNS. Por ejemplo, el PC podría utilizar un servidor DNS para resolver nombres de host y la plataforma System i podría utilizar otro servidor DNS. Tendrá que determinar cuántos servidores DNS se utilizan en su reino para la resolución de hosts y adaptar esta información a su caso particular.

PC

- Ejecuta el sistema operativo Windows 2000.
- Representa tanto el PC que sirve para administrar el servicio de autenticación de red como el PC que utiliza un usuario sin autorizaciones especiales para sus tareas rutinarias.
- Contiene el archivo `hosts` que indica que la dirección IP `10.1.1.1` se correlaciona con el nombre de host `systema.myco.com`.

Nota: El archivo de hosts se encuentra en estas carpetas:

- Sistema operativo Windows 2000: C:\WINNT\system32\drivers\etc\hosts
- Sistema operativo Windows XP y Windows Vista: C:\WINDOWS\system32\drivers\etc\hosts

Sistema A

- Ejecuta i5/OS V5R3.
- Contiene una aplicación de servicio a la que se tiene que acceder con el servicio de autenticación de red (autenticación Kerberos).
- En el menú Configurar TCP (CFGTCP), las opciones 10 y 12 indican la siguiente información del sistema A:
  - Opción 10 (Trabajar con entradas de tabla de hosts TCP/IP):
    - **Dirección Internet**: `10.1.1.1`
    - **Nombre de host**: `systema.myco.com`
  - Opción 12 (Cambiar información de dominio TCP/IP):
    - **Nombre de host**: `systema`
    - **Nombre de dominio**: `myco.com`
    - **Prioridad de búsqueda de nombres de host**: `*LOCAL` o `*REMOTE`

      Nota: El parámetro Prioridad de búsqueda de nombres de host indica *LOCAL o *REMOTE en función de la manera en que el administrador de la red haya configurado TCP/IP de cara a la resolución de hosts en el sistema.

Tabla 23. Ejemplo: Hoja de trabajo de resolución de nombres de host del PC

En el PC, determine el nombre de host del sistema A.		
Paso	**Origen**	**Nombre de host**
1.a.1	Archivo hosts del PC	systema.myco.com
1.b.1	Servidor DNS	systema.myco.com

Tabla 24. Ejemplo: Hoja de trabajo de resolución de nombres de host del i5/OS

En el sistema A, determine el nombre de host del sistema A.		
Paso	**Origen**	**Nombre de host**
2.a.2	Sistema A Menú CFGTCP, opción 12	**Nombre de host**: `systema` **Nombre de dominio**: `myco.com`
Nota: Valor de *Prioridad de búsqueda de nombres de host*: `*LOCAL` o `*REMOTE`		
2.b.2	Sistema A Menú CFGTCP, opción 10	systema.myco.com
2.c.1	Servidor DNS	systema.myco.com

Tabla 25. Ejemplo: Hoja de trabajo de nombres de host coincidentes

Estos tres nombres de host deben coincidir exactamente.	
Paso	**Nombre de host**
Paso 1	systema.myco.com
Paso 2.a.2	systema myco.com
2d	systema.myco.com

Puede utilizar las tres hojas de trabajo siguiente para verificar que los PC y las plataformas System i resuelvan el mismo nombre de host para el sistema en el que reside la aplicación de servicio.

Tabla 26. Hoja de trabajo de resolución de nombres de host del PC

En el PC, determine el nombre de host de la plataforma System i.		
Paso	**Origen**	**Nombre de host**
1.a.1	Archivo hosts del PC	
1.b.1	Servidor DNS	

Tabla 27. Hoja de trabajo de resolución de nombres de host del i5/OS

En la plataforma System i, determine el nombre de host de la plataforma System i.		
Paso	**Origen**	**Nombre de host**
2.a.2	System i Menú CFGTCP, opción 12	**Nombre de host**: **Nombre de dominio**:
Nota: el valor de *Prioridad de búsqueda de nombres de host* puede ser `*LOCAL` o `*REMOTE`		
2.b.2	System i Menú CFGTCP, opción 10	
2.c.1	Servidor DNS	

Tabla 28. Hoja de trabajo de nombres de host coincidentes

Estos tres nombres de host deben coincidir exactamente.	
Paso	**Nombre de host**
Paso 1	
Paso 2.a.2	
2d	

Resolver los nombres de host

Verificar que los PC y las plataformas System i resuelven el mismo nombre de host.

Utilice las hojas de trabajo de ejemplo anteriores como referencia para resolver los nombres de host. Para verificar que los PC y las plataformas System i resuelven el mismo nombre de host para el sistema A, siga estos pasos:

1. En el PC, determine el nombre de host TCP/IP totalmente calificado del sistema A.

   Nota: En función de cómo gestione la red, le interesará hacer esto en otros PC que se unan al entorno de inicio de sesión único (SSO).

   a. En el Explorador de Windows del PC, abra el archivo `hosts` en una de las siguientes ubicaciones:
      - Sistema operativo Windows 2000: C:\WINNT\system32\drivers\etc\hosts
      - Sistema operativo Windows XP: C:\WINDOWS\system32\drivers\etc\hosts

      Nota: Si el archivo `hosts` no existe en el PC, será que el PC utiliza un servidor DNS para resolver los nombres de host. En tal caso, vaya directamente al paso 1b.

      En la hoja de trabajo, anote la primera entrada de nombre de host del sistema A, fijándose si los caracteres están escritos en mayúsculas o minúsculas, por ejemplo, `systema.myco.com`.

Nota: Si el archivo hosts no contiene una entrada correspondiente al sistema A, significa que el PC utiliza un servidor DNS para resolver los nombres de host. En tal caso, consulte el paso 1b.

b. Utilice NSLOOKUP para consultar el servidor DNS.

Nota: Si ha encontrado una entrada de nombre de host en el archivo `hosts` del PC, sáltese este paso y continúe en el paso 2 (el archivo `hosts` tiene prioridad sobre los servidores DNS cuando el sistema operativo resuelve nombres de host del PC).

1) En un indicador de mandatos, teclee `NSLOOKUP` y pulse Intro. En el indicador de NSLOOKUP, escriba `10.1.1.1` para solicitar al servidor de DNS el sistema A. Escriba el nombre de host devuelto por el servidor DNS, anotando los caracteres en minúsculas y mayúsculas, por ejemplo, `systema.myco.com`.
2) En el indicador de NSLOOKUP, teclee `systema.myco.com`. Este debe ser el nombre de host devuelto por el servidor DNS en el paso anterior. Verifique que el servidor DNS devuelve la dirección IP que prevista, por ejemplo, `10.1.1.1`.

Nota: Si NSLOOKUP no devuelve los resultados previstos, la configuración del DNS debe estar incompleta. Por ejemplo, si NSLOOKUP devuelve una dirección IP distinta de la que entró en el paso 1.b.1, tendrá que ponerse en contacto con el administrador del DNS para solucionar este problema y poder continuar realizando los pasos siguientes.

2. En el sistema A, determine el nombre de host TCP/IP totalmente calificado que le corresponde.
   a. Información de dominio TCP/IP
      1) En el indicador de mandatos, teclee `CFGTCP` y seleccione la opción 12 (Cambiar dominio TCP/IP).
      2) Tome nota de los valores del parámetro *Nombre de host* y del parámetro *Nombre de dominio*, fijándose en si están escritos con mayúscula o minúscula. Por ejemplo:
         - **Nombre de host**: `systema`
         - **Nombre de dominio**: `myco.com`
      3) Tome nota del valor del parámetro *Prioridad de búsqueda de nombres de host*.
         - `*LOCAL`: el sistema operativo busca en la tabla de hosts local (que equivale al archivo `hosts` del PC) en primer lugar. Si no hay ninguna entrada coincidente en la tabla de hosts y ha configurado un servidor DNS, el sistema operativo buscará entonces en el servidor DNS.
         - `*REMOTE`: el sistema operativo busca en el servidor DNS en primer lugar. Si no hay ninguna entrada coincidente en el servidor DNS, el sistema operativo buscará entonces en la tabla de hosts local.
   b. Tabla de hosts TCP/IP
      1) En el indicador de mandatos, teclee `CFGTCP` y seleccione la opción 10 (Trabajar con entradas de tabla de hosts TCP/IP).
      2) Tome nota del valor de la columna *Nombre de host* que se corresponde con el sistema A (dirección IP 10.1.1.1), fijándose en si los caracteres están escritos en mayúsculas o minúsculas, por ejemplo, `systema.myco.com`.

Nota: Si no encuentra una entrada correspondiente al sistema A en la tabla de hosts, siga en el próximo paso.

   c. Servidor DNS
      1) En un indicador de mandatos, teclee `NSLOOKUP` y pulse Intro. En el indicador de NSLOOKUP, escriba `10.1.1.1` para solicitar al servidor de DNS el sistema A. Escriba el nombre de host devuelto por el servidor DNS, anotando los caracteres en minúsculas y mayúsculas, por ejemplo, `systema.myco.com`.
      2) En el indicador de NSLOOKUP, teclee `systema.myco.com`. Este debe ser el nombre de host devuelto por el servidor DNS en el paso anterior. Verifique que el servidor DNS devuelve la dirección IP que prevista, por ejemplo, `10.1.1.1`.

Nota: Si NSLOOKUP no devuelve los resultados previstos, la configuración del DNS debe estar incompleta. Por ejemplo, si NSLOOKUP devuelve una dirección IP distinta de la que entró en el paso 2.c.1, tendrá que ponerse en contacto con el administrador del DNS para solucionar este problema y poder continuar realizando los pasos siguientes.

d. Determine qué valor de nombre de host del sistema A hay que conservar, tomando como base la correspondiente configuración TCP/IP.
   - Si el valor del parámetro *Prioridad de búsqueda de nombres de host* es `*LOCAL`, conserve la entrada anotada en la tabla de hosts (paso 2.b.2).
   - Si el valor del parámetro *Prioridad de búsqueda de nombres de host* es `*REMOTE`, conserve la entrada anotada en el servidor DNS (paso 2.c.1).
   - Si solo uno de los dos orígenes contiene una entrada correspondiente al sistema A, conserve esa entrada.

3. Compare los resultados de estos pasos:
   a. Paso 1: Nombre utilizado por el PC para el sistema A.

      Nota: Si encuentra una entrada correspondiente al sistema A en el archivo hosts del PC, utilice esa entrada. En caso contrario, utilice la entrada del servidor DNS.

   b. Paso 2.a.2: Nombre que se da a sí mismo el sistema A en su configuración TCP/IP.
   c. Paso 2d: Nombre que se da a sí mismo el sistema A basándose en la resolución de nombres de host.

   Estas tres entradas deben coincidir exactamente, incluidas las mayúsculas y las minúsculas. Si los resultados no coinciden exactamente, recibirá un mensaje de error que indica que no se puede encontrar una entrada de tabla de claves.

Hojas de trabajo para la planificación del servicio de autenticación de red

Para configurar satisfactoriamente el servicio de autenticación de red, debe comprender los requisitos y llevar a cabo los pasos de planificación necesarios.

Este tema proporciona una hoja de trabajo de prerrequisitos y una hoja de trabajo de planificación que le permitirán asegurarse de que ha llevado a cabo todos los pasos necesarios. A la hora de planificar una implementación Kerberos y configurar el servicio de autenticación de red, utilice las siguientes hojas de trabajo:

Hoja de trabajo de prerrequisitos

Con esta hoja de trabajo de planificación podrá asegurarse de que ha cumplido con todos los prerrequisitos. Antes de pasar a las tareas de configuración, debe poder responder afirmativamente a todas las preguntas relacionadas con los prerrequisitos.

Tabla 29. Hoja de trabajo de prerrequisitos

Preguntas	Respuestas
¿La versión de i5/OS es V5R3 o posterior (5722-SS1), o bien V6R1 (5761-SS1)?	
Si utiliza i5/OS V5R3, ¿está instalado el producto Cryptographic Access Provider (5722-AC3) en sus sistemas? Si utiliza i5/OS V5R4 o posterior, ¿está instalado el producto Network Authentication Enablement (5722-NAE o 5761-NAE) en sus sistemas?	
¿Ha instalado System i Access para Windows (5722-XE1 o 5761-XE1) en el PC del administrador y en sus sistemas?	
¿Está el subcomponente de seguridad de System i Navigator instalado en el PC del administrador?	

Tabla 29. Hoja de trabajo de prerrequisitos (continuación)

Preguntas	Respuestas
¿Está el subcomponente de red de System i Navigator instalado en el PC del administrador?	
¿Ha instalado el último Service Pack de IBM System i Access para Windows? Consulte System i Access para obtener el paquete de servicio más reciente.	
¿Tiene las autorizaciones especiales *SECADM, *ALLOBJ e *IOSYSCFG?	
¿Ha instalado alguno de los siguientes sistemas operativos en un sistema seguro que funcionará como servidor Kerberos? ¿Cuál? 1. Windows 2000 Server 2. Windows Server 2003 3. AIX Server 4. i5/OS PASE (V5R3 o posterior) 5. z/OS	
Para Windows 2000 Server y Windows Server 2003, ¿ha instalado las herramientas de soporte de Windows (que proporcionan la herramienta ktpass) en el sistema que se utiliza como centro de distribución de claves (KDC)?	
Si el servidor Kerberos está en un servidor Windows 2000 ó 2003, ¿están todos los PC de la red configurados en un dominio Windows?	
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	
La hora del sistema en el System i, ¿difiere en menos de cinco minutos de la hora del sistema en el servidor Kerberos? Si la diferencia es superior, consulte “Sincronizar las horas de los sistemas” en la página 105.	

Tabla 30. Hoja de trabajo de planificación del servidor Kerberos

Preguntas	Respuestas
¿En qué sistema operativo se propone configurar el servidor Kerberos? • Windows 2000 Server • Windows Server 2003 • AIX Server • i5/OS PASE (V5R3 o posterior) • z/OS	
¿Cuál es el nombre de dominio totalmente calificado del servidor Kerberos?	
¿Están sincronizadas las horas entre los PC y los sistemas que se conectan al servidor Kerberos? ¿Cuál es el desvío horario máximo?	

Tabla 31. Hoja de trabajo de planificación del reino Kerberos

Preguntas	Respuestas
¿Cuántos reinos necesita?	
¿Cómo se propone organizar los reinos?	
¿Qué convenio de denominación utilizará para los reinos?	

Tabla 32. Hoja de trabajo de planificación de sujetos principales

Preguntas	Respuestas
¿Qué convenio de denominación se propone utilizar para los sujetos principales Kerberos que representan a los usuarios de la red?	
¿Qué convenio de denominación utilizará para las aplicaciones de la red?	
¿Para qué servicios de i5/OS piensa utilizar la autenticación Kerberos?	
¿Qué nombres de sujeto principal de i5/OS tiene cada uno de dichos servicios de i5/OS?	

Tabla 33. Hoja de trabajo para las consideraciones sobre la resolución de nombres de host

Pregunta	Respuesta
Los PC y la plataforma System i, ¿utilizan el mismo servidor DNS para resolver los nombres de host?	
¿Piensa utilizar una tabla de hosts en la plataforma System i para resolver los nombres de host?	
El PC y la plataforma System i, ¿resuelven el mismo nombre de host para la plataforma System i? Hallará ayuda en el tema "Consideraciones sobre la resolución de nombres de host" en la página 85.	

La siguiente hoja de trabajo de planificación ilustra el tipo de información que necesita antes de empezar a configurar el servidor Kerberos en i5/OS PASE y el servicio de autenticación de red. Podrá proseguir con la configuración del servidor Kerberos en i5/OS PASE cuando haya respondido a todas las preguntas de la hoja de trabajo de prerrequisitos.

Tabla 34. Hoja de trabajo de planificación de i5/OS PASE

Preguntas	Respuestas
¿Tiene instalado PASE?	
¿Qué nombre tiene el reino predeterminado?	
¿Cuál es el servidor Kerberos del reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	
¿Cuál es el convenio de denominación de los sujetos principales que representan a los usuarios de la red?	
¿Qué nombres de sujeto principal tienen sus usuarios en la red?	

La siguiente hoja de trabajo de planificación le ayudará a reunir la información que necesita antes de empezar a configurar el servicio de autenticación de red. Podrá proseguir con la configuración del servicio de autenticación de red cuando haya respondido a todas las preguntas de la hoja de trabajo de prerrequisitos.

Tabla 35. Hoja de trabajo de planificación del servicio de autenticación de red

Preguntas	Respuestas
¿Cuál es el nombre del reino Kerberos predeterminado al que pertenecerá el sistema? **Nota:** Los dominios en Windows 2000 son similares a los reinos en Kerberos. Microsoft Active Directory utiliza la autenticación de Kerberos como mecanismo de seguridad predeterminado.	

Tabla 35. Hoja de trabajo de planificación del servicio de autenticación de red (continuación)

Preguntas	Respuestas
¿Está utilizando Microsoft Active Directory?	
¿Cuál es el servidor Kerberos del reino Kerberos predeterminado? ¿En qué puerto está a la escucha el servidor Kerberos?	
¿Desea configurar un servidor de contraseñas para este reino predeterminado? Si es así, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este servidor Kerberos? ¿En qué puerto está a la escucha el servidor de contraseñas?	
¿Para qué servicios desea crear entradas de tabla de claves? • Autenticación de Kerberos de i5/OS • LDAP • IBM HTTP Server • i5/OS NetServer • Servidor del sistema de archivos de red	
Si se propone crear un sujeto principal de servicio para la autenticación Kerberos de i5/OS, ¿cuál será su contraseña?	
Si se propone crear un sujeto principal de servicio para LDAP, ¿cuál será su contraseña?	
Si se propone crear un sujeto principal de servicio para HTTP Server, ¿cuál será su contraseña?	
Si se propone crear un sujeto principal de servicio para i5/OS NetServer, ¿cuál será su contraseña? **Nota:** Cuando aparezca el asistente de servicio de autenticación de red, se crearán varios sujetos principales para i5/OS NetServer. Anótelos aquí a medida que se visualicen en el asistente. Los necesitará para añadirlos al servidor Kerberos.	
Si se propone crear un sujeto principal de servicio para el Servidor del sistema de archivos de red, ¿cuál será su contraseña?	
¿Desea crear un archivo por lotes para automatizar la adición de sujetos principales de servicio a Microsoft Active Directory?	
¿Desea incluir las contraseñas con los sujetos principales de servicio de i5/OS en el archivo por lotes?	

Configurar el servicio de autenticación de red

El servicio de autenticación de red permite que el producto System i participe en una red Kerberos existente. El servicio de autenticación de red presupone que se tiene un servidor Kerberos configurado en un sistema seguro de la red.

Configurar un servidor Kerberos

Actualmente es posible configurar un servidor Kerberos en el entorno de soluciones de aplicaciones portables (PASE) de i5/OS (i5/OS PASE). Además de este soporte de i5/OS, la plataforma System i también interactúa con Microsoft Windows 2000, Windows 2003, AIX Server y z/OS. Utilice la siguiente información como ayuda para configurar un servidor Kerberos en cada una de estas plataformas:

- Windows 2000 Server
- z/OS Security Server Network Authentication Service Administration

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*

  Nota: Encontrará esta documentación en el CD del paquete de ampliación y Bonus Pack de AIX 5L  .

Configurar un servidor Kerberos en i5/OS PASE

1. "Configurar un servidor Kerberos en i5/OS PASE"
2. "Cambiar los valores de cifrado en el servidor Kerberos" en la página 95
3. "Detener y reiniciar el servidor Kerberos" en la página 95
4. "Crear sujetos principales de host, usuario y servicio" en la página 96
5. "Configurar estaciones de trabajo Windows 2000, Windows XP y Windows Vista" en la página 96
6. "Configurar un servidor Kerberos secundario" en la página 97

Configurar el servicio de autenticación de red en la plataforma System i

1. "Configurar el servicio de autenticación de red" en la página 99
2. "Añadir sujetos principales i5/OS al servidor Kerberos" en la página 101
3. "Crear un directorio inicial" en la página 103
4. "Probar la configuración del servicio de autenticación de red" en la página 103

Configurar un servidor Kerberos en i5/OS PASE

Para proporcionar un entorno de ejecución integrado para las aplicaciones AIX, configure y gestione un servidor Kerberos desde la plataforma System i.

i5/OS permite utilizar un servidor Kerberos en el entorno de soluciones de aplicaciones portables (PASE) de i5/OS. i5/OS PASE proporciona un entorno de tiempo de ejecución integrado para las aplicaciones AIX. Podrá configurar y gestionar un servidor Kerberos desde la plataforma System i. Para configurar un servidor Kerberos en i5/OS PASE, siga los pasos siguientes:

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en el indicador de mandatos. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, especifique `config.krb5 -S -d systema.myco.com -r MYCO.COM`, donde `-d` es el DNS de la red y `-r` es el nombre de reino (en este ejemplo, myco.com es el nombre de DNS y MYCO.COM es el nombre de reino). Este mandato actualiza el archivo krb5.config con el nombre de dominio y el reino del servidor Kerberos, crea la base de datos Kerberos en el sistema de archivos integrado y configura el servidor Kerberos en i5/OS PASE. Se le pedirá que añada una contraseña maestra de base de datos y una contraseña para el sujeto principal admin/admin que se utiliza para administrar el servidor Kerberos.

   Nota: En V5R3 y V5R4, sólo se puede utilizar la base de datos existente para almacenar sujetos principales Kerberos. El conector del directorio LDAP todavía no se puede utilizar para ello.
4. Opcional: Si desea que el servidor Kerberos y el servidor de administración se inicien automáticamente durante una carga del programa inicial (IPL), tendrá que realizar dos pasos adicionales. Deberá crear una descripción de trabajo y añadir una entrada de trabajo de inicio automático. Para configurar el i5/OS para que inicie automáticamente el servidor Kerberos y el servidor de administración durante una IPL, siga estos pasos:
   a. Crear una descripción de trabajo.

      En una línea de mandatos de i5/OS, escriba el mandato siguiente, donde *xxxxxx* es el perfil de usuario de i5/OS con la autorización de usuario *ALLOBJ:

```
CRTJOBD JOBD(QGPL/KRB5PASE) JOBQ(QSYS/QSYSNOMAX) TEXT('Iniciar KDC y servidor admin en
PASE') USER(xxxxxx) RQSDTA('QSYS/CALL PGM(QSYS/QP2SHELL) PARM(''/usr/krb5/sbin/
start.krb5'')') SYNTAX(*NOCHK) INLLIBL(*SYSVAL) ENDSEV( 30)
```

b. Añadir una entrada de trabajo de inicio automático. En la línea de mandatos, escriba el mandato siguiente:

```
ADDAJE SBSD(QSYS/QSYSWRK) JOB(KRB5PASE) JOBD(QGPL/KRB5PASE).
```

Nota: En vez de iniciar los servidores durante una IPL, también puede iniciarlos manualmente después de la IPL, siguiendo estos pasos:

a. En una interfaz basada en caracteres, teclee `call QP2TERM` para abrir el entorno de shell interactivo de i5/OS PASE.

b. En la línea de mandatos, escriba `/usr/krb5/sbin/start.krb5` para iniciar los servidores.

Qué hacer a continuación

Si utiliza estaciones de trabajo Windows 2000, Windows XP o Windows Vista con un servidor Kerberos que no está configurado mediante Windows 2000 Active Directory (como puede ser un servidor Kerberos en i5/OS PASE), debe realizar varios pasos de configuración en el servidor Kerberos y en la estación de trabajo para asegurarse de que la autenticación Kerberos funciona como es debido.

Cambiar los valores de cifrado en el servidor Kerberos

Para trabajar con las estaciones de trabajo Windows, hay que cambiar los valores de cifrado por omisión del servidor Kerberos para que los clientes se puedan autenticar ante el servidor Kerberos de i5/OS PASE.

Para cambiar los valores de cifrado por omisión, tiene que editar el archivo kdc.conf situado en el directorio /etc/krb5 siguiendo estos pasos:

1. En una interfaz basada en caracteres, escriba `edtf '/var/krb5/krb5kdc/kdc.conf'` para acceder al archivo kdc.conf.
2. Cambie las siguientes líneas del archivo kdc.conf:

```
supported_enctypes = des3-cbc-sha1:normal
arcfour-hmac:normal aes256-cts:normal
des-cbc-md5:normal des-cbc-crc:normal
```

para que sean

```
supported_enctypes = des-cbc-crc:normal des-cbc-md5:normal
```

Detener y reiniciar el servidor Kerberos

Debe detener y reiniciar el servidor Kerberos en i5/OS PASE para actualizar los valores de cifrado que acaba de cambiar.

Siga estos pasos:

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `stop.krb5`. Este mandato detiene el servidor Kerberos.
4. En la línea de mandatos, escriba `start.krb5`. Este mandato inicia el servidor Kerberos.

Crear sujetos principales de host, usuario y servicio

Este es el procedimiento para crear sujetos principales de host para las estaciones de trabajo Windows 2000, Windows XP y Windows Vista, así como para crear sujetos principales de usuario y servicio en el servidor Kerberos.

Por cuestión de interoperatividad entre una estación de trabajo Windows 2000, Windows XP o Windows Vista y un servidor Kerberos de i5/OS PASE, tendrá que añadir un sujeto principal de host de la estación de trabajo al reino Kerberos. Para que los usuarios se autentiquen ante los servicios de la red, debe añadirlos al servidor Kerberos como sujetos principales. Estos sujetos principales de usuario se almacenan en el servidor Kerberos y sirven para validar a los usuarios de la red. Para que i5/OS acepte los tickets Kerberos, debe añadirlos al servidor Kerberos como sujetos principales. Realice las siguientes tareas:

Nota: Los nombres de usuario, los nombres de host y las contraseñas tan solo se utilizan a modo de ejemplo.

1. En una interfaz basada en caracteres, especifique `call QP2TERM` en la línea de mandatos. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En la línea de mandatos, escriba `kadmin -p admin/admin` y pulse Intro.
4. Inicie sesión con la contraseña de administrador.
5. En el indicador de kadmin, escriba `addprinc -pw secret1 host/pc1.myco.com`. Este mandato crea un sujeto principal de host para el PC de la red. Repita este paso para todos los PC de la red.
6. Escriba `addprinc -pw secret jonesm`. Este mandato crea un sujeto principal para el usuario Mary Jones. Repita este paso para todos los usuarios.
7. En el indicador de kadmin, escriba `addprinc -pw systema123 krbsvr400/systema.myco.com`. Este mandato crea un sujeto principal de servicio para el servidor Kerberos.
8. Escriba `quit` para salir de la interfaz kadmin y pulse F3 (Salir) para salir del entorno PASE.

Configurar estaciones de trabajo Windows 2000, Windows XP y Windows Vista

Para configurar estaciones de trabajo de cliente, establezca el reino Kerberos y el servidor Kerberos.

Tras haber creado un sujeto principal de host para la estación de trabajo Windows 2000 en el servidor Kerberos de i5/OS PASE, debe configurar las estaciones de trabajo clientes. Tendrá que hacer esta parte del cliente de un grupo de trabajo estableciendo el reino Kerberos y el servidor Kerberos en la estación de trabajo. También tendrá que fijar una contraseña para que se asocie a la estación de trabajo. Para configurar las estaciones de trabajo, siga estos pasos:

Nota: Los nombres de usuario, los nombres de sistema principal y las contraseñas tan solo se utilizan a modo de ejemplo.

1. En un indicador de mandato de la estación de trabajo Windows 2000, escriba:

```
C:> ksetup /setdomain NOMBRE.REINO.COM
C:> ksetup /addkdc NOMBRE.REINO.COM kdc1.hostname.com
```

   Por ejemplo, el administrador de MyCo, Inc., escribiría:

```
C:> ksetup /setdomain MYCO.COM
C:> ksetup /addkdc MYCO.COM kdc1.myco.com
```

2. Establezca la contraseña de la cuenta de la máquina local escribiendo lo siguiente en el indicador de mandatos de la estación de trabajo Windows 2000:

```
C:> ksetup /setmachpassword contraseña
```

Esta contraseña debe coincidir con la que se utilizó al crear el sujeto principal de sistema principal, `pc1.myco.com`. Por ejemplo, el usuario de MyCo, Inc., escribiría:

```
C:> ksetup /setmachpassword secret1
```

3. Correlacione el usuario de Kerberos con un usuario local escribiendo lo siguiente en el indicador de mandatos de la estación de trabajo Windows 2000:

```
C:> ksetup /mapuser jonesm@MYCO.COM maryjones
```

4. Reinicie la máquina para que los cambios entren en vigor.

Si lo desea, puede configurar un servidor Kerberos secundario para utilizarlo a modo de servidor de reserva si el servidor Kerberos primario se queda fuera de servicio o si está demasiado ocupado para manejar las peticiones. Encontrará instrucciones detalladas en el tema “Configurar un servidor Kerberos secundario”.

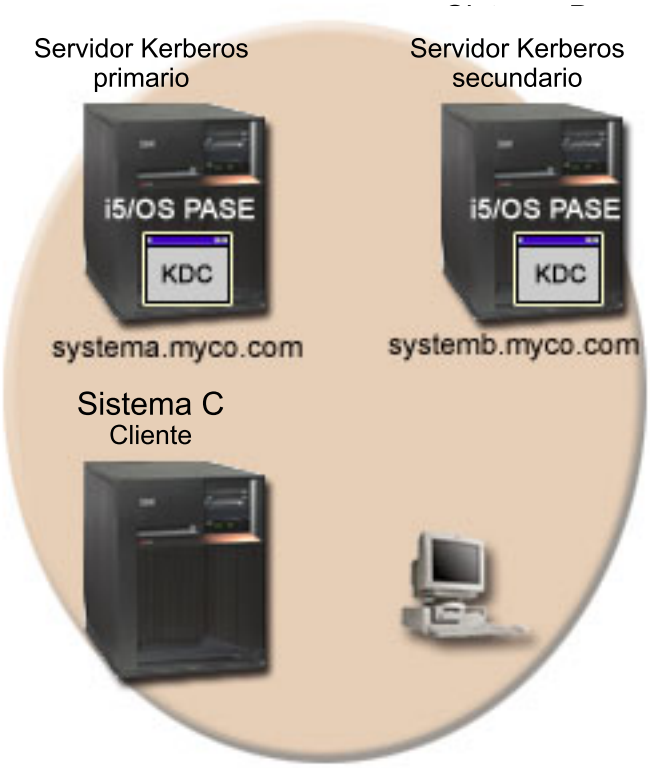
Configurar un servidor Kerberos secundario

Después de haber configurado el servidor Kerberos primario en i5/OS PASE, puede configurar opcionalmente un servidor Kerberos secundario para utilizarlo como servidor de reserva en el caso de que el servidor Kerberos primario falle o esté demasiado ocupado para manejar peticiones.

Por ejemplo, supongamos que en este momento utiliza el sistema A como servidor Kerberos. Ahora desea configurar el sistema B para que sea su servidor Kerberos secundario (de reserva).

Nota: El servidor Kerberos también se conoce como centro de distribución de claves (KDC).

La siguiente figura ilustra los productos System i mencionados en las instrucciones que figuran a continuación.



Detalles

- La figura ilustra los productos System i tal como son después de haber seguido los pasos para configurar un servidor Kerberos secundario:
  - El sistema A funciona como servidor Kerberos primario configurado en i5/OS PASE.
  - El sistema B funciona como servidor Kerberos secundario configurado en i5/OS PASE.
  - El sistema C funciona como cliente habilitado para utilizar el sistema B como servidor Kerberos.

Para configurar el sistema B para que sea un servidor Kerberos secundario en i5/OS PASE, siga estos pasos:

1. Configure el sistema B como cliente.
   a. En una interfaz basada en caracteres del sistema B, escriba `call QP2TERM`. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
   b. En la línea de mandatos, escriba el mandato siguiente:

      ```
      export PATH=$PATH:/usr/krb5/sbin
      ```

      Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
   c. En la línea de mandatos, escriba:

      ```
      config.krb5 -E -d rchland.ibm.com -r MYCO.COM -s lp16b1b.rchland.ibm.com
      ```
   d. Escriba la contraseña del administrador; por ejemplo: `secret`

   El mandato config.krb5 configura el cliente, el servidor primario y el servidor secundario. El distintivo **-C** configura el cliente en el sistema C. El distintivo **-s** configura el servidor Kerberos primario en el sistema A. El distintivo **-E** configura el servidor Kerberos secundario en el sistema B.
2. Añada un sujeto principal de i5/OS para los sistemas A y B al servidor Kerberos del sistema A.

a. En una interfaz basada en caracteres del sistema A, escriba `call QP2TERM`. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
b. En la línea de mandatos, escriba:

```
export PATH=$PATH:/usr/krb5/sbin
```

Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
c. En la línea de mandatos, escriba `kadmin -p admin/admin`.
d. Inicie sesión con la contraseña de administrador. Por ejemplo, `secret`.
e. En la línea de mandatos, escriba el mandato siguiente:

```
addprinc -randkey -clearpolicy host/systema.myco.com
```

f. En la línea de mandatos, escriba el mandato siguiente:

```
addprinc -randkey -clearpolicy host/systemb.myco.com
```

3. Propague la base de datos maestra del servidor Kerberos primario al servidor Kerberos secundario.
a. En una interfaz basada en caracteres del sistema A, escriba `call QP2TERM`. Este mandato abre un entorno de shell interactivo en el que puede trabajar con aplicaciones de i5/OS PASE.
b. En la línea de mandatos, escriba el mandato siguiente:

```
export PATH=$PATH:/usr/krb5/sbin
```

Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
c. En la línea de mandatos, escriba:

```
/usr/krb5/sbin/config.krb5 -P -r MYCO.COM -d rchland.ibm.com -e rchasrc2.rchland.ibm.com
```

Consejo: Puede cortar y pegar el mandato en el mensaje del sistema Kerberos primario.

El distintivo **-P** propaga la base de datos maestra del servidor Kerberos primario al servidor Kerberos secundario. El distintivo **-r** especifica el nombre del reino. El distintivo **-d** especifica el nombre del dominio DNS. El distintivo **-e** especifica el nombre de host del servidor Kerberos secundario.
4. En el servidor Kerberos secundario, verifique que la base de datos maestra se ha propagado satisfactoriamente.
a. En el servidor Kerberos secundario, responda `Y` (Sí) a la siguiente solicitud: `¿Ha ejecutado satisfactoriamente el mandato anterior?`
b. Escriba la contraseña maestra de base de datos; por ejemplo: `pasepwd`. Este mandato recoge la contraseña maestra.

Configurar el servicio de autenticación de red

Estos son los prerrequisitos y procedimientos para configurar el servicio de autenticación de red en los sistemas.

Antes de configurar el servicio de autenticación de red, debe llevar a cabo las siguientes tareas:

- Cumplimentar las hojas de trabajo de planificación necesarias.
- Verificar que los PC y las plataformas System i, cuando efectúan la resolución de nombres de host, los resuelven en los mismos nombres de host de los productos System i. Encontrará esta tarea en el tema “Consideraciones sobre la resolución de nombres de host” en la página 85.
- Configurar un servidor Kerberos en un sistema seguro de la red. Si ha configurado un servidor Kerberos en i5/OS PASE, asegúrese de que ha llevado a cabo todos los pasos de configuración necesarios de las estaciones de trabajo de cliente y servidor antes de configurar la autenticación de red

en la plataforma System i. En el tema “Configurar un servidor Kerberos en i5/OS PASE” en la página 94 encontrará los detalles para configurar un servidor Kerberos en i5/OS PASE.

También puede tener un servidor Kerberos configurado en Microsoft Windows 2000, Windows Server 2003 y z/OS. Consulte la documentación pertinente que corresponde a la configuración Kerberos del sistema que se empleará como servidor Kerberos.

Configure el servidor Kerberos antes de configurar el servicio de autenticación de red en la plataforma System i.

Para configurar el servicio de autenticación de red, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Configurar** para iniciar el asistente de configuración.

   Nota: Tras configurar el servicio de autenticación de red, esta opción indicará **Reconfigurar**.
3. En la página de bienvenida encontrará información sobre los objetos que crea el asistente. Pulse **Siguiente**.
4. En la página Especificar información de reino, entre el nombre del reino predeterminado en el campo **Reino predeterminado**. Si se propone utilizar Microsoft Active Directory para la autenticación Kerberos, seleccione **Se utiliza Microsoft Active Directory para la autenticación Kerberos**. Pulse **Siguiente**.
5. En la página Especificar información de KDC, escriba el nombre del servidor Kerberos de este reino en el campo **KDC** y escriba 88 en el campo **Puerto**. Pulse **Siguiente**.
6. En la página Especificar información de contraseña, seleccione **Sí** o **No** para configurar un servidor de contraseñas. El servidor de contraseñas permite a los sujetos principales cambiar las contraseñas en el servidor Kerberos. Si selecciona **Sí**, entre el nombre del servidor de contraseñas en el campo **Servidor de contraseñas**. El puerto predeterminado del servidor de contraseñas es el 464. Pulse **Siguiente**.
7. En la página Seleccionar entradas de tabla de claves, seleccione **Autenticación Kerberos de i5/OS**. También puede crear entradas de tabla de claves para los servicios de directorio (LDAP), i5/OS NetServer, servidor HTTP y servidor NFS (Network File System), si desea que estos servicios utilicen la autenticación Kerberos.

   Nota: Para algunos de estos servicios se necesita una configuración adicional con vistas a utilizar la autenticación Kerberos.
   Pulse **Siguiente**.
8. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña y confírmela. Pulse **Siguiente**.

   Nota: Se trata de la misma contraseña que utilizará cuando añada los sujetos principales de i5/OS al servidor Kerberos.
9. En la página Crear archivo por lotes, seleccione **Sí** para que se cree este archivo.

   Nota: Esta página solo aparece si ha seleccionado **Se utiliza Microsoft Active Directory para la autenticación Kerberos** en el paso 4 (más arriba).
10. En el campo **Archivo por lotes**, actualice la vía de acceso del directorio. Puede pulsar **Examinar** para localizar la vía de acceso de directorio pertinente y editarla en el campo.
11. En el campo **Incluir contraseña**, seleccione **Sí**. Así se asegura de que todas las contraseñas asociadas al sujeto principal de servicio de i5/OS se incluyen en el archivo por lotes. Es importante que se fije en que las contraseñas se visualizan en texto sin cifrar y que pueden leerlas todas las personas que tengan acceso de lectura al archivo por lotes.

    Nota: Los sujetos principales de servicio generados por el asistente también se pueden añadir manualmente a Microsoft Active Directory. Si desea saber cómo se añaden manualmente los

sujetos principales de servicio de i5/OS a Microsoft Active Directory, consulte el tema “Añadir sujetos principales i5/OS al servidor Kerberos”.

12. En la página Resumen, lea los detalles de configuración del servicio de autenticación de red. Pulse **Finalizar**.

El servicio de autenticación de red ya está configurado.

Conceptos relacionados

“Gestionar el servicio de autenticación de red” en la página 104
Después de haber configurado el servicio de autenticación de red, podrá solicitar tickets, trabajar con archivos de tabla de claves y administrar la resolución de nombres de host. También podrá trabajar con los archivos de credenciales y hacer copias de seguridad de los archivos de configuración.

Añadir sujetos principales i5/OS al servidor Kerberos

Después de configurar el servicio de autenticación de red en la plataforma System i, debe añadir los sujetos principales de i5/OS al servidor Kerberos.

El servicio de autenticación de red proporciona un nombre de sujeto principal de i5/OS, **krbsvr400**, para el sistema y las aplicaciones i5/OS. El nombre del sujeto principal que representa i5/OS es krbsrv400/nombre_host_*System i@NOMBRE_REINO*, donde *nombre_host_System i* es el nombre de host totalmente calificado o el nombre corto de host de la plataforma System i. Este nombre de sujeto principal se tiene que añadir al servidor Kerberos para que las aplicaciones de cliente Kerberos puedan solicitar y recibir tickets de servicio. Por ejemplo, en nuestros casos prácticos de configuración, el administrador de MyCo añadió en sujeto principal de servicio krbsvr400/systema.myco.com@MYCO.COM al servidor Kerberos de la compañía.

Los pasos para añadir el sujeto principal de i5/OS variarán en función del sistema operativo en el que haya configurado un servidor Kerberos. Esta información facilita instrucciones para añadir los sujetos principales de i5/OS a un servidor Kerberos de un dominio i5/OS PASE o Windows 2000. Si ha creado opcionalmente sujetos principales de servicio para IBM Directory Server para i5/OS (LDAP), i5/OS NetServer, servidor NFS (Network File System) y servidor HTTP, también debe añadirlos al servidor Kerberos.

1. i5/OS PASE Si su servidor Kerberos está en i5/OS PASE, puede añadir los sujetos principales de servicio de i5/OS utilizando el mandato QP2TERM, que abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE. Para añadir un sujeto principal de servicio de i5/OS a un servidor Kerberos en i5/OS PASE, siga estos pasos:
   a. En una interfaz basada en caracteres, teclee call QP2TERM.
   b. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
   c. En la línea de mandatos, teclee `kadmin -p admin/admin`.
   d. Inicie sesión con su nombre de usuario y su contraseña.
   e. En la línea de mandatos de kadmin, escriba `addprinc -pw secret krbsvr400/System i totalmente calificado de nombre_host@REINO`, donde `secret` es la contraseña del sujeto principal de servicio de i5/OS. Por ejemplo, `krbsvr400/systema.myco.com@MYCO.COM` sería un nombre de sujeto principal de servicio válido para i5/OS.
2. Microsoft Active Directory

   Para añadir un sujeto principal de servicio de i5/OS a un servidor Kerberos, tiene dos opciones: permitir que el asistente del servicio de autenticación de red añada los sujetos principales o añadirlos usted manualmente.

   El asistente del servicio de autenticación de red le permite crear opcionalmente un archivo por lotes, que se llama `NASConfig.bat`. En este archivo por lotes están todos los nombres de sujeto principal de los servicios que haya seleccionado durante la configuración. También puede optar por añadir las contraseñas asociadas a los nombres en este archivo por lotes.

Nota: Si incluye la contraseña, se expone a que la vean las personas que tengan acceso de lectura al archivo por lotes. Le recomendamos que, si incluye la contraseña, suprima el archivo por lotes del servidor Kerberos y de su PC inmediatamente después de haberlo utilizado. Si no la incluye en el archivo por lotes, se le solicitará una contraseña cuando el archivo por lotes se ejecute en el servidor Windows.

Utilizar el archivo por lotes generado por el asistente del servicio de autenticación de red

a. Mediante FTP en la estación de trabajo Windows 2000 que el administrador ha utilizado para configurar el servicio de autenticación de red, abra un indicador de mandatos y teclee `ftp servidor`, siendo *servidor* el nombre de host del servidor Kerberos. Así se iniciará una sesión FTP en su PC. Se le pedirá el nombre de usuario y la contraseña de administrador.

b. En el indicador FTP, teclee `lcd "C:\Documents and Settings\All Users\Documents\IBM\Client Access"`. Pulse **Intro**.

   Nota: Este es un ejemplo de un directorio que podría contener el archivo por lotes. Debe recibir el mensaje `Directorio local es ahora C:\Documents and Settings\All Users\Documents\IBM\Client Access`.

c. En el indicador FTP, teclee `binary`. Esto indica que el archivo que se transferirá es binario.

d. En el indicador FTP, teclee `cd \midirectorio`, siendo *midirectorio* un directorio del servidor Windows en el que desee colocar el archivo por lotes.

e. En el indicador FTP, teclee `put NASConfig.bat`. Debe recibir el mensaje: `226 Transferencia completada`.

f. En el servidor Windows 2000, abra el directorio al que ha transferido el archivo por lotes.

g. Localice el archivo `NASConfig.bat` y púlselo dos veces para ejecutarlo.

h. Una vez ejecutado, verifique que el nombre de sujeto principal de i5/OS se ha añadido a Microsoft Active Directory; para ello, siga estos pasos:

   1) En el servidor Windows 2000, expanda **Inicio** → **Programas** → **Herramientas administrativas** → **Usuarios y equipos de Active Directory** → **Usuarios**.

   2) Verifique que la plataforma System i tiene una cuenta de usuario seleccionando el dominio Windows 2000 pertinente.

      Nota: Este dominio Windows debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.

   3) En la lista de usuarios visualizada, localice el nombre que se corresponde con el sujeto principal de servicio que acaba de añadir.

   4) Acceda a las propiedades de los usuarios de Active Directory. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**.

      Nota: Este paso opcional permite que su sistema delegue, o reenvíe, las credenciales de un usuario a otros sistemas. Como resultado, el sujeto principal de servicio de i5/OS podrá acceder a los servicios en múltiples sistemas en nombre del usuario. Esto resulta útil en una red multinivel.

Añadir manualmente el sujeto principal de servicio a Microsoft Active Directory También puede añadir los sujetos principales de i5/OS a Microsoft Active Directory de forma manual con el mandato ktpass. Este mandato se envía junto con las herramientas de soporte de Windows y debe estar instalado en el sistema que funciona como servidor Kerberos.

a. En el servidor Windows 2000, expanda **Inicio** → **Programas** → **Herramientas administrativas** → **Usuarios y equipos de Active Directory**.

b. Seleccione el dominio Windows 2000 al que desea añadir la cuenta de usuario de i5/OS y expanda **Acción** → **Nuevo** → **Usuario**.

   Nota: Este dominio Windows 2000 debe coincidir con el nombre de reino predeterminado que especificó para la configuración del servicio de autenticación de red.

c. En el campo **Nombre**, escriba un nombre que servirá para identificar la plataforma System i ante este dominio Windows 2000. Así se añadirá una cuenta de usuario nueva para la plataforma System i. Por ejemplo, el nombre `krbsvr400systema` o `httpsystema` podría ser un nombre válido para la cuenta de usuario.

d. Acceda a las propiedades del usuario de Active Directory que creó en el paso 3. En la pestaña **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá que el sujeto principal de servicio de i5/OS acceda a otros servicios en nombre de un usuario conectado.

e. Tiene que correlacionar la cuenta de usuario que acaba de crear con el sujeto principal de servicio de i5/OS utilizando el mandato ktpass. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows 2000 Server. Para correlacionar la cuenta de usuario, lleve a cabo esta tarea:

   1) En un indicador de mandatos, entre:

```
ktpass -mapuser krbsvr400systema -pass secret -princ krbsvr400/nombre-dominio-sistema@REINO
    -mapop set
```

   Nota: En el mandato, `krbsvr400systema` representa el nombre de la cuenta de usuario creada en el paso 3, y `secret` es la contraseña que escribió durante la configuración del servicio de autenticación de red para el sujeto principal de i5/OS.

Conceptos relacionados

"Resolución de problemas del servicio de autenticación de red" en la página 125
Se incluye información sobre la resolución de los problemas más habituales relacionados con el servicio de autenticación de red, la correlación de identidades de empresa (EIM) y las aplicaciones suministradas por IBM que admiten la autenticación Kerberos.

Crear un directorio inicial

Tras haber añadido el sujeto principal de i5/OS al servidor Kerberos, tendrá que crear un directorio `/home` para cada usuario que se conectará a las aplicaciones de i5/OS.

En este directorio habrá un archivo que contiene el nombre de la antememoria de credenciales Kerberos del usuario. Cada usuario debe ser el propietario de este directorio o bien tener la debida autorización para crear archivos en este directorio.

Para crear un directorio inicial para un usuario, siga este paso:

1. En una línea de mandatos de i5/OS, escriba `CRTDIR '/home/perfil usuario'`, siendo `perfil usuario` el perfil i5/OS del usuario.

   Nota: Si se propone utilizar este perfil de usuario como asociación EIM destino, el perfil de usuario ya debe existir y la contraseña se puede establecer en *NONE.

Probar la configuración del servicio de autenticación de red

Para probar la configuración del servicio de autenticación de red, solicite un ticket de otorgamiento de tickets para el sujeto principal de i5/OS.

Tras haber creado los directorios iniciales (home) de cada usuario que se conectará a las aplicaciones de i5/OS, podrá probar la configuración del servicio de autenticación de red solicitando un ticket de otorgamiento de tickets (TGT) para su sujeto principal de i5/OS. Antes de solicitar un ticket, debe asegurarse de que se han corregido los siguientes errores más comunes:

- ¿Tiene todos los prerrequisitos del servicio de autenticación de red?
- ¿Existe en el sistema operativo i5/OS un directorio inicial para el usuario que emite la petición de obtener un ticket? Encontrará los detalles en el tema "Crear un directorio inicial".
- ¿Tiene la contraseña correcta del sujeto principal de i5/OS? Esta contraseña se creó durante la Especifique de la autenticación de red y debe estar especificada en las hojas de trabajo de planificación.
- ¿Ha añadido el sujeto principal de i5/OS al servidor Kerberos? Encontrará los detalles en el tema "Añadir sujetos principales i5/OS al servidor Kerberos" en la página 101.

Para probar el servicio de autenticación de red, siga estos pasos:

1. En una línea de mandatos del intérprete Qshell, escriba `QSH` para iniciar el intérprete Qshell.
2. Entre `keytab list` para visualizar una lista de los sujetos principales registrados en el archivo de tabla de claves. Deben visualizarse los siguientes resultados:

```
Sujeto principal: krbsvr400/systema.myco.com@MYCO.COM
  Versión de clave: 2
  Tipo de clave: DES de 56 bits mediante derivación de clave
  Indicación de la hora de la entrada: 200X/05/29-11:02:58
```

3. Escriba `kinit -k krbsvr400/nombre de host totalmente calificado@NOMBRE REINO` para solicitar un ticket de otorgamiento de tickets (TGT) al servidor Kerberos. Por ejemplo, krbsvr400/systema.myco.com@MYCO.COM sería un nombre de sujeto principal válido para el sistema. Este mandato verifica que el sistema está debidamente configurado y que la contraseña del archivo de tabla de claves concuerda con la almacenada en el servidor Kerberos. Si la verificación es satisfactoria, el mandato QSH mostrará que no hay errores.
4. Escriba `klist` para verificar que el sujeto principal predeterminado es krbsvr400/nombre de host totalmente calificado@*NOMBRE REINO*. Este mandato visualiza el contenido de una memoria caché de credenciales Kerberos y verifica que se ha creado un ticket válido para el sujeto principal de servicio de i5/OS y que se ha colocado en la memoria caché de credenciales del sistema.

```
 Memoria caché de tickets: FILE:/QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/creds/krbcred

 Sujeto principal predeterminado: krbsvr400/systema.myco.com@MYCO.COM

Servidor: krbtgt/MYCO.COM@MYCO.COM
  Válido del 200X/06/09-12:08:45 al 20XX/11/05-03:08:45
$
```

Qué hacer a continuación:

Configurar la correlación de identidades de empresa (EIM)

Esta tarea es opcional si está utilizando el servicio de autenticación de red con sus propias aplicaciones. No obstante, le recomendamos que lleve a cabo esta tarea cuando utilice las aplicaciones suministradas por IBM, para crear un entorno de inicio de sesión único (SSO).

Gestionar el servicio de autenticación de red

Después de haber configurado el servicio de autenticación de red, podrá solicitar tickets, trabajar con archivos de tabla de claves y administrar la resolución de nombres de host. También podrá trabajar con los archivos de credenciales y hacer copias de seguridad de los archivos de configuración.

Tareas de usuario de System i

La plataforma System i también puede funcionar como cliente en una red habilitada para Kerberos. Los usuarios pueden iniciar sesión en el sistema y realizar tareas relacionadas con Kerberos mediante el intérprete Qshell. En las siguientes tareas se emplean varios mandatos de Qshell para realizar las tareas más comunes en relación con los usuarios.

- "Crear un directorio inicial" en la página 103
- "Obtener o renovar tickets de otorgamiento de tickets" en la página 108
- "Cambiar las contraseñas de Kerberos" en la página 115
- "Gestionar archivos de tabla de claves" en la página 113
- "Suprimir archivos de memoria caché de credenciales caducados" en la página 117
- "Visualizar memoria caché de credenciales" en la página 111

- "Gestionar entradas de servicio Kerberos en directorios LDAP" en la página 119

Nota: Si se propone utilizar el emulador PC5250 en System i Navigator, tendrá que cambiar el valor del sistema del **Inicio de sesión remoto** para que le permita eludir el inicio de sesión. Para cambiar el valor del sistema del **Inicio de sesión remoto**, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Configuración y servicio** → **Valores del sistema** → **Inicio de sesión**.
2. En la página Remoto, seleccione **Permitir eludir el inicio de sesión** y **Los ID de usuario origen y destino deben coincidir** y pulse **Aceptar**.

Tareas de administración del servicio de autenticación de red

Las tareas siguientes se pueden puede llevar a cabo por parte de un administrador en System i Navigator. Para obtener más información relacionada con las tareas, consulte la ayuda para el servicio de autenticación de red en System i Navigator.

Tareas relacionadas

"Configurar el servicio de autenticación de red" en la página 99
Estos son los prerrequisitos y procedimientos para configurar el servicio de autenticación de red en los sistemas.

Sincronizar las horas de los sistemas

El servicio de autenticación de red utiliza 5 minutos (300 segundos) como valor predeterminado de la diferencia máxima que puede haber entre las horas de los sistemas. Puede cambiar la diferencia horaria mediante la tarea de trabajar con las propiedades del servicio de autenticación de red.

Antes de sincronizar las horas de los sistemas, utilice el valor QTIMZON del sistema para establecer la hora del sistema según el huso horario que le corresponde. Puede sincronizar las horas de los sistemas cambiando la hora establecida en el servidor Kerberos o utilizando el valor QTIME del sistema para cambiar la hora del sistema del System i. Sin embargo, para mantener sincronizadas las horas de los sistemas en una red, debe configurar el protocolo simple de hora de red (SNTP). El SNTP permite que múltiples sistemas basen su hora en un solo servidor horario.

Para configurar el SNTP, siga estos pasos:

- Para configurar SNTP en una plataforma System i, escriba `CHGNTPA` en una línea de mandatos.
- Para configurar SNTP en los sistemas Windows, utilice **NET HELP TIME** para visualizar información de configuración de un servidor SNTP.

Conceptos relacionados

Protocolo simple de hora de red

Añadir reinos

Para poder añadir un reino a la configuración de i5/OS, debe configurar el servidor Kerberos para el reino nuevo. Para añadir un reino a la tarea del servicio de autenticación de red del i5/OS, necesita el nombre del reino, el nombre del servidor Kerberos y el puerto en el que está a la escucha.

Para añadir un reino al servicio de autenticación de red, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad** → **Servicio de autenticación de red**.
2. Pulse **Reinos** con el botón derecho del ratón y seleccione **Añadir reino**.
3. En el campo **Reino a añadir**, escriba el nombre de sistema principal del reino que desea añadir. Por ejemplo, un nombre de reino válido podría ser: MYCO.COM.
4. En el campo **KDC**, escriba el nombre del servidor Kerberos correspondiente al reino que se propone añadir. Por ejemplo, un nombre válido podría ser: kdc1.myco.com.

5. Escriba el número del puerto en el que el servidor Kerberos está a la escucha de las peticiones. Los números de puerto válidos son los comprendidos entre el 1 y el 65535. El puerto por omisión del servidor Kerberos es el 88.
6. Pulse **Aceptar**.

Suprimir reinos

Como administrador de la red, podría interesarle suprimir un reino innecesario y sin utilizar de la configuración del servicio de autenticación de red. Quizás también podría ser necesario eliminar un reino predeterminado como recuperación ante algún problema de aplicación con aplicaciones integradas en el sistema.

Por ejemplo, si ha configurado el servicio de autenticación de red sin configurar el servidor Kerberos en la red, QFileSvr.400 y la gestión de datos distribuidos (DDM) presupondrán que está utilizando la autenticación Kerberos. Antes de configurar la autenticación para estos productos, debe suprimir el reino predeterminado que ha especificado durante la configuración del servicio de autenticación de red.

Para suprimir un reino en el servicio de autenticación de red, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad** → **Servicio de autenticación de red** → **Reinos**.
2. Con el botón derecho del ratón, pulse el nombre del reino que desea suprimir y después seleccione **Suprimir**.
3. Pulse **Aceptar** para confirmar la supresión.

Añadir un servidor Kerberos a un reino

Puede añadir un servidor Kerberos a un reino utilizando el servicio de autenticación de red. Para poder añadir el servidor Kerberos al reino, primero debe conocer el nombre y el puerto de escucha.

Para añadir un centro de distribución de claves a un reino, lleve a cabo estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad** → **Servicio de autenticación de red** → **Reinos**.
2. Pulse el nombre del reino con el botón derecho del ratón en el panel de la derecha y seleccione **Propiedades**.
3. En la pestaña **General**, escriba en el campo **KDC** el nombre del servidor Kerberos que desea añadir a este reino. El servidor Kerberos es necesario para todos los reinos. Por ejemplo, una entrada válida sería kdc2.myco.com.
4. Escriba el número del puerto en el que el servidor Kerberos está a la escucha de las peticiones. Los números de puerto válidos son los comprendidos entre el 1 y el 65535. El puerto por omisión del servidor Kerberos es el 88.
5. Pulse **Añadir**. El nuevo servidor Kerberos aparecerá en la lista **Centro de distribución de claves (KDC) de este reino**.
6. Pulse **Aceptar**.

Añadir un servidor de contraseñas

El servidor de contraseñas permite a los sujetos principales Kerberos cambiar sus contraseñas.

Actualmente, i5/OS PASE no admite la configuración opcional de un servidor de contraseñas. Para cambiar las contraseñas de los sujetos principales en un servidor Kerberos de i5/OS PASE, debe entrar en el entorno PASE (call QP2TERM) y emitir el mandato kpasswd. A continuación figuran las instrucciones para actualizar la configuración del servicio de autenticación de red para que señale hacia un servidor de contraseñas nuevo o adicional del reino por omisión. Para añadir un servidor de contraseñas a un reino, lleve a cabo los pasos siguientes:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad** → **Servicio de autenticación de red** → **Reinos**.

2. Pulse el nombre del reino con el botón derecho del ratón en el panel de la derecha y seleccione **Propiedades**.
3. En la pestaña **Servidor de contraseñas**, escriba el nombre del servidor de contraseñas. Por ejemplo, un nombre válido para el servidor de contraseñas podría ser: psvr.myco.com.
4. Escriba el número del puerto que se corresponde con el servidor de contraseñas. Los números de puerto válidos son los comprendidos entre el 1 y el 65535. El puerto por omisión del servidor de contraseñas es el 464.
5. Pulse **Añadir**. El nuevo servidor de contraseñas se añadirá a la lista.
6. Pulse **Aceptar**.

Referencia relacionada

"kpasswd" en la página 116
El mandato kpasswd de Qshell cambia la contraseña de un sujeto principal Kerberos.

Crear una relación de confianza entre reinos

El establecimiento de una relación de confianza entre reinos crea un método abreviado para la autenticación.

Esta función es opcional porque, por omisión, el protocolo Kerberos busca la confianza en la jerarquía de reinos. Esta función resulta útil si tiene reinos en dominios diferentes y desea acelerar este proceso. Para configurar la confianza de reinos, cada servidor Kerberos de cada uno de los reinos debe compartir una clave. Para crear una relación de confianza en el servicio de autenticación de red, primero debe configurar los servidores Kerberos para que confíen entre sí. Para crear una relación de confianza entre reinos, siga estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad** → **Servicio de autenticación de red** → **Reino**.
2. Pulse el nombre del reino con el botón derecho del ratón en el panel de la derecha y seleccione **Propiedades**.
3. En la pestaña **Reinos de confianza**, escriba los nombres de los reinos para los que desea establecer una relación de confianza. Por ejemplo, los nombres ORDEPT.MYCO.COM y SHIPDEPT.MYCO.COM serían válidos para la relación de confianza.
4. Pulse **Añadir**. De este modo se añadirá la asociación de confianza a la tabla.
5. Pulse **Aceptar**.

Cambiar la resolución de hosts

Para resolver los nombres de host y los nombres de reino, especifique un servidor LDAP, un sistema de nombres de dominio (DNS) y correlaciones estáticas.

Con el servicio de autenticación de red, podrá especificar un servidor LDAP, un sistema de nombres de dominio (DNS) y correlaciones estáticas que se añadan al archivo de configuración para resolver los nombres de host y los nombres de reino. También podrá seleccionar estos tres métodos para resolver los nombres de host. Si selecciona todos estos métodos, el servicio de autenticación de red comprobará el servidor de directorio en primer lugar, las entradas del DNS en segundo lugar y, por último, las correlaciones estáticas para resolver los nombres de host.

Para cambiar la resolución de hosts, lleve a cabo los pasos siguientes:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Resolución de host, seleccione **Utilizar búsqueda LDAP**, **Utilizar búsqueda DNS** o **Utilizar correlaciones estáticas**.
4. Si selecciona **Utilizar búsqueda LDAP** como tipo de resolución de hosts, escriba el nombre del servidor de directorio y el puerto que le corresponde. Por ejemplo, ldapsrv.myco.com sería un nombre válido para el servidor de directorio. Los números de puerto válidos son los comprendidos entre el 1

y el 65535. El puerto predeterminado del servidor de directorio es el 389. Después de indicar que utilizará un servidor LDAP para manejar la resolución de nombres de host, debe asegurarse de que el reino se ha definido correctamente en el servidor LDAP. Consulte el tema "Definir reinos en el servidor LDAP" en la página 123 para obtener más información.

5. Si selecciona **Utilizar búsqueda DNS** como tipo de resolución de hosts, debe haber configurado el DNS para correlacionar con los nombres de reino. Después de indicar que utilizará un servidor DNS para manejar la resolución de nombres de host, debe asegurarse de que el reino se ha definido correctamente en el DNS. Consulte el tema "Definir reinos en la base de datos DNS" en la página 121 para obtener más información.
6. Si selecciona **Utilizar correlaciones estáticas** como tipo de resolución de hosts, escriba el nombre de reino y el nombre DNS que corresponda. Por ejemplo, el nombre de host podría ser mypc.mycompanylan.com y el nombre del reino es MYCO.COM. También puede correlacionar nombres de host genéricos con un reino específico. Por ejemplo, si todas las máquinas cuyo nombre acaba en myco.lan.com forman parte del reino MYCO.COM, podría escribir `myco.lan.com` como nombre DNS y MYCO.COM como reino. Así se crea una asociación entre el nombre del reino y el nombre DNS en el archivo de configuración. Pulse **Añadir** para crear una correlación estática entre el nombre del reino y el nombre DNS en el archivo de configuración.
7. Tras entrar la información pertinente para el tipo de resolución de hosts seleccionado, pulse **Aceptar**.

Añadir valores de cifrado

Puede seleccionar los tipos de cifrado para los tickets de otorgamiento de tickets (TGT) y el servicio de otorgamiento de tickets (TGS).

El cifrado oculta los datos que fluyen en una red haciéndolos indescifrables. Un cliente cifra los datos y el servidor los descifra. Para garantizar que el cifrado funciona correctamente, debe utilizar el mismo tipo de cifrado que el especificado en el servidor Kerberos o en la otra aplicación de la comunicación. Si estos tipos de cifrado no coinciden, el cifrado fallará. Puede añadir valores de cifrado para los TGT y el TGS.

Nota: Los valores de cifrado por omisión para el TGT y TGS son des-cbc-crc y des-cbc-md5. Durante la configuración se establecen los valores de cifrado predeterminados. Puede añadir otros valores de cifrado de tickets a la configuración llevando a cabo estos pasos:

1. En System i Navigator, expanda ***su sistema*** → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Propiedades**.
3. En la página Tickets, seleccione el valor de cifrado en la lista de tipos de cifrado disponibles para los tickets de otorgamiento de tickets (TGT) o para el servicio de otorgamiento de tickets (TGS).
4. Pulse **Añadir antes** o **Añadir después** para añadir el tipo de cifrado a la lista de tipos de cifrado seleccionados. Cada uno de estos tipos de cifrado seleccionados se intentarán en el orden de aparición en la lista. Si falla un tipo de cifrado, se intenta el siguiente de la lista.
5. Pulse **Aceptar**.

Obtener o renovar tickets de otorgamiento de tickets

| El mandato kinit obtiene o renueva un ticket de otorgamiento de tickets Kerberos. También puede utilizar
| el mandato CL Añadir ticket de Kerberos (ADDKRBTKT) para obtener y guardar en la memoria caché
| tickets de otorgamiento de tickets.

Mandato kinit

Si no se especifican opciones de tickets en el mandato kinit, se utilizan para el servidor Kerberos las opciones especificadas en el archivo de configuración de Kerberos.

Si no se renueva un ticket existente, la memoria caché de credenciales se reinicializa y contendrá el nuevo ticket-granting de otorgamiento de tickets recibido del servidor Kerberos. Si el nombre del sujeto

principal no se especifica en la línea de mandatos, el nombre se obtiene de la memoria caché de credenciales. La nueva memoria caché de credenciales pasa a ser la memoria caché de credenciales predeterminada, a menos que se especifique el nombre de la memoria caché con la opción `-c`.

Los valores de tiempo del ticket se expresan como *nwndnhnmns*, donde *n* representa un número, *w* indica semanas, *d* indica días, *h* indica horas, *m* indica minutos y *s* indica segundos. Los componentes deben especificarse en este orden, pero puede omitirse cualquier componente (por ejemplo, *4h5m* representa 4 horas y 5 minutos, y *1w2h* representa 1 semana y 2 horas). Si solo se especifica un número, el valor predeterminado es en horas.

Para obtener un ticket de otorgamiento de tickets que dure 5 horas para el sujeto principal jday, realice una de las siguientes acciones:

- En la línea de mandatos de Qshell, escriba `kinit -l 5h Jday`
- En una línea de mandatos de lenguaje de control (CL) de i5/OS, escriba `call qsys/qkrbkinit parm('-l' '5h' 'jday')`

En las notas de utilización de **kinit** encontrará los detalles sobre cómo utilizar este mandato de Qshell y sus restricciones.

Mandato Añadir ticket de Kerberos (ADDKRBTKT)

En una línea de mandatos de i5/OS, puede utilizar el mandato CL ADDKRBTKT para obtener tickets de otorgamiento de tickets. Por ejemplo, para añadir un ticket reenviable mediante krbsrv400/jday.myco.com del sujeto principal y el reino predeterminado, especifique el mandato siguiente:

```
ADDKRBTKT PRINCIPAL('krbsrv400/jday.myco.com') PASSWORD('mypwd') ALWFWD(*YES)
```

Referencia relacionada

Mandato Añadir ticket de Kerberos (ADDKRBTKT)

kinit

El mandato kinit de Qshell obtiene o renueva el ticket de otorgamiento de tickets Kerberos.

Sintaxis

```
kinit [-r tiempo] [-R] [-p] [-f] [-A] [-l tiempo] [-c memoria caché] [-k] [-t tabla de
claves] [principal]
```

Autorización de uso público predeterminada: *USE

Opciones

-r tiempo
Intervalo de tiempo para renovar un ticket. El ticket no se puede renovar después de que haya transcurrido este intervalo. El tiempo de renovación debe ser mayor que el tiempo de finalización. Si esta opción no está especificada, el ticket no es renovable (todavía es posible generar un ticket renovable si el tiempo de vida del ticket solicitado supera el tiempo de vida máximo del ticket).

-R Se renovará un ticket existente. Cuando se renueva un ticket existente, no se puede especificar ninguna otra opción de ticket.

-p El ticket puede ser un proxy. Si no especifica esta opción, el ticket no puede ser un proxy.

-f El ticket se puede reenviar. Si no se especifica esta opción, el ticket no se puede reenviar.

-A El ticket no contendrá una lista de direcciones de cliente. Si no se especifica esta opción, el ticket contendrá la lista de direcciones del host local. Cuando un ticket inicial contiene una lista de direcciones, solo se le puede utilizar desde una de las direcciones de la lista.

-l tiempo
Intervalo de tiempo de finalización del ticket. Una vez transcurrido este intervalo, el ticket no se puede utilizar, a menos que se haya renovado. Si esta opción no está especificada, el intervalo se establece en 10 horas.

-c memoria caché
Nombre de la memoria caché de credenciales que se utilizará en el mandato kinit. Si esta opción no está especificada, el mandato utiliza la memoria caché de credenciales predeterminada.

-k La clave del sujeto principal del ticket se obtendrá de una tabla de claves. Si esta opción no está especificada, el sistema le solicitará que entre la contraseña del sujeto principal del ticket.

-t tabla de claves
Nombre de la tabla de claves. Si no especifica esta opción, pero sí especifica la opción `-k`, el sistema utiliza la tabla de claves predeterminada. La opción `-t` implica la opción `-k`.

principal
Sujeto principal del ticket. Si no especifica el sujeto principal en la línea de mandatos, el sistema lo obtiene de la memoria caché de credenciales.

Autorizaciones

Objeto al que se hace referencia	Autorización necesaria
Cada directorio del nombre de vía de acceso que precede al archivo de tabla de claves si se especifica la opción `-t`	*X
Archivo de tabla de claves cuando se especifica `-t`	*R
Cada directorio del nombre de vía de acceso que precede al archivo de memoria caché de credenciales que se utilizará	*X
Directorio padre del archivo de memoria caché que se utilizará, si se ha especificado mediante la variable de entorno **KRB5CCNAME** y se está creando el archivo	*WX
Archivo de memoria caché de credenciales	*RW
Cada directorio de las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Para permitir que la unidad ejecutable Kerberos encuentre el archivo de memoria caché de credenciales desde cualquier proceso en ejecución, el nombre del archivo de memoria caché se almacena normalmente en el directorio inicial en un archivo denominado **krb5ccname**. La ubicación de almacenamiento del nombre de archivo de memoria caché se puede alterar temporalmente estableciendo la variable de entorno **_EUV_SEC_KRB5CCNAME_FILE**. Para acceder a este archivo, el perfil de usuario debe tener la autorización ***X** sobre cada directorio de la vía de acceso y la autorización ***R** sobre el archivo en el que se almacena el nombre del archivo de memoria caché. La primera vez que un usuario crea una memoria caché de credenciales, el perfil de usuario debe tener la autorización ***WX** sobre el directorio padre.

Mensajes

- Se necesita un valor para la opción `nombre_opción`.
- `opción_mandato` no es una opción de mandato válida.
- No se permiten opciones cuando se renueva o valida un ticket.
- No se puede obtener el nombre de la memoria caché de credenciales predeterminada.
- No se puede resolver la memoria caché de credenciales `nombre_archivo`.
- No existe ningún ticket inicial disponible.
- Hay que especificar el nombre del sujeto principal.
- No se puede recuperar el ticket a partir de la memoria caché de credenciales `nombre_archivo`.

- El ticket inicial no es renovable.
- La opción `valor_opción` no es válida para la petición `nombre_petición`.
- No se pueden obtener credenciales iniciales.
- No se puede analizar el nombre de sujeto principal.
- No se puede resolver la tabla de claves `nombre_archivo`.
- La contraseña del `nombre_sujeto_principal` no es correcta.
- No se puede leer la contraseña.
- No se pueden almacenar las credenciales iniciales en la memoria caché de credenciales `nombre_archivo`.
- El valor de incremento de tiempo no es válido.

En el tema Obtener o renovar tickets de otorgamiento de tickets hallará un ejemplo de cómo se utiliza este mandato.

Visualizar memoria caché de credenciales

El mandato klist visualiza el contenido de una memoria caché de credenciales de Kerberos. También puede utilizar el mandato CL Visualizar archivo de memoria caché de credenciales (DSPKRBCCF) para visualizar las entradas de la memoria caché local de credenciales.

Mandato klist

Para obtener una lista de todas las entradas de la memoria caché predeterminada de credenciales y visualizar los distintivos de los tickets, elija una de las siguientes opciones:

- En una línea de mandatos de Qshell, escriba `klist -f -a`
- En una línea de mandatos de lenguaje de control (CL) de i5/OS, escriba `call qsys/qkrbklist parm('-f' '-a')`

En las notas de utilización de **klist** encontrará los detalles sobre cómo utilizar este mandato de Qshell y sus restricciones.

Mandato Visualizar archivo de memoria caché de credenciales de Kerberos (DSPKRBCCF)

En una línea de mandatos CL de i5/OS, también puede utilizar el mandato Visualizar archivo de memoria caché de credenciales (DSPKRBCCF) para visualizar la memoria caché de credenciales. Por ejemplo, para visualizar el archivo predeterminado de memoria caché de credenciales, escriba el mandato siguiente:

```
DSPKRBCCF CCF(*DFT) OUTPUT(*)
```

Referencia relacionada

Mandato Visualizar archivo de memoria caché de credenciales de Kerberos (DSPKRBCCF)

klist

El mandato klist de Qshell visualiza el contenido de una tabla de claves o memoria caché de credenciales Kerberos.

Sintaxis

klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [nombre_archivo]

Autorización de uso público predeterminada: *USE

Opciones

-a Mostrar todos los tickets de la memoria caché de credenciales, incluidos los caducados. Si no especifica esta opción, los tickets caducados no figuran en la lista. Esta opción solo es válida cuando se obtiene un listado de la memoria caché de credenciales.

-e Visualizar el tipo de cifrado de la clave de sesión y del ticket. Esta opción solo es válida cuando se obtiene un listado de la memoria caché de credenciales.

-c Listar los tickets de una memoria caché de credenciales. Es el valor predeterminado si no se especifica la opción `-c` ni la opción `-k`. Esta opción se excluye mutuamente con la opción `-k`.

-f Mostrar los distintivos de los tickets, según las siguientes abreviaturas:

Abreviatura	Significado
F	El ticket se puede reenviar
f	Ticket reenviado
P	El ticket puede ser un proxy
p	Ticket de proxy
D	El ticket se puede posfechar
d	Ticket posfechado
R	Ticket renovable
I	Ticket inicial
i	Ticket no válido
A	Se utiliza preautenticación
O	El servidor puede ser un delegado
C	Lista de tránsitos comprobada por el servidor Kerberos

Esta opción solo es válida cuando se obtiene un listado de la memoria caché de credenciales.

-s Suprimir salida de mandato, pero establecer el estado de la salida en 0 si se encuentra un ticket de otorgamiento de tickets válido en la memoria caché de credenciales. Esta opción solo es válida cuando se obtiene un listado de la memoria caché de credenciales.

-k Listar las entradas de una tabla de claves. Esta opción se excluye mutuamente con la opción **-c**.

-t Visualizar indicaciones de la hora de las entradas de la tabla de claves. Esta opción solo es válida cuando se lista una tabla de claves.

-K Visualizar el valor de la clave de cifrado de cada entrada de la tabla de claves. Esta opción solo es válida cuando se lista una tabla de claves.

nombre_archivo
Especifica el nombre de la tabla de claves o de la memoria caché de credenciales. Si no se especifica ningún nombre de archivo, se utiliza la tabla de claves o la memoria caché de credenciales predeterminada.

Autorizaciones

Objeto al que se hace referencia	Autorización necesaria
Cada directorio del nombre de vía de acceso que precede al archivo si la opción `-k` se especifica como tabla de claves.	*X
Archivo de tabla de claves cuando se especifica `-k`	*R
Cada directorio del nombre de vía de acceso que precede al archivo de memoria caché de credenciales si no se especifica la opción `-k`	*X
Archivo de memoria caché de credenciales si no se especifica la opción `-k`	*R

Para permitir que la unidad ejecutable Kerberos encuentre el archivo de memoria caché de credenciales desde cualquier proceso en ejecución, el nombre del archivo de memoria caché se almacena normalmente en el directorio inicial en un archivo denominado **krb5ccname**. La ubicación de almacenamiento del nombre de archivo de memoria caché se puede alterar temporalmente estableciendo la variable de entorno **_EUV_SEC_KRB5CCNAME_FILE**. Para acceder a este archivo, el perfil de usuario debe tener la autorización ***X** sobre cada directorio de la vía de acceso y la autorización ***R** sobre el archivo en el que se almacena el nombre del archivo de memoria caché. La primera vez que un usuario crea una memoria caché de credenciales, el perfil de usuario debe tener la autorización ***WX** sobre el directorio padre.

Mensajes

- Se necesita un valor para la opción `nombre_opción`.
- `opción_mandato` no es una opción de mandato válida.
- La `opción_mandato_uno` y la `opción_mandato_dos` no se pueden especificar juntas.
- No se ha encontrado una memoria caché de credenciales predeterminada.
- No se puede resolver la memoria caché de credenciales `nombre_archivo`.
- No se puede recuperar el nombre de sujeto principal a partir de la memoria caché de credenciales `nombre_archivo`.
- No se puede recuperar el ticket a partir de la memoria caché de credenciales `nombre_archivo`.
- No se puede decodificar el ticket.
- No se ha encontrado la tabla de claves predeterminada.
- No se puede resolver la tabla de claves `nombre_archivo`.

En el tema Visualizar memoria caché de credenciales hallará un ejemplo de cómo se utiliza este mandato.

Gestionar archivos de tabla de claves

Puede mantener el archivo de tabla de claves utilizando la interfaz basada en caracteres o System i Navigator.

Como administrador de la red, deberá mantener un archivo de tabla de claves, al que también se conoce como tabla de claves, y su contenido en el sistema operativo i5/OS. Puede gestionar el archivo de tabla de claves y las entradas de tabla de claves asociadas utilizando la interfaz basada en caracteres o bien System i Navigator.

Gestionar archivos de tabla de claves con la interfaz basada en caracteres

- El mandato keytab puede utilizarse para añadir, suprimir o listar una clave de una tabla de claves. Por ejemplo, para añadir una clave del sujeto principal de servicio, krbsvr400, en el host kdc1.myco.com del reino MYCO.COM, emplee uno de los métodos siguientes:
  - En una línea de mandatos de Qshell, escriba `keytab add krbsvr400/kdc1.myco.com@MYCO.COM`
  - En una línea de mandatos de lenguaje de control (CL) de i5/OS, especifique `call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.myco.com@MYCO.COM')`

  Se le pedirá la contraseña que se empleó al definir el servicio en el servidor Kerberos.

  En las notas de utilización de **keytab** encontrará los detalles sobre cómo utilizar este mandato de Qshell y sus restricciones.
- En la línea de mandatos CL, también puede utilizar los mandatos Añadir entrada de tabla de claves Kerberos (ADDKRBKTE), Visualizar entradas de tabla de claves Kerberos (DSPKRBKTE) y Eliminar entrada de tabla de claves Kerberos (RMVKRBKTE) para gestionar archivos de tabla de claves.

Gestionar archivos de tabla de claves con System i Navigator

Puede utilizar System i Navigator para añadir entradas a la tabla de claves. System i Navigator le permite añadir entradas de tabla de claves para los siguientes servicios:

- Autenticación de Kerberos de i5/OS
- LDAP
- IBM HTTP Server
- i5/OS NetServer
- Servidor del sistema de archivos de red

Para añadir una entrada al archivo de tabla de claves, siga estos pasos:

1. En System i Navigator, expanda *su sistema* → **Seguridad**.
2. Pulse **Servicio de autenticación de red** con el botón derecho del ratón y seleccione **Gestionar tabla de claves**. Se lanzará una parte del asistente del servicio de autenticación de red que le permitirá añadir entradas de tabla de claves.
3. En la página Seleccionar entradas de tabla de claves, seleccione los tipos de servicios para los que desea entradas de tabla de claves, por ejemplo, Autenticación de Kerberos de i5/OS. Pulse **Siguiente**.
4. En la página Crear entrada de tabla de claves de i5/OS, escriba una contraseña y confírmela. Esta contraseña debe coincidir con la que utiliza al añadir el sujeto principal de servicio asociado al servidor Kerberos. Si ha seleccionado en el paso 3 uno de los otros tipos de servicios, como LDAP, HTTP Server, i5/OS NetServer o servidor de Sistema de Archivos de Red, también verá páginas que le permitirán crear entradas de tabla de claves para cada uno de esos servicios.
5. En la página Resumen, verá la lista de servicios de i5/OS y sujetos principales de servicio que se añadirán como entradas de tabla de claves al archivo de tabla de claves.

Referencia relacionada

Mandato Añadir entrada de tabla de claves de Kerberos (ADDKRBKTE)

Mandato Visualizar entradas de tabla de claves de Kerberos (DSPKRBKTE)

Mandato Suprimir entrada de tabla de claves de Kerberos (RMVKRBKTE)

keytab

El mandato keytab de Qshell gestiona una tabla de claves.

Sintaxis

```
keytab add principal [-p contraseña] [-v versión] [-k tabla de claves] keytab delete principal
[-v versión] [-k tabla de claves] keytab list [principal] [-k tabla de claves]
```

Autorización de uso público predeterminada: *USE

Opciones

-k Nombre de la tabla de claves. Si esta opción no está especificada, se utiliza la tabla de claves predeterminada.

-p Especificar la contraseña. Si esta opción no está especificada, se solicita a los usuarios que entren la contraseña cuando añaden una entrada a la tabla de claves.

-v Número de versión de la clave. Cuando se añade una clave, si esta opción no está especificada, se asigna el siguiente número de versión. Cuando se suprime una clave, si esta opción no está especificada, se suprimen todas las claves del sujeto principal.

principal
Nombre del sujeto principal. Cuando se obtiene un listado de la tabla de claves, si esta opción no está especificada, se muestran todos los sujetos principales.

Autorizaciones

Objeto al que se hace referencia	Autorización necesaria
Cada directorio del nombre de vía de acceso que precede al archivo de tabla de claves destino que se debe abrir.	*X
Directorio padre del archivo de tabla de claves destino cuando se especifica añadir, si todavía no existe el archivo de tabla de claves.	*WX
Archivo de tabla de claves cuando se especifica listar	*R
Archivo de tabla de claves destino cuando se especifica añadir o suprimir	*RW
Cada directorio de las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Mensajes

- Debe especificar *add*, *delete*, *list* o *merge*.
- *opción_mandato* no es una opción de mandato válida.
- La *opción_mandato_uno* y la *opción_mandato_dos* no se pueden especificar juntas.
- La opción *valor_opción* no es válida para la petición *nombre_petición*.
- Se necesita un valor para la opción *nombre_opción*.
- No se puede analizar el nombre de sujeto principal.
- Debe especificar el nombre del sujeto principal.
- No se puede leer la contraseña.
- No se ha encontrado la tabla de claves predeterminada.
- No se puede resolver la tabla de claves *tabla_claves*.
- No se puede leer la entrada de la tabla de claves *tabla_claves*.
- No se puede eliminar la entrada de la tabla de claves *tabla_claves*.
- No se puede añadir la entrada a la tabla de claves *tabla_claves*.
- No se han encontrado entradas del sujeto principal *nombre_sujeto_principal*.
- El valor no es un número válido.
- La versión de clave debe estar entre 1 y 255.
- No se ha encontrado la versión de clave *versión_clave* del sujeto principal *nombre_sujeto_principal*.

En el tema Gestionar archivos de tabla de claves hallará un ejemplo de cómo se utiliza este mandato.

Cambiar las contraseñas de Kerberos

| El mandato kpasswd, utilizando el servicio de cambio de contraseña, cambia la contraseña del sujeto
| principal Kerberos especificado. También puede utilizar el mandato CL Cambiar contraseña de Kerberos
| (CHGKRBPWD) para cambiar las contraseñas de Kerberos.

Mandato kpasswd

Debe facilitar la contraseña actual del sujeto principal, así como la contraseña nueva. Antes de cambiar la contraseña, el servidor de contraseñas aplicará las reglas pertinentes de la política de contraseñas a la nueva contraseña. El servidor de contraseñas se configura durante el proceso de instalación y configuración del servidor Kerberos. Consulte la documentación correspondiente al sistema.

Nota: i5/OS PASE no da soporte a un servidor de contraseñas. Para cambiar una contraseña de un sujeto principal almacenado en el servidor Kerberos, debe entrar en el entorno PASE (call QP2TERM) y emitir el mandato kpasswd.

Durante la configuración del servicio de autenticación de red, puede especificar el nombre del servidor de contraseñas. Si no se ha especificado uno durante la configuración, puede añadir un servidor de contraseñas.

No podrá cambiar la contraseña de un sujeto principal del servicio de otorgamiento de tickets (krbtgt/reino) utilizando el mandato kpasswd.

Para cambiar la contraseña predeterminada del sujeto principal:

- En una línea de mandatos de Qshell, escriba `kpasswd`
- En una línea de mandatos, escriba `call qsys/qkrbkpsswd`

Para cambiar la contraseña de otro sujeto principal:

- En una línea de mandatos de Qshell, escriba `kpasswd jday@myco.com`

Para cambiar la contraseña de otro sujeto principal de i5/OS PASE:

Utilizando una interfaz basada en caracteres

1. En una interfaz basada en caracteres, teclee `call QP2TERM`. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, escriba `export PATH=$PATH:/usr/krb5/sbin`. Este mandato señala hacia los scripts Kerberos que se necesitan para ejecutar los archivos ejecutables.
3. En el indicador QSH, escriba `kadmin -p admin/admin`. Pulse Intro.
4. Inicie sesión con el nombre de usuario y la contraseña de administrador.
5. Escriba `kpasswd jday@myco.com`. Se le pedirá que cambie la contraseña de este sujeto principal.

Utilizando una línea de mandatos

En una línea de mandatos, escriba `call qsys/qkrbkpsswd parm ('jday@myco.com')`

En las notas de utilización de **passwd** encontrará más detalles sobre cómo utilizar este mandato.

Mandato Cambiar contraseña de Kerberos (CHGKRBPWD)

En la línea de mandatos de i5/OS, también puede utilizar el mandato Cambiar contraseña de Kerberos (CHGKRBPWD) para cambiar las contraseñas de Kerberos. Por ejemplo, para jday del sujeto principal de Kerberos en el reino myco.com, puede utilizar el mandato siguiente para cambiar la contraseña myoldpwd por mynewpwd:

```
CHGKRBPWD PRINCIPAL('jday' myco.com) CURPWD('myoldpwd') NEWPWD('mynewpwd') VFYPWD('mynewpwd')
```

Referencia relacionada

Mandato Cambiar contraseña de Kerberos (CHGKRBPWD)

kpasswd

El mandato kpasswd de Qshell cambia la contraseña de un sujeto principal Kerberos.

Sintaxis

```
kpasswd [-A ] [principal]
```

Autorización de uso público predeterminada: *USE

Opciones

-A El ticket inicial utilizado por el mandato kpasswd no contendrá una lista de direcciones de cliente. Si

esta opción no está especificada, el ticket contendrá la lista de direcciones del host local. Cuando un ticket inicial contiene una lista de direcciones, solo se le puede utilizar desde una de las direcciones de la lista.

principal
Sujeto principal cuya contraseña se cambiará. El sujeto principal se obtendrá a partir de la memoria caché de credenciales predeterminada si no se especifica en la línea de mandatos.

Mensajes

- El sujeto principal %3$s no es válido.
- No se puede leer la memoria caché de credenciales predeterminada nombre_archivo.
- No hay una memoria caché de credenciales predeterminada.
- No se puede recuperar el ticket a partir de la memoria caché de credenciales nombre_archivo.
- No se puede leer la contraseña.
- Se ha cancelado el cambio de contraseña.
- La contraseña del nombre_sujeto_principal no es correcta.
- No se puede obtener el ticket inicial.
- La petición de cambio de contraseña ha fallado.

En el tema Cambiar contraseñas de Kerberos hallará un ejemplo de cómo se utiliza este mandato.

Suprimir archivos de memoria caché de credenciales caducados

| El mandato kdestroy suprime un archivo de memoria caché de credenciales Kerberos. También puede
| utilizar el mandato CL Suprimir memoria caché de credenciales de Kerberos (DLTKRBCCF) para suprimir
| la memoria caché de credenciales. Los usuarios deben suprimir periódicamente las credenciales antiguas.

Mandato kdestroy

La opción *-e* hace que el mandato kdestroy compruebe todos los archivos de memoria caché de credenciales en el directorio de memoria caché predeterminado /QIBM/UserData/OS400/NetworkAuthentication/creds. Se suprimirán los archivos que solo contengan tickets que hayan caducado durante el valor de *incremento_tiempo*. La opción *incremento_tiempo* viene expresado como *nwndnhnmns*, donde *n* representa un número, *w* indica semanas, *d* indica días, *h* indica horas, *m* indica minutos y *s* indica segundos. Los componentes deben especificarse en este orden, pero puede omitirse cualquier componente (por ejemplo, *4h5m* representa 4 horas y 5 minutos, y *1w2h* representa 1 semana y 2 horas). Si solo se especifica un número, el valor predeterminado es en horas.

1. Para suprimir la memoria caché de credenciales predeterminada:
   - En una línea de mandatos de Qshell, escriba `kdestroy`
   - En una línea de mandatos de lenguaje de control (CL) de i5/OS, especifique `call qsys/qkrbkdstry`
2. Para suprimir todos los archivos de memoria caché de credenciales que tengan tickets caducados más antiguos que 1 día:
   - En una línea de mandatos de Qshell, escriba `kdestroy -e 1d`
   - En una línea de mandatos CL, escriba `call qsys/qkrbkdstry parm ('-e' '1d')`

En las notas de utilización de **kdestroy** encontrará los detalles sobre cómo utilizar este mandato de Qshell y sus restricciones.

| Mandato Suprimir memoria caché de credenciales de Kerberos (DLTKRBCCF)

| En la línea de mandatos de i5/OS, puede utilizar el mandato DLTKRBCCF para suprimir la memoria
| caché de credenciales.

| Para suprimir la memoria caché de credenciales predeterminada, especifique `DLTKRBCCF CCF(*DFT)`.

| Para suprimir todos los archivos de memoria caché de credenciales que tengan tickets caducados más
| antiguos que 1 día, especifique `DLTKRBCCF CCF(*EXPIRED) EXPTIME(1440)`.

Referencia relacionada

Mandato Suprimir archivo de memoria caché de credenciales de Kerberos (DLTKRBCCF)

kdestroy

El mandato kdestroy de Qshell destruye una memoria caché de credenciales Kerberos.

Sintaxis

```
kdestroy [-c nombre_caché] [-e incremento_tiempo]
```

Autorización de uso público por omisión: *USE

Opciones

-c nombre_caché
Nombre de la memoria caché de credenciales que se destruirá. Si no se especifican opciones de mandato, se destruye la memoria caché de credenciales predeterminada. Esta opción se excluye mutuamente con la opción `-e`.

-e incremento_tiempo
Todos los archivos de la memoria caché de credenciales que contienen tickets caducados se suprimen si los tickets llevan caducados como mínimo el mismo tiempo que el valor de `incremento_tiempo`.

Autorizaciones

Cuando la memoria caché de credenciales es de tipo **FILE** (en **krb5_cc_resolve()** hallará más información sobre los tipos de memoria caché), el comportamiento por omisión es que el archivo de la memoria caché de credenciales se crea en el directorio /QIBM/UserData/OS400/NetworkAuthentication/creds. La posición del archivo de memoria caché de credenciales se puede cambiar estableciendo la variable de entorno KRB5CCNAME.

Cuando el archivo de memoria caché de credenciales no reside en el directorio predeterminado, se necesitan las siguientes autorizaciones:

Objeto al que se hace referencia	Autorización sobre datos que se necesita	Autorización sobre objeto que se necesita
Cada directorio del nombre de vía de acceso que precede al archivo de memoria caché de credenciales	*X	Ninguna
Directorio padre del archivo de memoria caché de credenciales	*WX	Ninguna
Archivo de memoria caché de credenciales	*RW	*OBJEXIST
Cada directorio de las vías de acceso a los archivos de configuración	*X	Ninguna
Archivos de configuración	*R	Ninguna

Cuando el archivo de memoria caché de credenciales reside en el directorio predeterminado, se necesitan las siguientes autorizaciones:

Objeto al que se hace referencia	Autorización sobre datos que se necesita	Autorización sobre objeto que se necesita
Todos los directorios del nombre de la vía de acceso	*X	Ninguna
Archivo de memoria caché de credenciales	*RW	Ninguna
Cada directorio de las vías de acceso a los archivos de configuración	*X	Ninguna
Archivos de configuración	*R	Ninguna

Para permitir que el protocolo Kerberos encuentre el archivo de memoria caché de credenciales desde cualquier proceso en ejecución, el nombre del archivo de memoria caché normalmente se almacena en el directorio inicial en un archivo denominado krb5ccname. Un usuario que desee utilizar la autenticación Kerberos en la plataforma System i debe tener definido un directorio inicial. Por omisión, el directorio inicial es /home/. Este archivo se utiliza para encontrar la memoria caché de credenciales predeterminada si no se han especificado opciones de mandato. La ubicación de almacenamiento del nombre de archivo de memoria caché se puede alterar temporalmente estableciendo la variable de entorno *_EUV_SEC_KRB5CCNAME_FILE*. Para acceder a este archivo, el perfil de usuario debe tener la autorización ***X** sobre cada directorio de la vía de acceso y la autorización ***R** sobre el archivo en el que se almacena el nombre del archivo de memoria caché.

Mensajes

- No se puede resolver la memoria caché de credenciales *nombre_archivo_caché*.
- No se puede destruir la memoria caché de credenciales *nombre_archivo_caché*.
- La función *nombre_función* ha detectado un error.
- No se puede recuperar el ticket a partir de la antememoria de credenciales *nombre_archivo*.
- Se necesita un valor para la opción *nombre_opción*.
- *opción_mandato* no es una opción de mandato válida.
- La *opción_mandato_uno* y la *opción_mandato_dos* no se pueden especificar juntas.
- No se ha encontrado una memoria caché de credenciales predeterminada.
- El valor de incremento de tiempo *valor* no es válido.

En el tema Suprimir archivos de memoria caché de credenciales caducadas hallará un ejemplo de cómo se utiliza este mandato.

Gestionar entradas de servicio Kerberos en directorios LDAP

El mandato ksetup gestiona las entradas de servicio de Kerberos en el directorio de servidor LDAP.

Objetivo

El mandato ksetup gestiona las entradas de servicio de Kerberos en el directorio de servidor LDAP. Se admiten los siguientes submandatos:

addhost nombre-sistpral nombre-reino
: Este submandato añade una entrada de host del reino especificado. Debe utilizarse el nombre de host totalmente calificado para que se resuelva correctamente sea cual sea el dominio DNS predeterminado que esté en vigor en los clientes Kerberos. Si no se especifica un nombre de reino, se utiliza el nombre de reino predeterminado.

addkdc nombre-sistpral:número-puerto nombre-reino
: Este submandato añade una entrada en el servidor Kerberos para el reino especificado. Si una entrada de host todavía no existe, se crea una. Si no se especifica un número de puerto, el número se establece en 88. Utilice el nombre de host totalmente calificado para que se resuelva

correctamente sea cual sea el dominio DNS predeterminado que esté en vigor en los clientes Kerberos. Si no se especifica un nombre de reino, se utiliza el nombre de reino predeterminado.

delhost nombre-sistpral nombre-reino
Este submandato suprime del reino especificado una entrada de host y las especificaciones asociadas del servidor Kerberos. Si no se especifica un nombre de reino, se utiliza el nombre de reino predeterminado.

delkdc nombre-sistpral nombre-reino
Este submandato suprime una entrada existente en el servidor Kerberos para el host especificado. La propia entrada de host no se suprime. Si no se especifica un nombre de reino, se utiliza el nombre de reino predeterminado.

listhost nombre-reino
Este submandato proporciona una lista de las entradas existentes en el servidor Kerberos para un reino. Si no se especifica un nombre de reino, se utiliza el nombre de reino predeterminado.

exit Este submandato finaliza el mandato ksetup.

Restricción: Los productos System i admiten clientes LDAP en la interfaz basada en caracteres, pero no en i5/OS PASE.

Ejemplos

Para añadir el host kdc1.myco.com al servidor ldapserv.myco.com como servidor Kerberos del reino MYCO.COM, utilizando para ello un ID de administrador del servidor de directorios (LDAP) igual a Administrator y una contraseña igual a verysecret, seguiría estos pasos:

En una línea de mandatos de Qshell, escriba: `ksetup -h ldapserv.myco.com -n CN=Administrator -p verysecret`

O bien

1. En una línea de mandatos de lenguaje de control (CL) de i5/OS, especifique:
   ```
   call qsys/qkrbksetup parm('-h' 'ldapserv.myco.com' '-n' 'CN=Administrator' '-p' 'verysecret')
   ```
2. Cuando se establece contacto satisfactoriamente con el servidor de directorios LDAP, se visualiza un indicador de submandatos. Escriba:
   ```
   addkdc kdc1.myco.com MYCO.COM
   ```

En las notas de utilización de **ksetup** encontrará los detalles sobre cómo utilizar este mandato de Qshell y sus restricciones.

ksetup

El mandato ksetup de Qshell gestiona las entradas de servicio de Kerberos del servidor de directorio correspondientes a un reino de Kerberos.

Sintaxis

```
ksetup -h nombre_sistema_principal -n nombre_enlace -p contraseña_enlace -e
```

Autorización de uso público predeterminada: *USE

Opciones

-h Nombre de host del servidor de directorio. Si no especifica esta opción, se utiliza el servidor de directorio especificado en el archivo de configuración de Kerberos.

-n Nombre distinguido que se utilizará al enlazarse al servidor de directorio. Si no especifica esta opción, se utiliza la variable de entorno LDAP_BINDDN para obtener el nombre.

-p Contraseña que se utilizará al enlazarse al servidor de directorio. Si no se especifica esta opción, se utiliza la variable de entorno LDAP_BINDPW para obtener la contraseña.

-e Hacer eco de cada línea de mandatos en la salida estándar (stdout). Resulta útil cuando la entrada estándar (stdin) se redirige a un archivo.

Autorizaciones

Objeto al que se hace referencia	Autorización necesaria
Cada directorio de las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Mensajes

- `submandato` no es un submandato válido.
- Los submandatos válidos son `addhost`, `addkdc`, `delhost`, `delkdc`, `listhost`, `listkdc`, `exit`.
- La `opción_mandato_uno` y la `opción_mandato_dos` no se pueden especificar juntas.
- No se puede inicializar el cliente LDAP.
- No se puede enlazar al servidor de directorio.
- Hay que especificar el nombre del reino.
- Hay que especificar el nombre del host.
- Demasiados parámetros de posición.
- El host `host` ya existe.
- El dominio root `dominio` no está definido.
- El nombre de reino `reino` no es válido.
- La función `nombre de función LDAP` ha detectado un error.
- Almacenamiento disponible insuficiente.
- El nombre de host `host` no es válido.
- El número de puerto `puerto` no es válido.
- El host `host` no está definido.
- No hay ningún servidor Kerberos definido para el host `host`.
- No se puede obtener el nombre de reino predeterminado.

En el tema Gestionar entradas de servicio Kerberos en directorios LDAP hallará un ejemplo de cómo se utiliza este mandato.

Definir reinos en la base de datos DNS

Puede definir reinos en la base de datos DNS para resolver los nombres de sistema principal.

El servicio de autenticación de red le permite utilizar el servidor DNS para resolver los nombres de sistema principal. Para ello, tendrá que añadir un registro de servidor (SRV) y un registro de texto (TXT) para cada centro de distribución de claves (KDC) del reino. El protocolo Kerberos busca un registro SRV utilizando el nombre del reino como nombre de búsqueda en el DNS.

Para definir reinos con el DNS, lleve a cabo estos pasos:

1. Establecer el archivo de configuración para que utilice DNS.
2. Añada al servidor DNS registros SRV por cada servidor KDC existente en el reino. La unidad ejecutable Kerberos busca un registro SRV utilizando el nombre del reino como nombre de búsqueda. Tenga en cuenta que en las búsquedas del DNS no se distingue entre mayúsculas y minúsculas, y por ello no puede haber dos reinos distintos cuyos nombres tan solo difieran en las mayúsculas/minúsculas. El formato general del registro SRV de Kerberos es el siguiente:

```
servicio.protocolo.reino clase TTL SRV prioridad peso puerto destino
```

Las entradas de servicio _kerberos definen instancias de KDC, y las entradas de servicio _kpasswd definen instancias del servicio de cambio de contraseña.

Las entradas se intentan por orden de prioridad (0 corresponde a la máxima prioridad). Las entradas que tengan la misma prioridad se intentan por orden aleatorio. Los registros de protocolo _udp son necesarios para las entradas _kerberos y _kpasswd.

3. Añada registros TXT para asociar los nombres de sistema principal a los nombres de reino. El protocolo Kerberos busca un registro TXT que empiece por el nombre de sistema principal. Si no encuentra ningún registro TXT, se elimina la primera etiqueta y se reintenta la búsqueda con el nuevo nombre. Este proceso continúa hasta que se encuentre un registro TXT o hasta que se llegue a la raíz. Tenga en cuenta que en el nombre del reino del registro TXT se distingue entre mayúsculas y minúsculas. El formato general de un registro TXT es el siguiente:

   ```
   servicio.nombre clase TTL TXT reino
   ```

   En el caso de nuestro ejemplo de configuración, puede definir centros de distribución de claves (KDC) de ejemplo para dos reinos añadiendo los siguientes registros:

   ```
   _kerberos._udp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
   _kerberos._tcp.deptxyz.bogusname.com IN SRV 0 0 88 kdc1.deptxyz.bogusname.com
   _kerberos._udp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
   _kerberos._tcp.deptabc.bogusname.com IN SRV 0 0 88 kdc2.deptabc.bogusname.com
   _kpasswd._udp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
   _kpasswd._tcp.deptxyz.bogusname.com IN SRV 0 0 464 kdc1.deptxyz.bogusname.com
   _kpasswd._udp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
   _kpasswd._tcp.deptabc.bogusname.com IN SRV 0 0 464 kdc2.deptxyz.bogusname.com
   ```

   En el caso de nuestro ejemplo de configuración, siguiendo el formato general de un registro TXT Kerberos, podemos asociar los hosts de los dominios deptxyz y deptabc a los respectivos reinos con las siguientes sentencias:

   ```
   _kerberos.deptxyz.bogusname.com  IN  TXT  DEPTXYZ.BOGUSNAME.COM
   _kerberos.deptabc.bogusname.com  IN  TXT  DEPTABC.BOGUSNAME.COM
   ```

   A continuación figura un archivo de configuración **krb5.conf** de ejemplo que especifica la búsqueda utilizando DNS:

   Archivo de configuración krb5.conf de ejemplo

   ```
   ; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
   ;
   [libdefaults]
   ;  El valor de default_realm
   ;-default_realm = REALM1.ROCHESTER.IBM.COM
   default_realm = DEPTXYZ.BOGUSNAME.COM
   ; definir el sistema para que utilice la búsqueda DNS
   use_dns_lookup = 1
   [realms]
   ;
   ; Aquí podríamos definir la misma información de reino, pero
   ; solo se utilizaría si fallase la búsqueda DNS.
   ;
   [domain_realm]
   ;  Convertir nombres de sistema principal en nombres de reino.  Pueden especificarse
   ;  host individuales.  Pueden especificarse sufijos de dominio con un punto inicial
   ;  y se aplicarán a todos los nombres de sistema principal que acaben en ese sufijo.
   ;
   ;  Usaremos DNS para resolver a qué reino pertenece un nombre de sistema principal dado.
   ;
   [capaths]
   ;  Las vías de autenticación configurables definen las relaciones de confianza
   ;  entre cliente y servidores.  Cada entrada representa un reino de cliente
   ```

```
;  y consta de las relaciones de confianza para cada servidor al que se pueda
;  acceder desde ese reino.  Puede haber servidores que figuren numerosas veces en la
;  lista si son varias las relaciones de confianza implicadas.  Especifique '.' para
;  una conexión directa.
;-REALM1.ROCHESTER.IBM.COM = {
;-    REALM2.ROCHESTER.IBM.COM = .
;;}
DEPTXYZ.BOGUSNAME.COM = {
 DEPTABC.BOGUSNAME.COM = .
}
```

Definir reinos en el servidor LDAP

El servicio de autenticación de red le permite utilizar el servidor LDAP para resolver un nombre de sistema principal en un reino Kerberos y localizar el KDC de un reino Kerberos.

Si se propone utilizar LDAP para buscar esta información, primero debe definirla en el servidor LDAP. Para ello, lleve a cabo estos dos conjuntos de tareas:

1. Establecer el archivo de configuración para que utilice LDAP.

   Utilice System i Navigator para indicar qué servidor de directorios desea utilizar para resolver los nombres de sistema principal. Con ello actualizará el archivo de configuración **krb5.conf** que se encuentra en /QIBM/UserData/OS400/NetworkAuthentication/krb5.conf. El nombre del servidor de directorios se añade a la sección `libdefaults` del archivo de configuración. A continuación figura un ejemplo de este archivo de configuración:

   Archivo de configuración krb5.conf de ejemplo

```
; krb5.conf - Kerberos V5 configuration file DO NOT REMOVE THIS LINE
;
[libdefaults]
;  El valor de default_realm
;-default_realm = REALM1.ROCHESTER.IBM.COM
default_realm = DEPTXYZ.BOGUSNAME.COM
; definir el sistema para que utilice la búsqueda LDAP
use_ldap_lookup = 1
ldap_server = dirserv.bogusname.com
[realms]
;
; Aquí podríamos definir la misma información de reino, pero
; solo se utilizaría si fallase la búsqueda LDAP.
;
[domain_realm]
;  Convertir nombres de sistema principal en nombres de reino.  Pueden especificarse
;  host individuales.  Pueden especificarse sufijos de dominio con un punto inicial
;  y se aplicarán a todos los nombres de sistema principal que acaben en ese sufijo.
;
;  Usaremos LDAP para resolver a qué reino pertenece un nombre de sistema principal dado.
;  También los podríamos definir aquí, pero solo se utilizarían en el caso de que
;  fallase la búsqueda LDAP.
;
[capaths]
;  Las vías de autenticación configurables definen las relaciones de confianza
;  entre cliente y servidores.  Cada entrada representa un reino de cliente
;  y consta de las relaciones de confianza para cada servidor al que se pueda
;  acceder desde ese reino.  Puede haber servidores que figuren numerosas veces en la
;  lista si son varias las relaciones de confianza implicadas.  Especifique '.' para
;  una conexión directa.
;-REALM1.ROCHESTER.IBM.COM = {
;-    REALM2.ROCHESTER.IBM.COM = .
;;}
DEPTXYZ.BOGUSNAME.COM = {
 DEPTABC.BOGUSNAME.COM = .
}
```

2. Definir Kerberos para el servidor LDAP. El servidor LDAP debe tener un objeto dominio cuyo nombre se corresponda con el nombre del reino Kerberos. Por ejemplo, si el nombre del reino Kerberos es DEPTABC.BOGUSNAME.COM, debe haber un objeto en el directorio que se llame dc=DEPTABC,dc=BOGUSNAME,dc=com. Si este objeto no existe, será necesario que primero añada un sufijo a la configuración del servidor LDAP. Para este nombre de objeto, serían sufijos válidos dc=DEPTABC,dc=BOGUSNAME,dc=COM o una de las entradas padre (dc=BOGUSNAME,dc=COM o dc=COM). Para un servidor LDAP i5/OS, puede añadir un sufijo utilizando System i Navigator.
   a. Si desea añadir un sufijo, siga estos pasos:
      1) En System i Navigator, expanda *su sistema* → **Red** → **Servidores** → **TCP/IP**.
      2) Pulse **IBM Directory Server** con el botón derecho del ratón y seleccione **Propiedades**.
      3) En la página Base de datos/Sufijo, especifique el sufijo que desea añadir.
   b. Utilice el mandato LDAPADD para añadir el objeto dominio correspondiente al reino en el directorio LDAP.
   c. Siguiendo con nuestro ejemplo de integrado de dos reinos, que se llaman DEPTABC.BOGUSNAME.COM y DEPTXYZ.BOGUSNAME.COM, coloque las siguientes líneas en el archivo del sistema de archivos integrado:

```
dn: dc=BOGUSNAME,dc=COM
dc: BOGUSNAME
objectClass: domain

dn: dc=DEPTABC,dc=BOGUSNAME,dc=COM
dc: DEPTABC
objectClass: domain

dn: dc=DEPTXYZ,dc=BOGUSNAME,dc=COM
dc: DEPTXYZ
objectClass: domain
```

   d. Si el archivo del sistema de archivos integrado se llama **/tmp/addRealms.ldif**, tomando los mismos supuestos que en el ejemplo anterior, escriba estos mandatos:

```
STRQSH
ldapadd -h dirserv.bogusname.com -D cn=Administrator
  -w verysecret -c -f
/tmp/addRealms.ldif
```

   e. Defina las entradas KDC de sus reinos y, si lo desea, defina las entradas de nombre de sistema principal para asignar un nombre de reino concreto a cada sistema principal de la red. Para ello, puede utilizar el mandato ksetup, con los submandatos addkdc y addhost. Siguiendo con nuestro ejemplo de configuración, puede escribir estos mandatos:

```
STRQSH
ksetup -h dirserv.bogusname.com -n cn=Administrator
  -p verysecret
addkdc kdc1.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc2.deptxyz.bogusname.com DEPTXYZ.BOGUSNAME.COM
addkdc kdc1.deptabc.bogusname.com DEPTABC.BOGUSNAME.COM
addhost database.deptxyz.bogusname.com
  DEPTXYZ.BOGUSNAME.COM
```

      Repita este procedimiento para cada sistema principal de cada reino, según necesite.

Definir un esquema en un servidor LDAP

El servidor LDAP de i5/OS (IBM Directory Server) se suministra con el esquema LDAP ya definido. Sin embargo, si utiliza un servidor LDAP distinto del IBM Directory Server, puede definir su propio esquema en ese servidor.

Esquema LDAP

Si decide definir su propio esquema en un servidor LDAP, le será de utilidad la siguiente información.

Para el servicio de autenticación de red se necesitan las siguientes definiciones de esquema LDAP, teniendo en cuenta que:

- Los valores enteros se representan como una serie de, como máximo, 11 caracteres numéricos con signo.
- Los valores booleanos se representan mediante las series de caracteres “TRUE” y “FALSE”.
- Los valores de hora se representan como series de caracteres de 15 bytes codificadas con el formato “AAAAMMDDhhmmssZ”. Todas las horas vienen representadas como valores UTC.

Clases de objetos de LDAP

Objeto	Necesita	Permite
domain	dc	description seeAlso
ibmCom1986-Krb-KerberosService	serviceName ibmCom1986-Krb-KerberosRealm	ipServicePort description seeAlso
domain	dc objectClass	description seeAlso

Atributos de LDAP

Atributo	Tipo	Tamaño	Valor
dc	caseIgnoreString	64	sencillo
description	caseIgnoreString	1024	múltiple
ibmCom1986-Krb-KerberosRealm	caseExactString	256	sencillo
ipServicePort	integer	11	sencillo
seeAlso	DN	1000	múltiple
serviceName	caseIgnoreString	256	sencillo

Resolución de problemas del servicio de autenticación de red

Se incluye información sobre la resolución de los problemas más habituales relacionados con el servicio de autenticación de red, la correlación de identidades de empresa (EIM) y las aplicaciones suministradas por IBM que admiten la autenticación Kerberos.

1. Cumplimentar todos los prerrequisitos.
2. Asegúrese de que el usuario tiene un perfil de usuario en la plataforma System i y un sujeto principal en el servidor Kerberos. En la plataforma System i, verifique que el usuario existe abriendo Usuarios y Grupos en System i Navigator o escribiendo `WRKUSRPRF` (Trabajar con perfiles de usuario) en una línea de mandatos. En los sistemas que ejecutan Windows, verifique que el usuario existe accediendo a la carpeta Usuarios y equipos de Active Directory.
3. Compruebe si la plataforma System i establece contacto con el servidor Kerberos emitiendo el mandato kinit desde el intérprete Qshell. Si el mandato kinit falla, compruebe si el sujeto principal de servicio de i5/OS está registrado en el servidor Kerberos. Si no lo está, puede añadir el sujeto principal de i5/OS al servidor Kerberos.

   Tareas relacionadas

   “Añadir sujetos principales i5/OS al servidor Kerberos” en la página 101
   Después de configurar el servicio de autenticación de red en la plataforma System i, debe añadir los sujetos principales de i5/OS al servidor Kerberos.

Errores y recuperación del servicio de autenticación de red

Podría encontrar estos errores al utilizar el asistente del servicio de autenticación de red o cuando gestiona propiedades del servicio de autenticación de red en System i Navigator. Para resolver los problemas, utilice los métodos de recuperación correspondientes que se listan aquí.

Tabla 36. Errores y recuperación del servicio de autenticación de red

Error	Recuperación
KRBWIZ_CONFIG_FILE_FORMAT_ERROR: El formato del archivo de configuración del servicio de autenticación de red es erróneo.	Reconfigure el servicio de autenticación de red. Encontrará los detalles en el tema "Configurar el servicio de autenticación de red" en la página 99.
KRBWIZ_ERROR_READ_CONFIG_FILE: Error al leer el archivo de configuración del servicio de autenticación de red.	Reconfigure el servicio de autenticación de red. Encontrará los detalles en el tema "Configurar el servicio de autenticación de red" en la página 99.
KRBWIZ_ERROR_WRITE_CONFIG_FILE: Error al escribir en el archivo de configuración del servicio de autenticación de red.	El servicio utilizado para escribir en el archivo de configuración no está disponible. Vuelva a intentarlo más adelante.
KRBWIZ_PASSWORD_MISMATCH: La contraseña nueva no coincide con la que ha escrito en el campo Confirmar contraseña nueva.	Vuelva a escribir la contraseña nueva y la del campo Confirmar contraseña nueva.
KRBWIZ_PORT_ERROR: El número de puerto debe estar comprendido entre 1 y 65535.	Vuelva a entrar un número de puerto que esté comprendido entre 1 y 65535.
KRBWIZ_ERROR_WRITE_KEYTAB: Error al escribir el archivo de tabla de claves.	El servicio utilizado para escribir la tabla de claves no está disponible en estos momentos. Vuelva a intentarlo más adelante.
KRBWIZ_NOT_AUTHORIZED_CONFIGURE: No tiene autorización para configurar el servicio de autenticación de red.	Asegúrese de que tiene las siguientes autorizaciones: *ALLOBJ y *SECADM.
KrbPropItemExists: El elemento ya existe.	Entre un elemento nuevo.
KrbPropKDCInListRequired: Debe tener un KDC en la lista.	El servidor Kerberos especificado no existe en la lista. Seleccione un servidor Kerberos de la lista.
KrbPropKDCValueRequired: Hay que entrar un nombre de KDC.	Entre un nombre válido para el servidor Kerberos. El servidor Kerberos debe estar configurado en un sistema seguro de la red.
KrbPropPwdServerRequired: Hay que entrar un nombre para el servidor de contraseñas.	Entre un nombre válido para el servidor de contraseñas.
KrbPropRealmRequired: Hay que entrar un nombre de reino.	Entre el nombre del reino al que pertenece este sistema.
KrbPropRealmToTrustRequired: Hay que entrar un nombre para el reino de confianza.	Entre el nombre del reino con el que se propone establecer una relación de confianza.
KrbPropRealmValueRequired: Hay que entrar un nombre de reino.	Entre un nombre válido para el reino.
CPD3E3F: Se ha producido el error de servicio de autenticación de red &2.	Consulte la información de recuperación específica que se corresponde con este mensaje.

Problemas de conexión de aplicaciones y su recuperación

Estos son algunos de los errores habituales y sus métodos de recuperación en interfaces i5/OS habilitadas para Kerberos.

Tabla 37. Errores comunes de las interfaces de i5/OS habilitadas para Kerberos

Problema	Recuperación
Recibe este mensaje de error: No se puede obtener el nombre de la memoria caché de credenciales predeterminada.	Averigüe si el usuario que ha iniciado sesión en el System i tiene un directorio en el directorio /home. Si no existe el directorio del usuario, cree un directorio inicial para la memoria caché de credenciales.
CPD3E3F: Se ha producido el error de servicio de autenticación de red &2.	Consulte la información de recuperación específica que se corresponde con este mensaje.
La conexión DRDA/DDM falla en una plataforma System i que se ha conectado con anterioridad.	Compruebe si existe el reino predeterminado especificado durante la configuración del servicio de autenticación de red. Si no se ha configurado un reino predeterminado ni un servidor Kerberos, la configuración del servicio de autenticación de red es incorrecta y las conexiones DRDA/DDM fallarán. Como recuperación de este error, puede llevar a cabo una de estas tareas: 1. Si no está utilizando la autenticación Kerberos, siga estos pasos: Suprima el reino predeterminado especificado en la configuración del servicio de autenticación de red. 2. Si está utilizando la autenticación Kerberos, siga estos pasos: a. Reconfigure el servicio de autenticación de red especificando el reino predeterminado y el servidor Kerberos que creó en el paso 1. b. Configure las aplicaciones de System i Access para Windows para que utilicen la autenticación de Kerberos. De este modo se establecerá la autenticación Kerberos en todas las aplicaciones de System i Access para Windows, incluida la aplicación DRDA/DDM (consulte el apartado "Caso práctico: habilitar el inicio de sesión único para i5/OS" en la página 53).

Tabla 37. Errores comunes de las interfaces de i5/OS habilitadas para Kerberos (continuación)

Problema	Recuperación
La conexión QFileSvr.400 falla en una plataforma System i que se ha conectado con anterioridad.	Compruebe si existe el reino predeterminado especificado durante la configuración del servicio de autenticación de red. Si no se ha configurado un reino predeterminado ni un servidor Kerberos, la configuración del servicio de autenticación de red es incorrecta y las conexiones QFileSvr.400 fallarán. Como recuperación de este error, puede llevar a cabo una de estas tareas: 1. Si no está utilizando la autenticación Kerberos, siga estos pasos: Suprima el reino predeterminado especificado en la configuración del servicio de autenticación de red. 2. Si está utilizando la autenticación Kerberos, siga estos pasos: a. Configure un reino predeterminado y un servidor Kerberos en un sistema seguro de la red. Consulte la documentación correspondiente a ese sistema. b. Reconfigure el servicio de autenticación de red especificando el reino predeterminado y el servidor Kerberos que creó en el paso 1. c. Configure las aplicaciones de System i Access para Windows para que utilicen la autenticación de Kerberos. De este modo se establecerá la autenticación Kerberos en todas las aplicaciones de System i Access para Windows, incluida la aplicación DRDA/DDM (consulte el apartado "Caso práctico: habilitar el inicio de sesión único para i5/OS" en la página 53).
CWBSY1011: No se han encontrado credenciales de cliente Kerberos.	El usuario no posee un ticket de otorgamiento de tickets (TGT). Este error de conexión se produce en un PC cliente cuando un usuario no inicia sesión en un dominio de Windows 2000. Como recuperación de este error, inicie sesión en el dominio de Windows 2000.
Se produjo un error mientras se verificaban los valores de la conexión. El URL no indica el host. **Nota:** Este error se produce cuando se utiliza la correlación de identidades de empresa (EIM).	Como recuperación de este error, siga estos pasos: 1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP**. 2. Pulse **Directorio** con el botón derecho del ratón y seleccione **Propiedades**. 3. En la página General, compruebe que el nombre distinguido y la contraseña del administrador coinciden con los que ha escrito durante la configuración de EIM.
Se produjo un error mientras se cambiaba la configuración del servidor de directorio local. GLD0232: La configuración no puede contener sufijos que se solapen. **Nota:** Este error se produce cuando se utiliza la correlación de identidades de empresa (EIM).	Como recuperación de este error, siga estos pasos: 1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP**. 2. Pulse **Directorio** con el botón derecho del ratón y seleccione **Propiedades**. 3. En la página Base de datos/Sufijos, elimine las entradas **ibm-eimDomainName** y reconfigure EIM.

Tabla 37. Errores comunes de las interfaces de i5/OS habilitadas para Kerberos (continuación)

Problema	Recuperación
Se produjo un error mientras se verificaban los valores de la conexión. Se produjo una excepción al llamar a un programa de i5/OS. El programa llamado es eimConnect. Los detalles son: com.ibm.as400.data.PcmlException. **Nota:** Este error se produce cuando se utiliza la correlación de identidades de empresa (EIM).	Como recuperación de este error, siga estos pasos: 1. En System i Navigator, expanda ***su sistema*** → **Red** → **Servidores** → **TCP/IP**. 2. Pulse **Directorio** con el botón derecho del ratón y seleccione **Propiedades**. 3. En la página Base de datos/Sufijos, elimine las entradas **ibm-eimDomainName** y reconfigure EIM.
Un ticket de Kerberos procedente del sistema remoto no se puede autenticar. **Nota:** Este error se produce cuando se configuran sistemas de Management Central para que utilicen la autenticación Kerberos.	Verifique que Kerberos está debidamente configurado en todos los sistemas. Este error podría indicar una violación de la seguridad. Vuelva a intentar la petición. Si el problema persiste, póngase en contacto con el Centro de soporte al cliente de IBM.
No se puede recuperar el ticket de servicio de Kerberos. **Nota:** Este error se produce cuando se configuran sistemas de Management Central para que utilicen la autenticación Kerberos.	Verifique que el sujeto principal Kerberos krbsvr400/*System i totalmente calificado de iSeries@REINO* está en el servidor Kerberos así como en el archivo de tabla de claves de cada uno de sus sistemas. Para verificar si el sujeto principal Kerberos se ha entrado en el servidor Kerberos, vea el tema "Añadir sujetos principales i5/OS al servidor Kerberos" en la página 101. Para verificar si los nombres de sujeto principal de servicio Kerberos se han entrado en el archivo de tabla de claves, consulte el apartado "Gestionar archivos de tabla de claves" en la página 113 para obtener información detallada.
El sujeto principal Kerberos no está en un grupo de confianza. **Nota:** Este error se produce cuando se configuran sistemas de Management Central para que utilicen la autenticación Kerberos.	Añada al archivo de grupos de confianza el sujeto principal Kerberos del sistema que está intentando conectarse a este sistema. Como recuperación de este error, siga estos pasos: 1. Establecer el sistema central para que utilice la autenticación Kerberos. 2. Recoger el inventario de valores del sistema. 3. Comparar y actualizar. 4. Reiniciar los servidores de Management Central en el sistema central y en los sistemas destino. 5. Añadir el sujeto principal Kerberos al archivo de grupos de confianza de todos los sistemas de punto final. 6. Permitir las conexiones de confianza. 7. Reiniciar los servidores de Management Central en el sistema central y en los sistemas destino. 8. Probar la autenticación en los servidores de Management Central.

Herramienta de rastreo de API

Puede configurar la herramienta de rastreo de API para resolver problemas con las llamadas de las API de Kerberos y de los servicios de seguridad genéricos (GSS).

El servicio de autenticación de red proporciona una herramienta de rastreo de API que un administrador puede utilizar para crear un archivo que contenga todas las llamadas a las API de Kerberos y de los servicios de seguridad genéricos (GSS). Con esta herramienta, podrá resolver con métodos más avanzados los errores que impliquen sus propias aplicaciones habilitadas para Kerberos y los errores que

podrían producirse durante la configuración del servicio de autenticación de red y durante las peticiones de tickets de Kerberos. Mediante las variables de entorno, podrá crear la herramienta y hacer que genere un archivo de anotaciones en el directorio inicial de un usuario.

Nota: Para poder llevar a cabo estos pasos, el directorio inicial ya debe existir.

Configurar la herramienta de rastreo de API

Para escribir la herramienta de rastreo de API en un archivo, lleve a cabo estos pasos en la plataforma System i en la que está configurado el servicio de autenticación de red.

Para configurar la herramienta de rastreo de API, lleve a cabo los pasos siguientes:

1. Cree un archivo envar en el directorio inicial (home) del usuario a rastrear. Por ejemplo, puede especificar `/home/nombre_perfil_usuario/envar`.
2. En la interfaz basada en caracteres, utilice `edtf /home/nombre_perfil_usuario/envar` para editar el archivo.
3. Añada las líneas siguientes al archivo envar, teniendo cuidado de que empiecen en la columna 1.

```
_EUV_SVC_MSG_LOGGING=STDOUT_LOGGING
_EUV_SVC_MSG_LEVEL=VERBOSE
_EUV_SVC_STDOUT_FILENAME=/home/nombre_perfil_usuario/trace.txt
_EUV_SVC_DBG_MSG_LOGGING=1
_EUV_SVC_DBG_TRACE=1
_EUV_SVC_DBG=*.9
```

4. Vuelva a intentar el mandato anómalo.
5. Visualice el rastreo al que hace referencia _EUV_SVC_STDOUT_FILENAME.

Después de completar el rastreo del mandato anómalo, elimine o redenomine el archivo envar, o de contrario se rastrearán todos los mandatos Kerberos que especifiquen los usuarios.

Acceder al archivo de notaciones de rastreo de API

Después de haber configurado la herramienta de rastreo de API, puede acceder al archivo de anotaciones para dar comienzo a la resolución de problemas.

Para acceder a este archivo de anotaciones, siga estos pasos:

1. En la interfaz basada en caracteres, escriba `wrklnk ('home/perfil usuario')`, siendo `perfil usuario` el nombre del perfil de usuario.
2. En el recuadro de diálogo **Trabajar con enlace de objeto**, seleccione la opción 5 para visualizar el contenido del archivo trace.txt almacenado en ese directorio.

A continuación se muestra una parte de un archivo de anotaciones de ejemplo:

```
Examinar: /home/day/trace.txt
 Registro:       1   de    5430 por 14           Columna:    1    140 por 79
 Control :

 ************Principio de datos*************
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: Version 5, Release 3, Service level V5R3M0
030515 08:53:13 (00000003) DBG1 KRB/KRB_GENERAL: STDOUT handle=4, STDERR handle==-1,
DEBUG handle=4
030515 08:53:13 (00000003) DBG6 KRB/KRB_GENERAL: Using variant character table for code set 37
030515 08:53:13 (00000003) DBG1 KRB/KRB_API: --> krb5_init_context()
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Updating profile from
QIBM/USERDATA/OS400/NETWORKAUTHENTICATION/krb5.conf
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [libdefaults]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_keytab_name = /
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   default_realm = MYCO.COM
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [realms]
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   MYCO.COM = {
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kdc = kdc1.myco.com:88
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   kpasswd_server = kdc1.myco.com:464
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   }
030515 08:53:13 (00000003) DBG8 KRB/KRB_GENERAL: Line:   [domain_realm]

F3=Salir  F10=Visualizar hex  F12=Salir  F15=Servicios  F16=Repetir buscar
F19=Izquierda   F20=Derecha
```

Si desea información sobre los mensajes de error concretos que se encuentran en el rastreo de las API, consulte la correspondiente API en Information Center.

Información relacionada

Buscador de API

Interfaces de programación de aplicaciones (API) de servicios de seguridad genéricos (GSS)

Interfaces de programación de aplicaciones (API) del servicio de autenticación de red

Resolución de problemas del servidor Kerberos en i5/OS PASE

Puede acceder a archivos de anotaciones de estado y de información para resolver problemas del servidor Kerberos en i5/OS PASE.

Durante la configuración de un servidor Kerberos en i5/OS PASE, se crean el servidor de autenticación y el servidor de administración. Estos servidores escriben mensajes de estado e informativos en un archivo de anotaciones situado en el directorio /var/krb5/log. Este archivo de anotaciones, krb5kdc.log, contiene mensajes cuya finalidad es ayudar al administrador en la tarea de resolver los problemas relacionados con las peticiones de configuración y autenticación.

Debe acceder a los archivos de anotaciones del servidor Kerberos desde la plataforma System i en la que tenga configurado el servidor Kerberos en i5/OS PASE. Para acceder a los archivos de anotaciones, siga estos pasos:

1. En una interfaz basada en caracteres, teclee `QP2TERM`. Este mandato abre un entorno de shell interactivo que le permite trabajar con aplicaciones de i5/OS PASE.
2. En la línea de mandatos, teclee `cd /var/krb5/log`.
3. En la línea de mandatos, teclee `cat /krb5kdc.log`. Así se abrirá el archivo krb5kdc.log que contiene los mensajes de error del centro de distribución de claves (KDC) de i5/OS PASE.

Archivo krb5kdc.log de ejemplo

El siguiente archivo de anotaciones de ejemplo contiene varios mensajes:

```
$
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM para kadmin/changepw@SYSTEMA.MYCO.COM,
Se necesita autenticación previa adicional

30 abr 14:18:08 systema.myco.com /usr/krb5/sbin/krb5kdc[334](Informativo):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): ISSUE: authtime 1051730288,
etypes {rep=16 tkt=16 ses=16}, jday@SYSTEMA.MYCO.COM para
kadmin/changepw@SYSTEMA.MYCO.COM

30 abr 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](Atención):
AS_REQ (3 etypes {16 3 1}) 10.1.1.2(88): NEEDED_PREAUTH:
jday@SYSTEMA.MYCO.COM para kadmin/changepw@SYSTEMA.MYCO.COM,
Se necesita autenticación previa adicional

30 abr 14:18:56 systema.myco.com /usr/krb5/sbin/krb5kdc[334](Informativo):
DISPATCH: reproducción encontrada y retransmitida
$
```

Mandatos del servicio de autenticación de red

Estos mandatos pueden ayudarle a configurar y utilizar el servicio de autenticación de red.

Tabla 38. Mandatos del servicio de autenticación de red

Mandato	Descripción
config.krb	Configura los servidores y los clientes del servicio de autenticación de red.
kadmin	Administra la base de datos del servicio de autenticación de red.
kadmind_daemon	Inicia el servidor de administración del servicio de autenticación de red.
kdb5_util	Permite que un administrador realice procedimientos de mantenimiento de bajo nivel en la base de datos del servicio de autenticación de red.
kdestroy	Destruye una memoria caché de credenciales (también llamada tabla de claves).
kinit	Obtiene o renueva un ticket de otorgamiento de tickets.
klist	Visualiza el contenido de una tabla de claves o memoria caché de credenciales.
kpasswd	Cambia la contraseña de un sujeto principal.
krb5kdc	Inicia el centro de distribución de claves (KDC) multihebra del servicio de autenticación de red.
ksetup	Gestiona las entradas de servicio de autenticación de red en el directorio LDAP para un reino de servicio de autenticación de red.
ksu	Conmuta a otro ID de usuario.
ktutil	Permite a un administrador leer, escribir o editar entradas en un archivo de tabla de claves.
kvno	Visualiza el número de versión de clave actual para un sujeto principal
start.krb5	Inicia el servidor del servicio de autenticación de red.
stop.krb5	Detiene el servidor del servicio de autenticación de red.
unconfig.krb5	Desconfigura los clientes y los servicios del servicio de autenticación de red.

Para obtener más información acerca de estos mandatos, consulte la publicación *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.

Información relacionada para el servicio de autenticación de red

Los manuales del producto, los sitios Web y otras colecciones de temas de Information Center contienen información relacionada con la colección de temas del servicio de autenticación de red. Puede ver o imprimir cualquiera de los archivos PDF.

Manuales

Si pide el CD del *paquete de ampliación de AIX*, podrá acceder a la documentación del servicio de autenticación de red. Aunque los manuales están escritos para los sistemas operativos AIX, Solaris y Linux, puede utilizar muchos de los mandatos del servicio de autenticación de red en el sistema operativo i5/OS. Cuando instale el producto Servicio de autenticación de red en el sistema AIX, la documentación se instala en el directorio /usr/lpp/krb5/doc/pdf/en_US.

Además, si instala el producto Network Authentication Enablement (5722-NAE o 5761-NAE) en el sistema, podrá acceder a los mismos manuales, tanto en formato PDF como HTML, desde el directorio /usr/lpp/krb5/doc/.

- *IBM Network Authentication Service AIX, Linux, and Solaris Administrator's and User's Guide*.
- *IBM Network Authentication Service AIX, Linux, and Solaris Application Development Reference*.

Nota: Encontrará esta documentación en el CD del paquete de ampliación y Bonus Pack de AIX 5L.

Sitios Web

En los siguientes sitios Web hallará más información sobre cómo configurar un servidor Kerberos con un sistema operativo concreto.

- Windows 2000 Server
- z/OS Security Server Network Authentication Service Administration

Otros temas de Information Center

- Las interfaces de programación de aplicaciones (API) del servicio de autenticación de red
- Las interfaces de programación de aplicaciones (API) de servicios de seguridad genéricos (GSS)
- Correlación de identidades de empresa (EIM)
- Inicio de sesión único

Petición de comentarios (RFC)

Las peticiones de comentarios (RFC) son definiciones escritas de los estándares de protocolos y estándares propuestos que se utilizan para Internet. Las siguientes peticiones de comentarios (RFC) podrían servirle de ayuda para comprender el protocolo Kerberos y las funciones relacionadas con él:

RFC 1509
: En la RFC 1509: Generic Security Service API : C-bindings, el equipo negociador de ingenieros de Internet (IETF) define formalmente las API de GSS.

RFC 1510
: En la RFC 1510: The Kerberos Network Authentication Service (V5), el equipo negociador de ingenieros de Internet (IETF) define formalmente el protocolo Kerberos V5.

RFC 1964
: En la RFC 1964: The Kerberos Version 5 GSS-API Mechanism, el equipo negociador de ingenieros de Internet (IETF) define las especificaciones de Kerberos Versión 5 y de las API de GSS.

RFC 2743

En la RFC 2743: Generic Security Service Application Program Interface Versión 2, Actualización 1, el equipo negociador de ingenieros de Internet (IETF) define formalmente las API de GSS.

Para ver las peticiones de comentarios (RFC), vaya al motor de búsqueda del índice de RFC que se encuentra en el sitio Web del editor de RFC  . Busque el número de la RFC que desea ver. Los resultados del motor de búsqueda visualizan el correspondiente título de la RFC, su autor, la fecha y el estado.

Referencia relacionada

"Archivo PDF para el Servicio de autenticación de red" en la página 2
Puede ver e imprimir un archivo PDF de esta información.

Capítulo 2. Términos y condiciones especiales

Esta información contiene términos y condiciones especiales, así como las marcas registradas aplicables al servicio de autenticación de red.

Esta información se ha escrito para productos y servicios ofrecidos en Estados Unidos de América. IBM puede no ofrecer los productos, servicios o características tratados en este documento en otros países. Póngase en contacto con el representante local de IBM que le informará sobre los productos y servicios disponibles actualmente en su área. 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 temas de este documento. La posesión de este documento no le confiere 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
Tokio 106-0032, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en que dichas disposiciones entren en contradicción con las leyes locales: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, DE COMERCIALIZACIÓN O DE ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad de las garantías, 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. Periódicamente se efectúan cambios en la información incluida en este documento; estos cambios se incorporarán en nuevas ediciones de la información. IBM puede efectuar mejoras y/o cambios en los productos y/o programas descritos en esta información en cualquier momento y sin previo aviso.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno 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 uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

Los licenciatarios de este programa que deseen obtener información acerca de él con el fin de: (i) intercambiar la información entre los 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
Department LZKS
11400 Burnet Road
Austin, TX 78758
Estados Unidos de América

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluyendo en algunos casos el pago de una cantidad.

IBM proporciona el programa bajo licencia descrito en este documento, así como todo el material bajo licencia disponible, según los términos del Acuerdo de Cliente de IBM, del Acuerdo Internacional de Programas bajo Licencia de IBM o de cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Tal vez se hayan realizado mediciones en sistemas que estén en fase de desarrollo y no existe ninguna garantía de que esas mediciones vayan a ser iguales en los sistemas disponibles generalmente. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no 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 los 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 posibilidades de los productos que no son de IBM deben dirigirse a las personas que los suministran.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Todos los precios de IBM mostrados son precios actuales de venta al por menor sugeridos por IBM y están sujetos a modificaciones sin previo aviso. Los precios de los concesionarios pueden ser diferentes.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que muestran técnicas de programación en varias plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar nada a IBM, bajo el propósito de desarrollo, uso, márketing o distribución de programas de aplicación de acuerdo con la interfaz de programación de la aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo.

Los ejemplos no se han probado minuciosamente bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni implicar la fiabilidad, servicio o funcionalidad de estos programas.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

El siguiente aviso de copyright y permiso se aplica a partes de esta información obtenidas del Massachusetts Institute of Technology.

Copyright © 1985-1999 del Massachusetts Institute of Technology.

La exportación de software que emplee cifrado fuera de Estados Unidos puede exigir una licencia específica del Gobierno de EE.UU. Es responsabilidad de la persona u organización que contemple la exportación obtener dicha licencia antes de efectuar la exportación.

DENTRO DE DICHA RESTRICCIÓN, por la presente se otorga permiso para utilizar, copiar, modificar y distribuir este software y su documentación para cualquier finalidad y sin pagar ninguna tasa, siempre que la anterior nota de derechos de autor conste en todas las copias y que tanto la nota de derechos de autor como la nota referente a este permiso aparezcan en la documentación de soporte, y que el nombre del M.I.T. no se utilice en anuncios ni en publicidad relacionados con la distribución del software sin el previo permiso por escrito específico. Además, si modifica este software, debe etiquetarlo como software modificado y no distribuirlo de forma que pueda confundirse con el software original de MIT. El M.I.T. no efectúa ninguna declaración sobre la idoneidad de este software para un fin determinado. Este software se ofrece "tal cual", sin garantías implícitas ni explícitas.

El siguiente aviso de copyright y permiso se aplica al sistema OpenVision Kerberos Administration ubicado en kadmin/create, kadmin/dbutil, kadmin/passwd, kadmin/server, lib/kadm5 y en partes de lib/rpc:

Copyright, OpenVision Technologies, Inc., 1996. Reservados todos los derechos. AVISO: La recuperación del código fuente del sistema OpenVision Kerberos Administration, como se describe más abajo, indica su aceptación de los siguientes términos. Si no acepta los siguientes términos, no recupere el sistema de administración OpenVision Kerberos. Puede utilizar y distribuir libremente el código fuente y el código de objeto compilados a partir de él, con o sin modificaciones, aunque este código fuente se suministra al cliente "TAL CUAL", SIN GARANTÍAS DE NINGÚN TIPO, INCLUIDAS, SIN LIMITACIÓN, LAS GARANTÍAS DE COMERCIALIZACIÓN O ADECUACIÓN A UN PROPÓSITO DETERMINADO O CUALQUIER OTRA GARANTÍA, EXPLÍCITA O IMPLÍCITA. EN NINGÚN CASO TENDRÁ OPENVISION NINGUNA RESPONSABILIDAD SOBRE LAS PÉRDIDAS DE BENEFICIOS, PÉRDIDAS DE DATOS O COSTES DE ADQUISICIÓN O SUSTITUCIÓN DE BIENES O SERVICIOS, NI SOBRE LOS DAÑOS ESPECIALES, INDIRECTOS O CONSECUTIVOS PROCEDENTES DE ESTE ACUERDO, INCLUIDOS, SIN LIMITACIÓN, LOS RESULTANTES DE LA UTILIZACIÓN DEL CÓDIGO FUENTE O LAS ANOMALÍAS DE EJECUCIÓN DEL MISMO O DE CUALQUIER OTRO TIPO.

OpenVision conserva todos los copyrights sobre el código fuente donado. OpenVision también conserva el copyright de los trabajos derivados del código fuente, ya sean creados por OpenVision o por terceros. Debe conservarse el aviso de copyright de OpenVision si se efectúan trabajos derivados basados en el código fuente donado. OpenVision Technologies Inc. ha donado este sistema de Administración de Kerberos a MIT para su inclusión en la distribución estándar de Kerberos 5. Esta donación subraya nuestro compromiso en proseguir el desarrollo de la tecnología Kerberos y nuestro agradecimiento por el valioso trabajo realizado por el MIT y la comunidad Kerberos.

Kerberos V5 incluye documentación y software desarrollado en la University de California en Berkeley, que incluye este aviso de copyright:

Copyright © 1983 Regents of the University of California. Reservados todos los derechos.

Se permite la redistribución y utilización en formato fuente y binario, con o sin modificaciones, siempre y cuando se cumplan las siguientes condiciones:

1. Las redistribuciones de código fuente deben contener el aviso de copyright anterior, esta lista de condiciones y la siguiente declaración de limitación de responsabilidad.

2. Las redistribuciones en formato binario deben reproducir el aviso de copyright anterior, esta lista de condiciones y la siguiente declaración de limitación de responsabilidad en la documentación y/o en otros materiales suministrados con la distribución.
3. Todos los materiales de publicidad que mencionen características o uso de este software deben mostrar el siguiente reconocimiento:

   Este producto incluye software desarrollado por la University de California, Berkeley y sus colaboradores.
4. Ni el nombre de la Universidad ni los nombres de sus colaboradores pueden utilizarse para respaldar o promocionar productos derivados de este software sin previo permiso escrito específico.

Se otorga permiso para realizar y distribuir copias literales de este manual siempre y cuando se conserven los avisos de copyright y este permiso en todas las copias.

Se otorga permiso para copiar y distribuir versiones modificadas de este manual bajo las condiciones para copias literales, siempre y cuando todo el trabajo derivado resultante se distribuya bajo los términos de un aviso de permiso idéntico a este. Se otorga permiso para copiar y distribuir traducciones de este manual a otros idiomas, bajo las condiciones anteriores referentes a versiones modificadas.

Marcas registradas

Los términos siguientes son marcas registradas de International Business Machines Corporation en Estados Unidos y/o en otros países:

- AIX
- IBM
- Tivoli
- VisualAge

Kerberos es una marca registrada del Massachusetts Institute of Technology (MIT).

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y/o en otros países.

Los demás nombres de empresas, productos y servicios pueden ser marcas registradas o marcas de servicio de terceros.

Apéndice. Avisos

Esta información se ha escrito para productos y servicios ofrecidos en Estados Unidos de América.

IBM puede no ofrecer los productos, servicios o características tratados en este documento en otros países. Póngase en contacto con el representante local de IBM que le informará sobre los productos y servicios disponibles actualmente en su área. 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 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
Tokio 106-0032, Japón

El párrafo siguiente no se aplica al Reino Unido ni a ningún otro país en que dichas disposiciones entren en contradicción con las leyes locales: INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN “TAL CUAL” SIN GARANTÍA DE NINGÚN TIPO, NI EXPLÍCITA NI IMPLÍCITA, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERACIÓN, DE COMERCIALIZACIÓN O DE ADECUACIÓN A UN PROPÓSITO DETERMINADO. Algunas legislaciones no contemplan la declaración de limitación de responsabilidad de las garantías, 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. Periódicamente, se efectúan cambios en la información incluida en este documento; estos cambios 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.

Cualquier referencia hecha en esta información a sitios Web no de IBM se proporciona únicamente para su comodidad y no debe considerarse en modo alguno 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 uso que se haga de estos sitios Web es de la entera responsabilidad del usuario.

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 licenciatarios de este programa que deseen obtener información acerca de él con el fin de: (i) intercambiar la información entre los 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

Dicha información puede estar disponible, sujeta a los términos y condiciones apropiados, incluyendo en algunos casos el pago de una cantidad.

El programa bajo licencia descrito en este documento y todo el material bajo licencia disponible para el mismo, se proporciona bajo los términos del Acuerdo de Cliente IBM, el Acuerdo de Licencia de Programa Internacional IBM, el Acuerdo de Licencia para Código Máquina IBM o cualquier otro acuerdo equivalente entre ambas partes.

Los datos de rendimiento incluidos aquí se determinaron en un entorno controlado. Por lo tanto, los resultados que se obtengan en otros entornos operativos pueden variar significativamente. Tal vez se hayan realizado mediciones en sistemas que estén en fase de desarrollo y no existe ninguna garantía de que esas mediciones vayan a ser iguales en los sistemas disponibles generalmente. Además, es posible que algunas mediciones se hayan estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información concerniente a productos no 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 los 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 posibilidades de los productos que no son de IBM deben dirigirse a las personas que los suministran.

Todas las declaraciones relativas a la dirección o intención futura de IBM están sujetas a cambios o anulación sin previo aviso y representan únicamente metas y objetivos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos 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.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicación de ejemplo en lenguaje fuente, que ilustra las técnicas de programación en diversas plataformas operativas. Puede copiar, modificar y distribuir estos programas de ejemplo de cualquier forma sin pagar nada a IBM, bajo el propósito de desarrollo, uso, márketing o distribución de programas de aplicación de acuerdo con la interfaz de programación de la aplicación para la plataforma operativa para la cual se han escrito los programas de ejemplo. Los ejemplos no se han probado minuciosamente bajo todas las condiciones. IBM, por lo tanto, no puede garantizar ni implicar la fiabilidad, servicio o funcionalidad de estos programas.

Cada copia o cada parte de los programas de ejemplo o de los trabajos que se deriven de ellos debe incluir un aviso de copyright como se indica a continuación:

© (nombre de empresa) (año). Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. _escriba el año o los años_. Reservados todos los derechos.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Información de interfaces de programación

Esta publicación sobre el servicio de autenticación de red facilita información sobre las interfaces de programación relacionadas que permiten 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
AIX 5L
Distributed Relational Database Architecture
DRDA
i5/OS
IBM
IBM (logotipo)
iSeries
NetServer
OS/400
Redbooks
System i
System p
System z
Tivoli
VisualAge
z/OS

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en Estados Unidos y/o en otros países.

Linux es una marca registrada de Linus Torvalds en Estados Unidos y/o en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y/o en otros países.

Los demás nombres de empresas, productos y servicios pueden ser marcas registradas o marcas 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