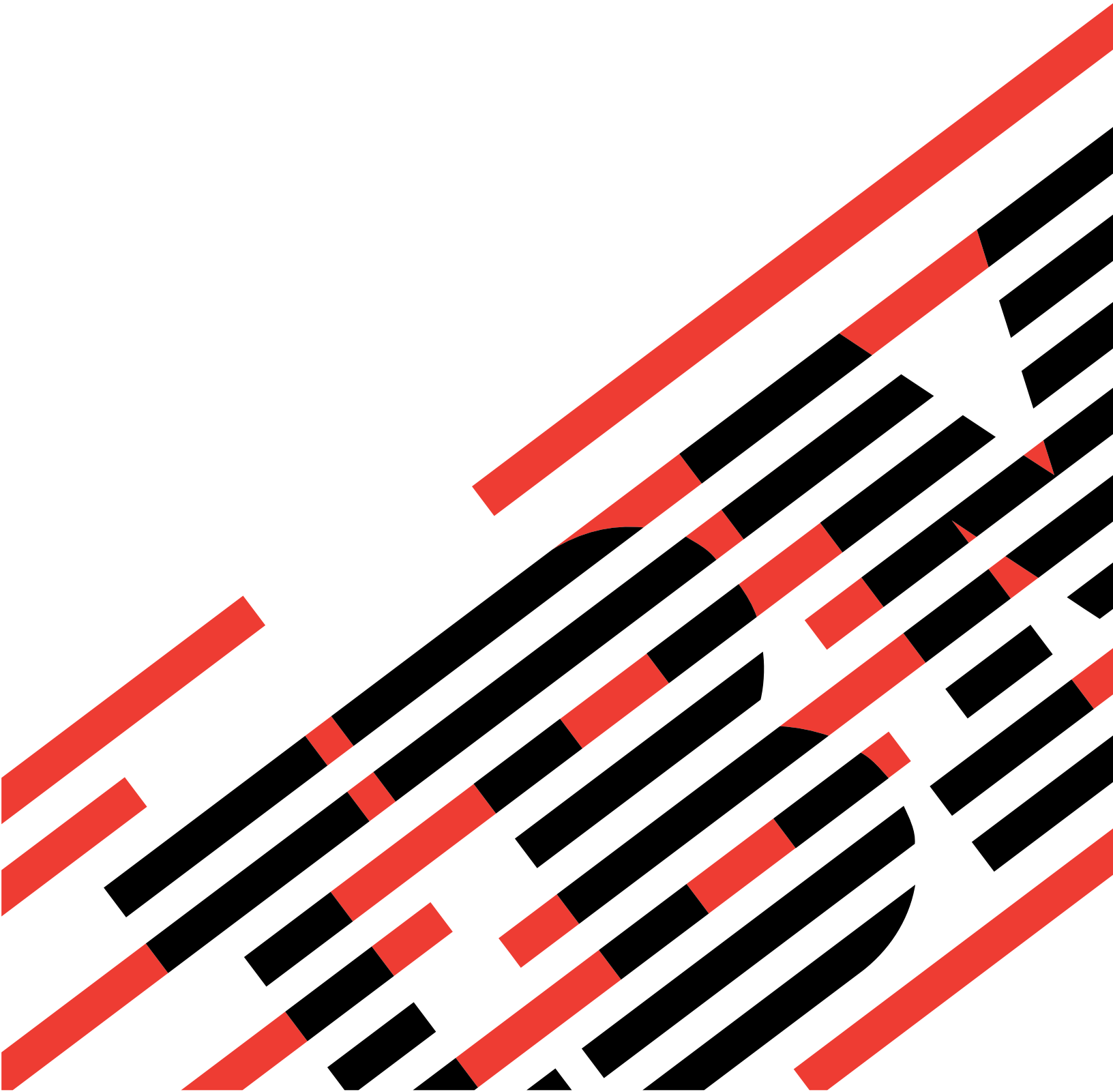
IBM

eserver

iSeries

Servicio de autenticación de red



IBM

@server

iSeries

Servicio de autenticación de red

Contenido

Servicio de autenticación de red

El servicio de autenticación de red permite al iSeries y a varios servicios del iSeries, como iSeries Access para Windows, utilizar un ticket Kerberos como sustituto opcional del nombre y la contraseña de usuario para la autenticación de un usuario. El protocolo Kerberos, desarrollado por el Massachusetts Institute of Technology, permite a un sujeto (a un usuario o servicio) demostrar su identidad ante otro servicio en una red no segura. La autenticación de sujetos se completa a través de un servidor centralizado conocido como centro de distribución de claves (KDC). El KDC autentica a un usuario con un ticket Kerberos. Estos tickets demuestran la identidad del sujeto ante otros servicios en una red. Cuando un sujeto se ha autenticado mediante estos tickets, pueden intercambiarse datos cifrados con un servicio de destino. El servicio de autenticación de red verifica la identidad de un usuario o servicio en una red. Las aplicaciones pueden autenticar con garantías a un usuario y transmitir 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 red. El servicio de autenticación de red implementa las siguientes especificaciones:

- Protocolo Kerberos Versión 5 tal como define la petición de comentario (RFC) 1510
- Muchas de las API de protocolo Kerberos estándar corrientes en la industria actual
- Las API GSS (Generic Security Service) tal como las definen los RFC 1509, 1964, y 2743

El servicio de autenticación de red del iSeries interopera con servicios de autenticación, delegación y confidencialidad de datos que se ajustan a estos RFC, como las API SSPI (Security Service Provider Interface) Windows 2000 de Microsoft.

Además, el servicio de autenticación de red puede utilizarse con EIM (Enterprise Identity Mapping) para habilitar un entorno único de inicio de sesión. El inicio de sesión único es útil para usuarios, administradores y desarrolladores de aplicaciones porque permite un sistema de gestión de contraseñas más sencillo en múltiples plataformas sin necesidad de cambiar las políticas de seguridad subyacentes. Los siguientes artículos proporcionan detalles sobre la habilitación del inicio de sesión único utilizando el servicio de autenticación de red y EIM(Enterprise Identity Mapping):

Habilitación de inicio de sesión único
Este artículo proporciona información conceptual sobre las ventajas del inicio de sesión único y un resumen de cómo el servicio de autenticación de red y EIM (Enterprise Identity Mapping) colaboran para crear un entorno de inicio de sesión único.

Escenario: habilitación de inicio de sesión único
Este artículo muestra un ejemplo de cómo el administrador del Departamento de entrada de pedidos de MyCo ha habilitado un entorno de inicio de sesión único. El administrador desea que el usuario se autentique para las aplicaciones iSeries utilizando su contraseña e ID de dominio de Windows (R). Se incluyen instrucciones detalladas que muestran cómo el administrador de MyCo ha configurado el servicio de autenticación de red y EIM para habilitar el inicio de sesión único.

El debate sobre el servicio de autenticación de red incluye los siguientes temas:

Novedades de la V5R2
Este tema describe las funciones nuevas para el servicio de autenticación de red en este release e incluye enlaces a información adicional sobre estas funciones.

Imprima este tema
Este tema proporciona instrucciones para descargar e imprimir una versión PDF sobre esta información.

¿Cómo funciona el servicio de autenticación de red?
Este tema proporciona un resumen sobre cómo funciona el servicio de autenticación de red en una red que utiliza el protocolo Kerberos para la autenticación de usuarios.

Terminología del servicio de autenticación de red
Este tema define la terminología relacionada con los servicios de autenticación de red.

Protocolos de servicio de autenticación de red
Este tema discute los conceptos básicos del protocolo Kerberos y las API GSS. Se facilitan enlaces a RFC y otra información relacionada.

Escenarios de servicio de autenticación de red
Este tema describe varios escenarios empresariales diferentes en los que se implementa el servicio de autenticación de red.

Planificación del servicio de autenticación de red
Este tema describe los pasos previos necesarios antes de trabajar con el servicio de autenticación de red.

Configuración del servicio de autenticación de red
Este tema describe cómo configurar el servicio de autenticación de red en el Navigator de iSeries.

Gestión del servicio de autenticación de red
Este tema describe las tareas que pueden utilizar los administradores y usuarios para gestionar el servicio de autenticación de red.

Solución de problemas relacionados con el servicio de autenticación de red
Este tema describe los mensajes y la solución de problemas para el servicio de autenticación de red y aplicaciones relacionadas.

Información relacionada
Este tema describe y facilita enlaces a otros temas relacionados con el protocolo Kerberos y las API GSS.

Información legal
Este tema facilita información legal importante relacionada con el uso del protocolo Kerberos y sus API asociadas.

Novedades de la V5R2

El servicio de autenticación de red permite al iSeries participar en una red que utiliza el protocolo Kerberos para autenticar a los usuarios en la red.

El servicio de autenticación de red en el Navigator de iSeries
El asistente de autenticación de red facilita la configuración del iSeries para participar en una red Kerberos. El asistente le permite configurar el iSeries para participar en un reino Kerberos. De este modo, utilizando el protocolo Kerberos pueden transmitirse tickets a los servicios en representación de un usuario, autenticando a este usuario para los recursos de la red. Consulte los temas siguientes para completar la configuración:

- Escenarios de servicio de autenticación de red
  Proporciona breves descripciones de dos situaciones de cliente en las que se utiliza el servicio de autenticación de red.
-
- Configuración del servicio de autenticación de red
  Proporciona un resumen de todos los pasos necesarios para configurar el servicio de autenticación de red.
-
- Gestión del servicio de autenticación de red
  Proporciona un resumen de todas las tareas que puede completar con el Navigator de iSeries.

Soporte para mandato de Qshell nuevo
Los usuarios pueden solicitar y trabajar con tickets con mandatos Qshell. En este release, se ha añadido el mandato **kpasswd** para permitir a los usuarios cambiar sus contraseñas en el centro de distribución de claves.

- Cambiar las contraseñas de Kerberos
  Proporciona información sobre cómo utilizar el mandato Qshell kpasswd.

EIM (Enterprise Identity Mapping)
EIM es un mecanismo para correlacionar una persona o identidad (p.ej. un servicio) con las identidades de usuario apropiadas en varios registros de usuario de la empresa. Si se utiliza con el servicio de autenticación de red, EIM habilita un entorno de inicio de sesión único. El iSeries utiliza EIM para permitir a las interfaces del OS/400 autenticar a los usuarios a través del servicio de autenticación de red. El iSeries y las aplicaciones también pueden aceptar tickets Kerberos y utilizar EIM para correlacionar un ID de usuario en un sistema con su sujeto Kerberos asociado.

- Habilitación de inicio de sesión único
  Proporciona información conceptual sobre las ventajas del inicio de sesión único y un resumen de cómo el servicio de autenticación de red y EIM (Enterprise Identity Mapping) colaboran para crear un entorno de inicio de sesión único.
- Escenario: habilitar el inicio de sesión único
  Proporciona un ejemplo detallado de una situación en la que se utilizan al mismo tiempo el servicio de autenticación de red y EIM para habilitar un entorno de inicio de sesión único.

Soporte de autenticación para varias aplicaciones del iSeries:

- **SQL (Structured Query Language)/ DRDA (Distributed Relational Database Architecture)**
  Ahora SQL/DRDA da soporte al uso de un ticket Kerberos para autenticar a los usuarios que acceden a las funciones de la base de datos. DRDA busca un ticket de otorgación de tickets para un usuario determinado. Si existe un ticket, en ese caso se utilizará para obtener tickets de servicio para ese usuario.
-

- **DDM (Distributed Data Management)**
  Ahora DDM da soporte al uso de un ticket Kerberos para autenticar a los usuarios que acceden a archivos remotos. DDM busca un ticket de otorgación de tickets para un usuario determinado. Si existe un ticket, en ese caso se utilizará para obtener tickets de servicio para ese usuario. **Nota:** si ha especificado un reino por omisión en el archivo de configuración Kerberos, pero no utiliza Kerberos como método de autenticación, debe eliminar el reino por omisión antes de configurar la autenticación para DDM. Para obtener información sobre la recuperación de este problema, consulte Problemas de conexión de aplicaciones y recuperación .
-
- **iSeries Access for Windows y OS/400 Host Servers**
  iSeries Access for Windows y OS/400 Host Servers dan soporte a la autenticación mediante tickets Kerberos. Desde el cliente, un usuario puede especificar que se utilice un ticket Kerberos cuando se acceda a iSeries Access Host Servers.
-
- **iSeries NetServer**
  Los clientes de iSeries NetServer pueden utilizar tickets Kerberos para la autenticación con el servidor, si se ha configurado Kerberos en la red. Sólo los clientes que dan soporte a la v5 de Kerberos pueden conectarse a iSeries NetServer cuando se habilita este soporte. Para obtener más detalles sobre los requisitos para el soporte iSeries NetServer de Kerberos, consulte soporte iSeries NetServer para la autenticación de Kerberos v5.
-
- **QFileSvr.400**
  QFileSvr.400 determinará si existe un ticket de otorgación de tickets para el usuario actual. Si existe un ticket de otorgación de tickets, en ese caso se creará un ticket de servidor para autenticar el usuario en el sistema de destino. Si no existe ningún ticket, entonces se utilizará el método actual de sustitución de contraseñas. **Nota:** si ha especificado un reino por omisión en el archivo de configuración Kerberos, pero no utiliza Kerberos como método de autenticación, debe eliminar el reino por omisión antes de configurar la autenticación para QFileSvr.400. Para obtener información sobre la recuperación de este problema, consulte Problemas de conexión de aplicaciones y recuperación .

Cómo ver qué ha cambiado o cuáles son las novedades

Para ayudarle a detectar los cambios técnicos, esta información utiliza:

- La imagen

  marca donde empieza la información nueva o modificada.
- La imagen

  marca dónde acaba la información nueva o modificada.

Para obtener más información sobre las novedades o los cambios de este release, consulte Memorándum para los usuarios

.

Imprima este tema

Para ver o descargar la versión en PDF, seleccione Servicio de autenticación de red (unos 199 KB o 50 páginas).

Para salvar un PDF en su estación de trabajo para la posterior visualización o impresión:

1. Abra el PDF en su navegador (pulse sobre el enlace anterior).
2. En el menú de su navegador, pulse **Archivo**.
3. Pulse **Guardar como...**
4. Pase al directorio en el que desea salvar el PDF.
5. Pulse **Guardar**.

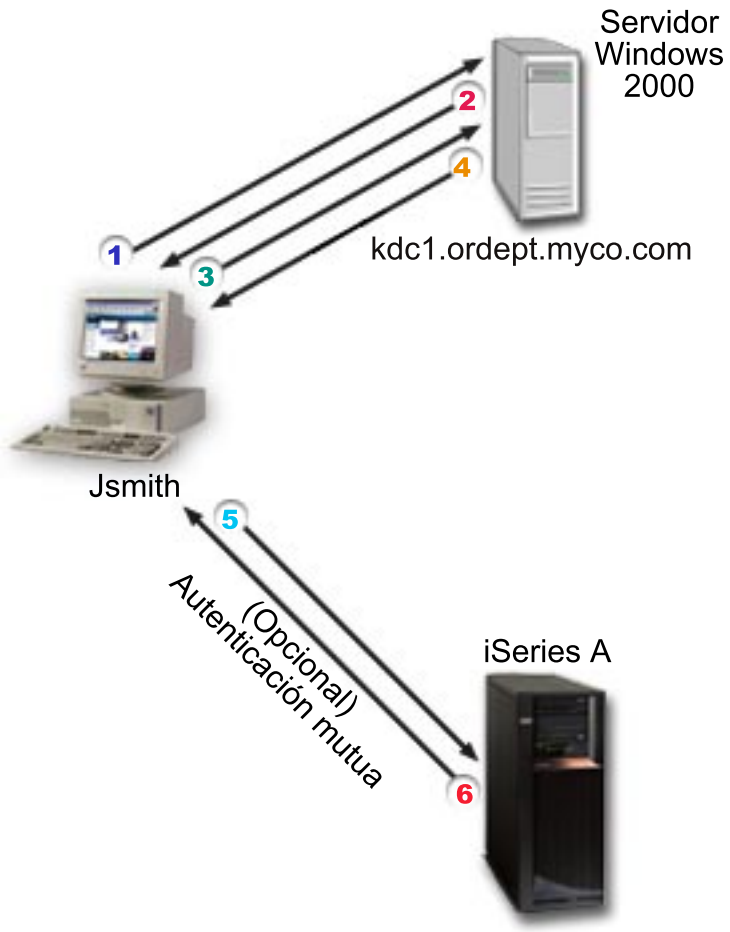
Si necesita Adobe Acrobat Reader para ver o imprimir el PDF, puede descargar una copia del sitio Web de Adobe (www.adobe.com/product/acrobat/readstep.html).

¿Cómo funciona el servicio de autenticación de red?

Como administrador de red, puede configurar el servicio de autenticación de red de forma que el sistema iSeries acepte tickets Kerberos creados por un centro de distribución de claves (KDC) centralizado con una base de datos de todos los usuarios y servicios de un reino. El iSeries y muchas aplicaciones específicas del iSeries actúan como cliente/servidor en una red Kerberos, solicitando tickets para usuarios y para servicios. Cuando un usuario solicita un ticket al KDC, se le emite un ticket inicial conocido como ticket de otorgación de tickets (TGT). El usuario puede entonces utilizar el TGT para solicitar un ticket de servicio para acceder a otros servicios y aplicaciones en la red. Para que la autenticación tenga éxito, un administrador debe registrar los usuarios, el sujeto de servicio del iSeries y las aplicaciones que utilizarán el protocolo Kerberos con el KDC. El iSeries puede actuar como un servidor, en el que los sujetos solicitan autenticación para los servicios, o bien puede actuar como un cliente que solicita tickets para aplicaciones y servicios en la red. Los siguientes gráficos ilustran el flujo de los tickets en estas dos situaciones.

iSeries como servidor

Este gráfico muestra cómo funciona la autenticación cuando un iSeries actúa como servidor en una red Kerberos. En este gráfico, el KDC de Windows (R) 2000 emite tickets al sujeto Jsmith. Jsmith desea acceder a una aplicación en el iSeries-A. En este caso, se utilizaría EIM (Enterprise Identity Mapping) en el servidor para correlacionar el sujeto Kerberos con un perfil de usuario de iSeries. Ello se haría para cualquier función del servidor iSeries bajo el protocolo Kerberos, como iSeries-Access for Windows.

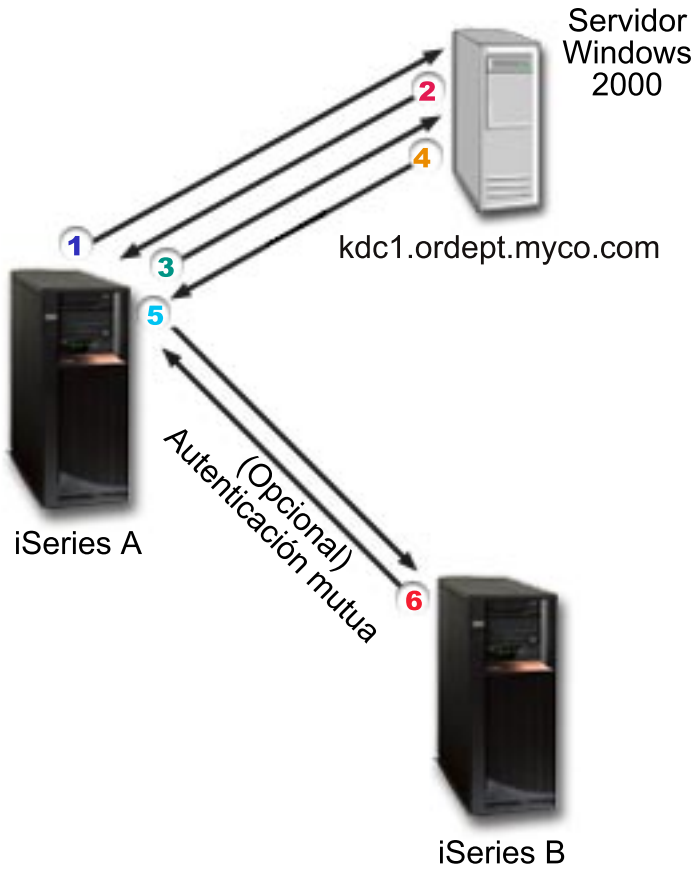


Esta descripción muestra una visión general de cómo funciona este proceso de autenticación en una red:

1. El usuario, Jsmith, solicita un ticket del KDC cuando inicia la sesión en la red Kerberos. Éste remite una solicitud al KDC referente a un ticket de otorgación de tickets.
2. El KDC valida el nombre de sujeto y la contraseña y envía un ticket de otorgación de tickets a Jsmith.
3. Jsmith requiere acceso a una aplicación de un servidor iSeries. Llamando a las API del servicio de autenticación de red, la aplicación envía el TGT de Jsmith al KDC para solicitar un ticket de servicio para la aplicación o servicio en cuestión. La máquina local del sujeto administra una antememoria de credenciales que contiene tickets e información de identificación de otro tipo para el usuario. Estas credenciales se leen de la antememoria cuando se necesitan y, cuando se obtienen nuevas credenciales, éstas se almacenan en la antememoria. De este modo se libera a la aplicación de la responsabilidad de gestionar las credenciales por sí misma.
4. El KDC responde con el ticket de servicio.
5. La aplicación envía el ticket del servidor al servicio iSeries para autenticar al usuario.
6. La aplicación del servidor valida el ticket llamando las API de servicio de autenticación de red y, opcionalmente puede remitir una respuesta al cliente para una autenticación mutua.

iSeries como cliente

Este gráfico muestra cómo funciona la autenticación cuando un iSeries actúa como cliente en una red Kerberos. En este gráfico, el KDC de Windows (R) 2000 emite tickets al sujeto iSeries-A. El iSeries-A puede autenticarse para otros servicios. En este ejemplo, se utilizaría EIM (Enterprise Identity Mapping) en el iSeries B para correlacionar el sujeto kerberos con un perfil de usuario de iSeries. Ello se haría para cualquier función del servidor iSeries bajo el protocolo Kerberos, como QFileSvr.400.



*

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

1. Un sujeto, Jsmith, se registra en el iSeries-A y seguidamente solicita un ticket de otorgación de tickets mediante un mandato kinit en el Intérprete Qshell. El iSeries envía esta solicitud al KDC.
2. El KDC valida el nombre de sujeto y la contraseña y envía un ticket de otorgación de tickets a Jsmith.
3. Jsmith requiere acceso a una aplicación de un servidor iSeries. Llamando a las API del servicio de autenticación de red, la aplicación envía el TGT de Jsmith al KDC para solicitar un ticket de servicio para la aplicación o servicio en cuestión. La máquina local del sujeto administra una antememoria de credenciales que contiene tickets, claves de sesión e información de identificación de otro tipo para el usuario. Estas credenciales se leen de la antememoria cuando se necesitan y, cuando se obtienen nuevas credenciales, éstas se almacenan en la antememoria. De este modo se libera a la aplicación de la responsabilidad de gestionar las credenciales por sí misma.

4. El KDC responde con el ticket de servicio. **Nota:** debería añadirse al KDC un sujeto de servicio para iSeries-B y también debería configurarse el servicio de autenticación de red en el iSeries-B.
5. La aplicación envía el ticket del servidor al servicio iSeries para autenticar al usuario.
6. La aplicación del servidor valida el ticket llamando las API de servicio de autenticación de red y, opcionalmente puede remitir una respuesta al cliente para una autenticación mutua.

Terminología del servicio de autenticación de red

El servicio de autenticación de red utiliza la siguiente terminología relacionada con el protocolo Kerberos:

Tickets reenviables
Los tickets reenviables permiten a un servidor transmitir las credenciales del solicitante a otro servicio. Para ello, debe haberse solicitado el TGT con la opción reenviable y se permitirá al servidor delegar credenciales.

Centro de distribución de claves (KDC)
Un servicio de red que proporciona tickets y claves de sesión provisionales. El KDC guarda una base de datos de sujetos (usuarios y servicios) y sus claves secretas asociadas. Está compuesto del servidor de autenticación y el servidor de tickets de otorgación de tickets. Es importante que utilice una máquina segura para actuar como KDC. Si algún intruso accediera al KDC, todo el reino podría verse comprometido. **Nota:** en el sistema iSeries no existe soporte para el KDC

Tabla de claves
Un archivo del sistema principal del servicio. Cada entrada del archivo contiene la clave secreta y el nombre del sujeto del servicio. En el iSeries, se crea un archivo de claves durante la configuración del servicio de autenticación de red. Cuando un servicio solicita autenticación para un iSeries con el servicio de autenticación de red configurado, ese iSeries busca las credenciales de ese servicio en el archivo de claves. Para asegurarse de que los usuarios y servicios se autentican correctamente, debe registrarlos en el KDC y en el iSeries.

Servidor de contraseñas
Permite a los clientes cambiar remotamente sus contraseñas en el KDC. El servidor de contraseñas normalmente se ejecuta en la misma máquina que el KDC.

Sujeto
El nombre de un usuario o servicio en una red Kerberos. Un usuario se considera una persona que utiliza un servicio para identificar una aplicación específica o conjunto de servicios del sistema operativo. En el iSeries, se utiliza el sujeto de servicio **krbsvr400** para identificar el servicio que utiliza iSeries Access for Windows, servidores de Telnet y QFileSrv.400 cuando la autenticación se realiza desde el cliente para el iSeries.

Tickets que admiten proxy
Un ticket que admite proxy es un ticket de otorgación de tickets (TGT) que le permite obtener un ticket para un servicio con direcciones IP distintas de las del TGT. A diferencia de los tickets reenviables, no es posible enviar por proxy un TGT nuevo desde su TGT actual; sólo pueden enviarse por proxy los tickets de servicio. Los tickets reenviables le permiten transferir su identidad

completa (TGT) a otra máquina, mientras que los tickets que admiten proxy sólo le permiten transferir determinados tickets. Los tickets que admiten proxy permiten a un servicio realizar una tarea en representación de un sujeto. El servicio debe poder asumir la identidad del sujeto con una finalidad determinada. Un ticket que admite proxy indica al KDC que puede enviar un ticket nuevo a una dirección de red diferente, basándose en el ticket de otorgación de tickets original. Los tickets que admiten proxy no requieren contraseñas.

Reino
Un conjunto de usuarios y servidores para los que un determinado centro de distribución de claves (KDC) es la autoridad de autenticación.

Confianza de los reinos
El protocolo Kerberos busca el archivo de configuración para determinar la confianza de los reinos o, por omisión, busca las relaciones de confianza en la jerarquía de los reinos. El uso de **reinos de confianza** en el servicio de autenticación de red le permite saltarse este proceso y crea un método abreviado para la autenticación. La confianza de los reinos puede utilizarse en las redes en las que los reinos se encuentran en dominios diferentes. Por ejemplo, si una empresa tiene un reino en NY.myco.com y otro en LA.myco.com, puede establecer una relación de confianza entre estos dos reinos. Si dos reinos tienen confianza entre sí, sus KDC asociados deben compartir una clave. Antes de crear un método abreviado, debe configurar los KDC para que confíen entre sí.

Tickets renovables
En algunos casos, es posible que una aplicación o servicio necesite disponer de tickets que sean válidos para un período de tiempo prolongado. Sin embargo, ese tiempo prolongado podría permitir a alguien robar esas credenciales que serían válidas hasta que el ticket caducara. Los tickets renovables permiten a las aplicaciones obtener tickets válidos para períodos prolongados de tiempo, al mismo tiempo que reducen las posibilidades de robo. Los tickets renovables contienen dos fechas de caducidad. La primera caducidad es válida para la instancia actual del ticket y la segunda se refiere a la caducidad más tardía permitida para el ticket.

Ticket de servicio
Un ticket que autentica un sujeto para un servicio.

Servicio de otorgación de tickets (TGS)
Un servicio proporcionado por el KDC que emite tickets de servicio.

Tickets de otorgación de tickets (TGT)
Un ticket que permite el acceso al servicio que otorga tickets en el KDC. El KDC transmite los tickets de otorgación de tickets al sujeto cuando el sujeto completa una petición satisfactoria. En un entorno Windows (R) 2000, un usuario entra en la red y el KDC verifica el nombre del sujeto y la contraseña cifrada y, a continuación, envía un ticket de otorgación de tickets al usuario. Los usuarios pueden solicitan un ticket desde un servidor iSeries utilizando el mandato kinit en la interfaz basada en caracteres del Intérprete de Qshell.

Protocolos del servicio de autenticación de red

El servicio de autenticación de red utiliza el protocolo Kerberos junto con las API GSS (Generic Security Services) para la autenticación, facilitando servicios de autenticación y seguridad. Las secciones siguientes proporcionan una descripción general de estos protocolos y el modo en que se utilizan en el iSeries. Para obtener más información sobre estos estándares, se incluyen enlaces a la solicitud de comentarios (RFC) asociada y a otras fuentes externas.

Protocolo Kerberos

El protocolo Kerberos proporciona autenticación de terceros cuando un usuario demuestra su identidad ante un servidor centralizado, llamado el centro de distribución de claves (KDC), que emite tickets al usuario. El usuario puede entonces utilizar estos tickets para demostrar su identidad en la red. El ticket suprime la necesidad de registros múltiples en sistemas diferentes. Las API Kerberos a las que el iSeries da soporte tienen su origen en el Massachusetts Institute of Technology y se han convertido en el estándar utilizado para el uso del protocolo Kerberos.

Las presunciones del entorno de seguridad

El protocolo Kerberos asume que todos los intercambios de datos se producen en un entorno en el que pueden insertarse, modificarse o interceptarse paquetes a voluntad. Utilice Kerberos como uno de los niveles de un plan de seguridad global. A pesar de que el protocolo Kerberos le permite autenticar usuarios y aplicaciones en la red, debe tener en cuenta ciertas restricciones al definir sus objetivos de seguridad de la red:

- El protocolo Kerberos no protege contra ataques de denegación de servicio. Existen lugares en estos protocolos donde un intruso puede evitar que una aplicación participe en los pasos de autenticación apropiados. Es preferible dejar la detección y solución de dichos ataques en manos de administradores y usuarios humanos.
- El proceso de compartir claves o el robo de claves puede permitir ataques de imitación. Si de algún modo los intrusos logran robar la clave de un sujeto, 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 el adivinar una contraseña. Si un usuario escoge 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.

Para obtener más información sobre el protocolo Kerberos, consulte las siguientes fuentes:

The Kerberos Network Authentication Service (V5)

.
El grupo IETF (Internet Engineering Task Force) define formalmente el protocolo Kerberos en RFC 1510.

Kerberos: The 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 del servicio de autenticación de red

Este tema del Centro de información proporciona una lista de las API del servicio de autenticación de red y descripciones breves de sus funciones.

Las API GSS (Generic Security Services)

Las API GSS proporcionan servicios de seguridad genéricamente y les dan soporte una amplia gama de tecnologías de seguridad, como el protocolo Kerberos. Ello permite transferir las aplicaciones GSS a diferentes entornos. Por ello es recomendable utilizar estas API en lugar de las API Kerberos. Puede escribir aplicaciones que utilicen las API GSS para comunicarse con otras aplicaciones y clientes de la misma red. Cada una de las aplicaciones que participan en la comunicación tiene un papel en este intercambio. Con las API GSS, las aplicaciones pueden realizar las siguientes operaciones:

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

Para obtener más información sobre las API GSS, consulte las siguientes fuentes:

Generic Security Service Application Program Interface Version 2, Update 1

.
El grupo IETF (Internet Engineering Task Force) define formalmente las API GSS en RFC 2743.

Generic Security Service API : C-bindings

.
El grupo IETF (Internet Engineering Task Force) especifica los enlaces C de las API GSS en RFC 1509.

The Kerberos Version 5 GSS-API Mechanism

.
El grupo IETF (Internet Engineering Task Force) define las especificaciones de la API GSS y de Kerberos versión 5 en RFC 1964.

Las API GSS (Generic Security Service Application Programmable Interfaces)
Este tema del Centro de información proporciona una lista de las API GSS y descripciones breves de sus funciones.

Escenarios del servicio de autenticación de red

Los siguientes escenarios proporcionan descripciones de entornos habituales en los que puede utilizarse el servicio de autenticación de red para permitir al iSeries participar en una red Kerberos. Consulte los escenarios siguientes para familiarizarse con los detalles técnicos y de configuración relacionados con la configuración del servicio de autenticación de red:

Escenario: configurar el servicio de autenticación de red con el KDC existente
Este tema describe la situación de un cliente, en la que un administrador está configurando la autenticación de red en un entorno Windows (R) 2000, donde se ha instalado y configurado un centro de distribución de claves.

Escenario: habilitar el inicio de sesión único
Este escenario muestra cómo utilizar el servicio de autenticación de red con EIM /Enterprise Identity Mapping) para habilitar el inicio de sesión único. El administrador desea que los usuarios puedan utilizar su inicio de sesión en Windows (R) 2000 para autenticarse ante los sistemas iSeries y las aplicaciones de iSeries Access for Windows.

Escenario: configurar el servicio de autenticación de red con el KDC existente

Situación

Usted es un administrador de red que se encarga de la administración de la red del departamento de entrada de pedidos de su empresa. Recientemente ha incorporado un iSeries a su red para alojar varias aplicaciones necesarias para su departamento. Actualmente dispone de un servidor Windows (R) 2000 que actúa como centro de distribución de claves (KDC) para el reino. Todos los usuarios de esta tienen nombres de sujeto y contraseñas almacenados en el KDC. Desea añadir el iSeries al KDC. Su intención es añadir el iSeries a este reino y seguir utilizando el servidor Windows (R) 2000 como el servidor de autenticación. Tiene sus propias aplicaciones habilitadas para Kerberos que utilizan API GSS.

Este escenario tiene las siguientes ventajas:

- Simplifica el proceso de autenticación de usuarios
- Reduce los costos operativos de gestionar el acceso a los servidores de la red
- Minimiza la amenaza de robo de contraseñas

Objetivos

En este escenario, MyCo, Inc. desea añadir un sistema iSeries a un reino existente en el que un servidor Windows (R) 2000 actúa como el centro de distribución de claves. El iSeries contiene diversas

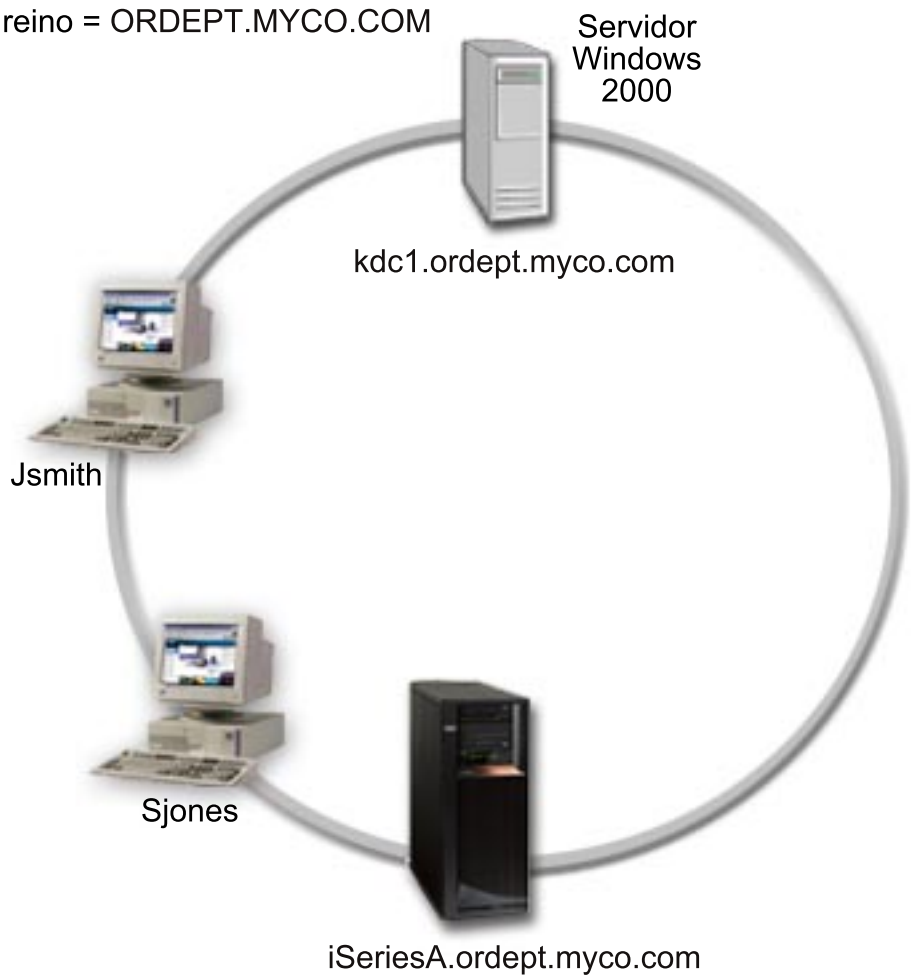
aplicaciones fundamentales para la empresa a las que deben acceder los usuarios apropiados. Para poder acceder a estas aplicaciones, el KDC debe autenticar a los usuarios. El iSeries debe añadirse al KDC del servidor Windows (R) 2000.

Los objetivos de este escenario son los siguientes:

- Permitir al iSeries participar con un centro de distribución de claves existente
- Permitir nombres de sujeto y nombres de usuario en la red
- Permitir a los usuarios de Kerberos cambiar sus propias contraseñas en el KDC

Detalles del escenario

La imagen siguiente ilustra las características de la red de MyCo.



Departamento de entrada de pedidos

- El iSeries-A se ejecuta en OS/400 Versión 5 Release 2 (V5R2) y contiene varias aplicaciones empresariales.

- El nombre de DNS del KDC es kdc1.ordept.myco.com
- El nombre de sujeto del iSeries-A es krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
- El reino por omisión para el KDC es ORDEPT.MYCO.COM
- Los PC cliente se ejecutan en Windows (R) 2000.

Pasos de configuración para este escenario

1. Completar (Ver 14) las hojas de trabajo de planificación y las listas de verificación para el servicio de autenticación de red.
2. Configurar (Ver 15) el servicio de autenticación de red en el iSeries-A.
3. Añadir (Ver 16) el iSeries-A al KDC.
4. Crear (Ver 16) un directorio de inicio para cada usuario en el iSeries-A
5. Verificar (Ver 17) la información de dominio TCP/IP para iSeries-A
6. Comprobar (Ver 17) la configuración del servicio de autenticación de red en el iSeries-A.

Detalles de configuración

Paso 1: complete las hojas de trabajo de planificación

Las siguientes listas de comprobación de planificación ilustran el tipo de información que necesita antes de empezar a configurar el servicio de autenticación de red. Para poder seguir con la configuración del servicio de autenticación de red, debe poder responder afirmativamente a todas las preguntas de la lista de comprobación de requisitos previos.

Lista de comprobación de requisitos previos	**Respuestas**
¿Su OS/400 es de la versión V5R2 (5722-SS1) o posterior?	Sí
¿Ha instalado el Proveedor de acceso de cifrado (5722-AC3) en sus sistemas iSeries?	Sí
¿Ha instalado iSeries Access for Windows (5722-XE1) en todos los PC de la red y en sus sistemas iSeries?	Sí
¿Ha instalado el subcomponente de Seguridad del Navigator de iSeries en todos los PC de la red y en sus sistemas iSeries?	Sí
¿Ha instalado el subcomponente de Red del Navigator de iSeries en todos los PC de la red y sus sistemas iSeries?	Sí
¿Tiene las autorizaciones especiales: *SECADM, *ALLOBJ y *IOSYSCFG?	Sí
¿Ha instalado alguno de los siguientes programas en el sistema seguro que actuará como un centro de distribución de claves? En caso afirmativo, ¿cuál? 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	Sí Windows (R) 2000 Server
Para Windows (R) 2000 Server y Windows (R) XP Server, ¿Ha instalado en el sistema que se utiliza como el centro de distribución de claves las Herramientas de soporte de Windows (R) que proporcionan la herramienta ktpass?	Sí

¿Están todos los PC de la red configurados en un dominio Windows (R) 2000?	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
¿Entre la hora del sistema del iSeries y la hora del sistema del KDC no hay más de cinco minutos de diferencia? Si la diferencia es superior, consulte Sincronizar las horas de los sistemas.	Sí

Necesita esta información para configurar el servicio de autenticación de red	**Respuestas**
¿Cuál es el nombre del reino por omisión Kerberos al que pertenecerá el iSeries-A?	ORDEPT.MYCO.COM
¿Cuál es el KDC para este reino Kerberos por omisión? ¿Cuál es el puerto de escucha del KDC?	kdc1.ordept.myco.com 88 (**Nota:** este es el puerto por omisión para el KDC).
¿Desea configurar un servidor de contraseñas para este reino por omisión? En caso afirmativo, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este KDC? ¿Cuál es el puerto de escucha del servidor de contraseñas?	Sí kdc1.ordept.myco.com 464 (**Nota:** este es el puerto por omisión para el servidor de contraseñas).
¿Cuál es la contraseña para los sujetos de servicio del iSeries?	iseriesa123 **Nota:** todas las contraseñas que se utilizan en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.
¿Con qué otros reinos interactuarán sus sistemas iSeries?	N/D
¿Cuál es el nombre de sistema principal del centro de distribución de claves, para cada reino?	N/D

Paso 2: Configurar el servicio de autenticación de red en el iSeries-A

Utilice la información de las hojas de trabajo para configurar el servicio de autenticación de red en el iSeries-A, del siguiente modo:

1. En el Navigator de iSeries, expanda **iSeries-A —>Seguridad**.
2. Pulse el botón derecho sobre **Servicio de autenticación de red** y seleccione **Configurar** para iniciar el asistente para la configuración. **Nota:** tras configurar el servicio de autenticación de red, esta opción será **Volver a configurar**.
3. Consulte la página **Bienvenid** donde encontrará información sobre los objetos que crea el asistente. Pulse en **Siguiente**.
4. En la página **Especificar la información del reino**, entre `ORDEPT.MYCO.COM` en el campo **Reino por omisión**. Pulse en **Siguiente**.
5. En la página **Especificar información del KDC**, entre `kdc1.ordept.myco.com` en el campo **KDC** y 88 en el campo **Puerto**. Pulse en **Siguiente**.
6. En la página **Especificar información de la contraseña**, seleccione **Sí**. Entre `kdc1.ordept.myco.com` en el campo **Servidor de contraseñas** y 464 en el campo **Puerto**. Pulse en **Siguiente**.

7. En la página **Crear entrada de tabla de claves**, seleccione la **Autenticación de Kerberos del iSeries**. Pulse en **Siguiente**.
8. En la página **Crear entrada de tabla de claves del iSeries**, anote la tabla de claves y el sujeto del iSeries-A. Necesitará el nombre de sujeto cuando lo añada al KDC. Entre y confirme una contraseña. Por ejemplo, el administrador de MyCo ha entrado `iseriesa123`. **Nota:** todas las contraseñas que se utilizan en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.
9. Pulse en **Siguiente**.
10. En la página **Resumen**, repase los detalles de configuración del servicio de autenticación de red. Pulse en **Finalizar**.

Ya ha configurado el servicio de autenticación de red en el iSeries-A. El siguiente paso consiste en añadir el nombre de sujeto en el KDC.

Paso 3: Añadir el nombre de sujeto del iSeries-A en el KDC

Para añadir el sistema iSeries al KDC de Windows (R) 2000, utilice la documentación referente a la incorporación de sujetos al KDC. Por convención, el nombre del sistema iSeries puede utilizarse como nombre de usuario. Añada el siguiente nombre de sujeto al KDC:

```
krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
```

En un servidor Windows (R) 2000, siga estos pasos:

1. Utilice la herramienta administrativa Active Directory (R) para crear una cuenta de usuario para el sistema iSeries (seleccione la carpeta **Usuarios**, pulse el botón derecho, seleccione **Nuevo**, a continuación seleccione **Usuario**). Especifique iSeriesA como el usuario de Active Directory.
2. Acceda a las propiedades del usuario de Active Directory iSeriesA. Desde la ficha **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá al sujeto de servicio iSeries-A acceder a otros servicios en nombre de un usuario registrado.
3. Correlacione la cuenta de usuario con el sujeto utilizando el mandato **ktpass**. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows (R) 2000 Server. Para correlacionar la cuenta de usuario, entre:

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   donde `iseriesa123` es la contraseña que especificó cuando configuró (Ver 15) el servicio de autenticación de red. **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.

Paso 4: Crear un directorio de inicio para usuarios en el iSeries-A

Todos los usuarios que se conectarán al iSeries y a las aplicaciones del iSeries necesitan un directorio en el directorio /home. Este directorio contendrá el nombre de la antememoria de credenciales Kerberos del usuario. Para crear un directorio de inicio para un usuario, siga estos pasos:

1. En un línea de mandatos iSeries, entre

   ```
   CRTDIR '/home/nombre_usuario'
   ```

   donde `nombre_usuario` es el nombre de usuario del iSeries para el usuario.
   Por ejemplo, el administrador de MyCo ha entrado:
   `CRTDIR '/home/Johns'` para el usuario John Smith.
2. Repita estos pasos para todos sus usuarios.

Paso 5: Verificar la información de dominio TCP/IP para iSeries-A

1. En un línea de mandatos iSeries, entre

   ```
   CFGTCP
   ```
2. Seleccione la Opción 10 (Trabajar con entradas de tabla de sistemas principales TCP/IP).
3. En el campo del nombre de sistema principal, verifique que el nombre de sistema principal totalmente calificado para iSeries-A está en minúsculas. Verifique también que el nombre de sistema principal totalmente calificado aparece en primer lugar si hay varias entradas de nombre de sistema principal. Por ejemplo, iSeries A debe tener la entrada de nombre de sistema principal: iseriesa.ordept.myco.com.
4. Una vez haya verificado la entrada de nombre de sistema principal, pulse F3 para regresar al menú principal de Configurar TCP/IP.
5. Seleccione la Opción 12 (Cambiar información de dominio TCP/IP).
6. Verifique que el nombre del sistema aparece en el campo del nombre de sistema principal. Verifique también que el nombre de dominio es correcto. En este ejemplo, el nombre de sistema principal puede ser `iseriesa` y el nombre de dominio puede ser `ordept.myco.com` .

Paso 6: Comprobar el servicio de autenticación de red en iSeries-A

Ahora puede comprobar que ha configurado el servicio de autenticación de red correctamente solicitando un ticket de otorgación de tickets para el nombre de sujeto del iSeries-A:

1. En una línea de mandatos, entre `QSH` para iniciar el Intérprete de Qshell.
2. Entre `lista de tabla de claves` para visualizar una lista de los sujetos registrados en el archivo de claves. En este escenario, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM debe aparecer como el nombre de sujeto para iSeries-A. **Nota:** si decide configurar sujetos para LDAP e iSeries NetServer, aparecerán otras entradas en el archivo de claves. En este escenario, el administrador ha decidido no configurar sujetos para estos servicios.
3. Entre `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`. Si tiene éxito, el mandato QSH se visualizará sin errores.
4. Entre `klist` para verificar que el sujeto por omisión es krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.

Escenario: habilitar el inicio de sesión único

Situación

Usted es un administrador de red que se encarga de la administración de la red del departamento de entrada de pedidos de su empresa. Actualmente, sus usuarios tienen ordenadores que utilizan Windows (R) 2000. Necesitan administrar sus ID y contraseñas de Windows y sus nombres de usuario de OS/400. Desea poder utilizar el inicio de sesión de Windows (R) 2000 para la autenticación en el iSeries. No quiere que los ID de Windows (R) 2000 y los nombres de usuario de OS/400 sean los mismos, tampoco desea utilizar la copia en antememoria de contraseñas o la sincronización de contraseñas debido a los problemas de seguridad que presentan estas soluciones. Ha oído que el servidor iSeries puede permitir el inicio de sesión único configurando el servicio de autenticación de red y EIM (Enterprise Identity Mapping) en su servidor. Mientras que el servicio de autenticación de red permite a un sistema iSeries participar en

un dominio Windows (R) 2000, EIM proporciona un mecanismo para asociar los ID de Windows (R) 2000 a un identificador EIM único que representa a ese usuario en la empresa. Debido a estas asociaciones, los sujetos Kerberos de la red pueden a acceder a algunas de las aplicaciones del iSeries sin que sea necesario que se registren con su nombre de usuario y contraseña de iSeries. Para obtener más detalles sobre las ventajas de utilizar el inicio de sesión único y el funcionamiento conjunto de EIM y el servicio de autenticación de red, consulte el tema Habilitación del inicio de sesión único.

Ventajas del escenario

Este escenario tiene las siguientes ventajas:

- Simplifica el proceso de autenticación de usuarios
- Reduce los costos operativos de gestionar el acceso a los servidores de la red
- Minimiza la amenaza de robo de contraseñas
- Evita inicios de sesión múltiples
- Simplifica la administración de las identidades de los usuarios en la red

Objetivos

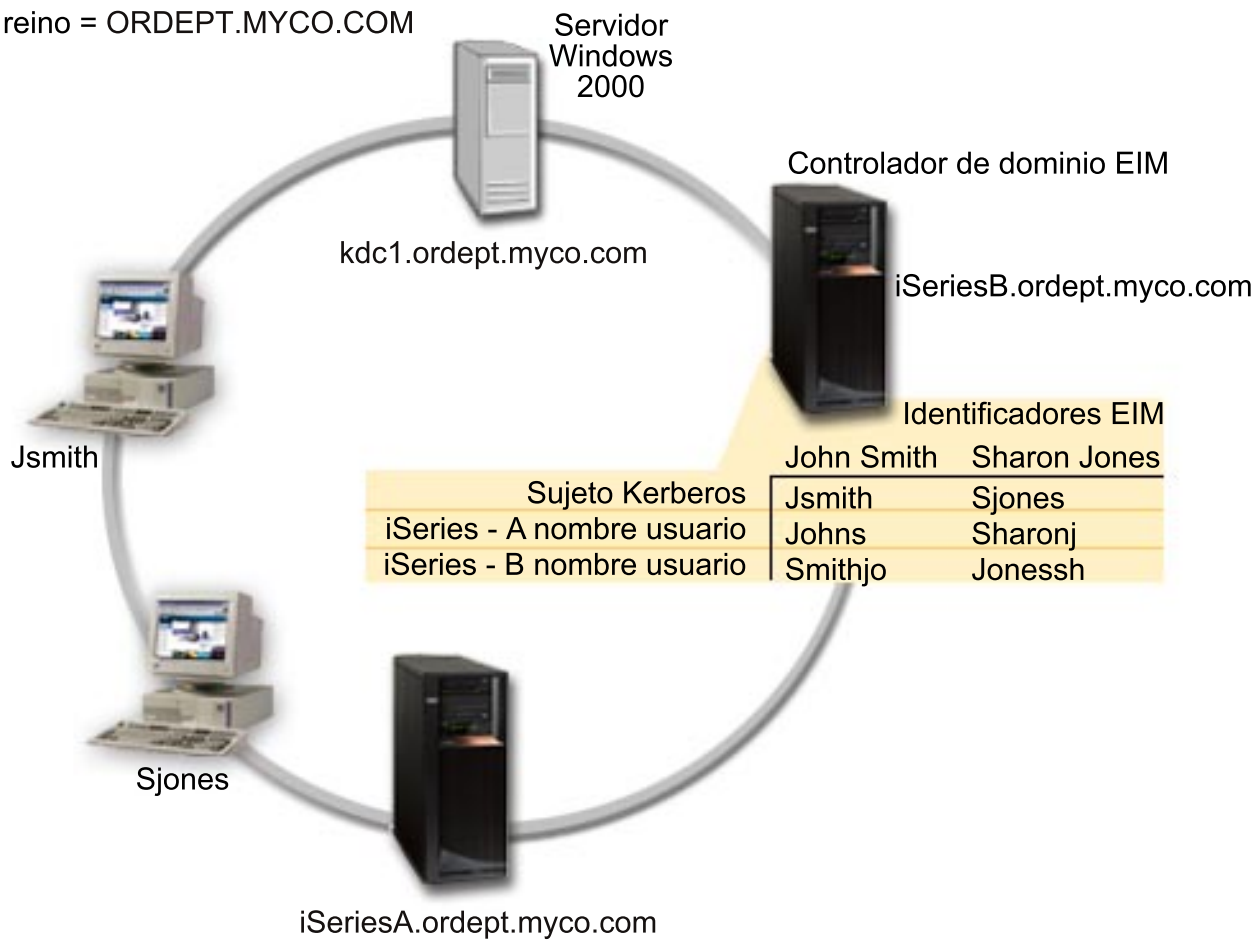
En este escenario, MyCo, Inc. desea añadir un sistema iSeries a un dominio Windows (R) 2000 existente para la autenticación. Los sistemas iSeries contienen varias aplicaciones a las que necesitan acceder los usuarios. Para poder acceder a estas aplicaciones, el KDC debe autenticar a los usuarios. El sujeto de servicio del iSeries debe añadirse al KDC del servidor Windows (R) 2000 para que los sujetos puedan solicitar tickets de servicio. Además, se configurará EIM y posteriormente se crearán asociaciones para correlacionar los perfiles de usuarios de OS/400 y los sujetos Kerberos a un identificador EIM que representa a un solo usuario en la empresa. Puesto que los usuarios del departamento de entrada de pedidos utilizan aplicaciones de iSeries Access for Windows, ha decidido utilizar un sujeto Kerberos como el método de autenticación preferente para iSeries Access for Windows y sus aplicaciones relacionadas.

Los objetivos de este escenario son los siguientes:

- Permitir a iSeries-A e iSeries-B participar con un centro de distribución de claves existente
- Configurar el Servidor de directorios del iSeries-B de forma que funcione como el controlador de dominios EIM para el dominio
- Permitir perfiles de usuario en el iSeries-A y el iSeries-B y correlacionar los sujetos Kerberos a un solo identificador de EIM
- Utilizar el sujeto Kerberos en la autenticación para las aplicaciones de iSeries Access for Windows.

Detalles del escenario

La imagen siguiente ilustra las características de la red de MyCo.



Departamento de entrada de pedidos

- El iSeries-A y el iSeries-B se ejecutan en OS/400 Versión 5 Release 2 (V5R2) y contienen varias aplicaciones empresariales.
- El nombre del KDC es `kdc1.ordept.myco.com`.
- El nombre de sujeto del iSeries-A es `krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`.
- El nombre de DNS del iSeries-A es `iSeriesA.ordept.myco.com`.
- El reino por omisión para el KDC es `ORDEPT.MYCO.COM`.
- El servidor de directorios (LDAP) del iSeries-B se configurará de forma que actúe como el controlador de dominios EIM para la red. **Nota:** antes de configurar EIM, debe configurarse LDAP; sin embargo , el asistente de configuración de EIM facilita la configuración de LDAP si no está configurado en el sistema. En este escenario, no se ha configurado el LDAP para el iSeries-B. El administrador tiene la intención de configurar el LDAP durante la configuración de EIM.
- El nombre de DNS del iSeries-B es `iSeriesB.ordept.myco.com`.
- El nombre de sujeto del iSeries-B es `krbsvr400/iSeriesB.ordept.myco.com@ORDEPT.MYCO.COM`.
- Los PC cliente se ejecutan en Windows (R) 2000.
- Los sujetos Kerberos Jsmith y Sjones se han registrado en el KDC.

Pasos de configuración para este escenario

1. Completar (Ver 20) las hojas de trabajo de planificación para el iSeries-A y el iSeries-B.
2. Configurar (Ver 22) el servicio de autenticación de red en el iSeries-A
3. Añadir (Ver 22) sujetos de servicio del iSeries-A al KDC

4. Crear (Ver 23) un directorio de inicio para cada usuario en el iSeries-A
5. Verificar (Ver 23) la información de dominio TCP/IP para iSeries-A
6. Comprobar (Ver 24) la configuración del servicio de autenticación de red en el iSeries-A
7. Repita los pasos 2-6 en el iSeries-B
8. Configurar (Ver 24) el dominio EIM y configurar el servidor de directorios en el iSeries-B de forma que actúe como el controlador de dominios EIM
9. Configurar (Ver 25) el iSeries-A para participar en el dominio EIM
10. Crear (Ver 25) identificadores de EIM para los usuarios de la empresa
11. Añadir (Ver 26) asociaciones de EIM para los nombres de sujeto y los perfiles de usuario del OS/400 al identificador de EIM

12. Configurar (Ver 27) las conexiones de iSeries Access for Windows de forma que utilicen los sujetos Kerberos como método de autenticación
13. Verificar (Ver 27) la configuración del servicio de autenticación de red y EIM

Detalles de configuración

Paso 1:Completar las hojas de trabajo de planificación

Las siguientes listas de comprobación de planificación ilustran el tipo de información que necesita antes de empezar a configurar el servicio de autenticación de red y EIM. Para poder seguir con la configuración del servicio de autenticación de red, debe poder responder afirmativamente a todas las preguntas de la lista de comprobación de requisitos previos y debe conocer la información para la configuración de la autenticación de red.

Lista de comprobación de requisitos previos	**Respuestas**
¿Su OS/400 es de la versión V5R2 (5722-SS1) o posterior?	Sí
¿Ha instalado el Proveedor de acceso de cifrado (5722-AC3) en sus sistemas iSeries?	Sí
¿Ha instalado iSeries Access for Windows (5722-XE1) en todos los PC de la red y en sus sistemas iSeries?	Sí
¿Ha instalado el subcomponente de Seguridad del Navigator de iSeries en todos los PC de la red y en sus sistemas iSeries?	Sí
¿Ha instalado el subcomponente de Red del Navigator de iSeries en todos los PC de la red y sus sistemas iSeries?	Sí
¿Tiene las autorizaciones especiales: *SECADM, *ALLOBJ y *IOSYSCFG?	Sí

¿Tiene alguno de los siguientes sistemas actuando como el centro de distribución de claves? ¿Cuál? 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	Sí Windows (R) 2000 Server
Para Windows (R) 2000 Server y Windows (R) XP Server, ¿Ha instalado las Herramientas de soporte de Windows que proporcionan la herramienta ktpass?	Sí
¿Están todos los PC de la red configurados en un dominio Windows (R) 2000?	Sí
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	Sí
¿Entre la hora del sistema del iSeries y la hora del sistema del KDC no hay más de cinco minutos de diferencia? Si la diferencia es superior, consulte Sincronizar las horas de los sistemas.	Sí

Necesita esta información para configurar el servicio de autenticación de red	**Respuestas**
¿Cuál es el nombre del reino por omisión Kerberos al que pertenecerá el iSeries?	ORDEPT.MYCO.COM
¿Cuál es el KDC para este reino Kerberos por omisión? ¿Cuál es el puerto de escucha del KDC?	kdc1.ordept.myco.com 88 (**Nota:** este es el puerto por omisión para el KDC).
¿Desea configurar un servidor de contraseñas para este reino por omisión? En caso afirmativo, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este KDC? ¿Cuál es el puerto de escucha del servidor de contraseñas?	Sí kdc1.ordept.myco.com 464 (**Nota:** este es el puerto por omisión para el servidor de contraseñas).
¿Cuál es la contraseña para los sujetos de servicio del iSeries?	iseriesa123 iseriesb345 **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.
¿Con qué otros reinos interactuará el iSeries?	N/D
¿Cuál es el nombre de sistema principal del centro de distribución de claves, para cada reino?	N/D

Necesita esta información para configurar EIM (Enterprise Identity Mapping)	Respuestas
¿Cuál es el nombre distinguido y la contraseña del administrador de LDAP?	nombre distinguido: cn=administrator contraseña: mycopwd **Nota:** todas las contraseñas que se utilizan en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.
¿Cuál es el nombre del servidor LDAP (Directory Services)?	iSeriesB.ordept.myco.com
¿Cuál es el número de puerto del servidor LDAP (Directory Services)?	389

Paso 2: Configurar el servicio de autenticación de red en el iSeries-A

Utilice la información de las hojas de trabajo para configurar el servicio de autenticación de red en el iSeries-A, completando las tareas siguientes:

1. En el Navigator de iSeries, expanda **iSeries-A —>Seguridad**.
2. Pulse el botón derecho sobre **Servicio de autenticación de red** y seleccione **Configurar** para iniciar el asistente para la configuración. **Nota:** tras configurar el servicio de autenticación de red, esta opción será **Volver a configurar**.
3. Consulte la página de **Bienvenida** donde encontrará información sobre los objetos que crea el asistente. Pulse en **Siguiente**.
4. En la página **Especificar la información del reino**, entre `ORDEPT.MYCO.COM` en el campo **Reino por omisión**. Pulse en **Siguiente**.
5. En la página **Especificar información del KDC**, entre `kdc1.ordept.myco.com` en el campo **KDC** y 88 en el campo **Puerto**. Pulse en **Siguiente**.
6. En la página **Especificar información de la contraseña**, seleccione **Sí**. Entre `kdc1.ordept.myco.com` en el campo **Servidor de contraseñas** y 464 en el campo **Puerto**. Pulse en **Siguiente**. **Nota:** la contraseña debe ser la misma que entró al añadir el sujeto al KDC.
7. En la página **Crear entrada de tabla de claves**, seleccione la **Autenticación de Kerberos del iSeries**. Pulse en **Siguiente**.
8. En la página **Crear entrada de tabla de claves del iSeries**, anote la tabla de claves y el sujeto del iSeries-A. Necesitará el nombre de sujeto cuando lo añada al KDC. Entre y confirme una contraseña. Por ejemplo, el administrador de MyCo ha utilizado la contraseña `iseriesa123`. Esta contraseña será la que se utilice al añadir el iSeries-A al KDC. **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real. Pulse en **Siguiente**.
9. En la página **Resumen**, repase los detalles de configuración del servicio de autenticación de red. Pulse en **Finalizar**.

Ya ha configurado el servicio de autenticación de red en el iSeries-A. El siguiente paso consiste en añadir el nombre de sujeto en el KDC.

Paso 3: Añadir el nombre de sujeto del iSeries-A en el KDC

Para añadir el iSeries al KDC de Windows (R) 2000, utilice la documentación referente a la incorporación de sujetos al KDC. Por convención, el nombre del sistema iSeries puede utilizarse como el nombre de usuario. Añada el siguiente nombre de sujeto al KDC:

krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM

En un servidor Windows (R) 2000, siga estos pasos:

1. Utilice la herramienta administrativa Active Directory (R) para crear una cuenta de usuario para el iSeries-A (seleccione la carpeta **Usuarios**, pulse el botón derecho, seleccione **Nuevo**, y a continuación **Usuario**). Especifique iSeriesA como el usuario de Active Directory.
2. Acceda a las propiedades del usuario de Active Directory iSeriesA. Desde la ficha **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá al sujeto de servicio iSeries-A acceder a otros servicios en nombre de un usuario registrado.
3. Correlacione la cuenta de usuario con el sujeto utilizando el mandato **ktpass**. La herramienta ktpass se facilita en la carpeta **Herramientas de servicio** del CD de instalación de Windows (R) 2000 Server. Para correlacionar la cuenta de usuario, entre:

   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM
   -mapuser iSeriesA -pass iseriesa123
   ```

   donde `iseriesa123` es la contraseña que especificó en el paso 6 cuando configuró (Ver 22) el servicio de autenticación de red. **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.

Paso 4: Crear un directorio de inicio para usuarios en el iSeries-A

Todos los usuarios que se conectarán al iSeries y a las aplicaciones del iSeries necesitan un directorio en el directorio /home. Este directorio contendrá el nombre de la antememoria de credenciales Kerberos del usuario. Para crear un directorio de inicio para un usuario, siga estos pasos:

1. En un línea de mandatos iSeries, entre

   ```
   CRTDIR '/home/nombre_usuario'
   ```

   donde `nombre_usuario` es el nombre de usuario del iSeries para el usuario.
   Por ejemplo, el administrador de MyCo ha entrado:
   `CRTDIR '/home/Johns'` para el usuario John Smith.
2. Repita estos pasos para todos sus usuarios.

Paso 5: Verificar la información de dominio TCP/IP para iSeries A

1. En un línea de mandatos iSeries, entre

   ```
   CFGTCP
   ```

2. Seleccione la Opción 10 (Trabajar con entradas de tabla de sistemas principales TCP/IP).
3. En el campo del nombre de sistema principal, verifique que el nombre de sistema principal totalmente calificado para iSeries A está en minúsculas. Verifique también que el nombre de sistema principal totalmente calificado aparece en primer lugar si hay varias entradas de nombre de sistema principal. Por ejemplo, iSeries A debe tener la entrada de nombre de sistema principal: iseriesa.ordept.myco.com.
4. Una vez haya verificado la entrada de nombre de sistema principal, pulse F3 para regresar al menú principal de Configurar TCP/IP.
5. Seleccione la Opción 12 (Cambiar información de dominio TCP/IP).
6. Verifique que el nombre del sistema aparece en el campo del nombre de sistema principal. Verifique también que el nombre de dominio es correcto. En este ejemplo, el nombre de sistema principal puede ser `iseriesa` y el nombre de dominio puede ser `ordept.myco.com` .

Paso 6: Comprobar el servicio de autenticación de red en iSeries-A

Ahora puede comprobar que ha configurado el servicio de autenticación de red correctamente solicitando un ticket de otorgación de tickets para el nombre de sujeto del iSeries-A:

1. En una línea de mandatos, entre `QSH` para iniciar el Intérprete de Qshell.
2. Entre `lista de tabla de claves` para visualizar una lista de los sujetos registrados en el archivo de claves. En este escenario, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM debe aparecer como el nombre de sujeto para iSeries-A.
3. Entre `kinit -k krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM`. Si tiene éxito, el mandato QSH se visualizará sin errores.
4. Entre `klist` para verificar que el sujeto por omisión es krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.

Paso 7: Repita los pasos 2 y 6 para el iSeries-B.

Paso 8: Configurar EIM y el controlador de dominios EIM en el iSeries-B

Debe configurar un dominio EIM en su red. También es preciso configurar el iSeries-B de forma que actúe como el controlador de dominios EIM para el nuevo dominio EIM. Cuando finalice este paso, habrá completado las tareas siguientes:

- Habrá creado un dominio EIM nuevo.
- Habrá configurado el Servidor de directorios del iSeries-B de forma que funcione como el controlador de dominios EIM.
- Habrá creado registros EIM para el iSeries-B y un registro de usuario Kerberos en el dominio.
- Habrá configurado el iSeries-B para participar en el dominio EIM.

1. En el Navigator de iSeries, expanda **iSeries-B —>Red—>Enterprise Identity Mapping**.
2. Pulse el botón derecho sobre **Configuración** y seleccione **Configurar** para iniciar el asistente de configuración.
3. En la página de **Bienvenida**, seleccione **Crear y unir un dominio nuevo**. Pulse en **Siguiente**.
4. En la página **Configurar servidor de directorios**, en el campo **Puerto** acepte el valor por omisión 389. En el campo **Nombre distinguido**, entre `cn=administrator`. Entre y confirme una contraseña. Esta contraseña se utilizará al acceder a las tareas de administración de dominios EIM. Por ejemplo, el administrador de MyCo, ha entrado `mycopwd` en la contraseña y ha confirmado los campos de contraseña. **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real. Pulse en **Siguiente**.
5. En la página **Especificar dominio**, entre el nombre del dominio. Por ejemplo, el administrador de MyCo, ha entrado `mycoeimDomain` en el campo **Dominio**. **Nota**: el nombre de dominio no puede contener ninguno de los caracteres siguientes: = + < > , # ; \ y *. El campo **Descripción** es opcional. Si lo desea, entre una breve descripción del controlador de dominios. Pulse en **Siguiente**.
6. En la página **Especificar DN padre para dominio**, seleccione **No**. Pulse en **Siguiente**.
7. En la página **Información de registro**, seleccione **OS/400 local** y **Kerberos**. Seleccione **Las identidades de usuario Kerberos distinguen entre mayúsculas/minúsculas**. Pulse en **Siguiente**. Anote los nombres de registro. Necesitará estos nombres de registro cuando cree asociaciones a identificadores EIM. **Nota:** los nombres de registro deben ser únicos para el dominio.

8. En la página **Especificar usuario del sistema EIM**, seleccione el usuario EIM del sistema. Acepte los valores por omisión que aparecen en esta página. Por ejemplo, MyCo tenía la siguiente información en esta página:
   - Tipo de usuario: nombre distinguido y contraseña
   - Nombre distinguido: cn=administrator
   - Contraseña: mycopwd
     Nota: todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.

   Pulse en **Siguiente**.
9. En la página **Resumen**, confirme la información de configuración de EIM. Pulse en **Finalizar**.

Ya ha configurado el servidor de directorios en el iSeries-B como el controlador de dominios EIM para el dominio EIM que acaba de configurarse en la red. Ahora debe especificar el iSeries-A como participante en este dominio EIM.

Ahora debe configurar el iSeries-A para participar en el dominio EIM.

1. En el Navigator de iSeries, expanda **iSeries-A —>Red—>Enterprise Identity Mapping**.
2. Pulse el botón derecho sobre **Configuración** y seleccione **Configurar** para iniciar el asistente de configuración.
3. En la página de **Bienvenida**, seleccione **Unir un dominio existente**. Pulse en **Siguiente**.
4. En la página **Especificar controlador de dominios**, entre el nombre del controlador de dominios. Por ejemplo, el administrador de MyCo ha entrado `iSeriesB.ordept.myco.com` en el campo **nombre del controlador de dominios**. Pulse en **Siguiente**.
5. En la página **Especificar usuario para conexión**, seleccione **Nombre distinguido y contraseña** para el tipo de usuario. Por ejemplo, el administrado de MyCo ha entrado `cn=administrator` en el campo **Nombre distinguido** y `mycopwd` en los campos contraseña y confirmar contraseña. **Nota:** todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real. Pulse en **Siguiente**.
6. En la página **Especificar dominio**, seleccione el nombre del dominio en el que desea participar. Pulse en **Siguiente**. Por ejemplo, el administrador de MyCo ha seleccionado **mycoeimDomain**.
7. En la página **Información de registro**, seleccione **OS/400 local**. Pulse en **Siguiente**. Anote los nombres de registro. Necesitará estos nombres de registro cuando cree asociaciones a identificadores EIM. **Nota:** los nombres de registro deben ser únicos para el dominio.
8. En la página **Especificar usuario del sistema EIM**, seleccione el usuario EIM del sistema. Acepte los valores por omisión que aparecen en esta página. Por ejemplo, MyCo tenía la siguiente información en esta página:
   - Tipo de usuario: nombre distinguido y contraseña
   - Nombre distinguido: cn=administrator
   - Contraseña: mycopwd
     Nota: todas las contraseñas utilizadas en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.

   Pulse en **Siguiente**.
9. En la página **Resumen**, confirme la configuración de EIM. Pulse en **Finalizar**.

Ha configurado el iSeries-A para participar en el dominio.

Ahora debe crear identificadores EIM para cada usuario de la empresa. Un identificador EIM representa a un usuario o entidad en la red. En el caso de MyCo, el administrador ha creado dos identificadores EIM, John Smith y Sharon Jones.

1. En iSeries-B, expanda **Red**—> **Enterprise Identity Mapping**.
2. Pulse el botón derecho sobre **Administración de dominios** y seleccione **Añadir dominio...**
3. En el diálogo **Añadir dominio**, deben visualizarse estos valores por omisión para el dominio EIM de MyCo:
   - Puerto: 389
   - Dominio: mycoeimDomain
   - DN padre: ninguno
   - Controlador de dominios: iSeriesB.ordept.myco.com

   Nota: estos valores por omisión se crearon durante la configuración del controlador de dominios EIM.
4. Pulse en **Aceptar**.
5. La jerarquía del Navigator de iSeries se actualiza con **mycoeimDomain** bajo **Administración de dominios**. Pulse en **mycoeimDomain**. Aparecerá el diálogo **Conectar al controlador de dominios EIM**. Debe conectarse al controlador de dominios EIM antes de poder administrar el dominio.
6. En la página **Conectar al controlador de dominios EIM**, entre el nombre distinguido y la contraseña del administrador del controlador de dominios. Deben coincidir con el nombre distinguido y la contraseña creados durante la configuración del controlador de dominios EIM. Para MyCo, el administrador ha entrado lo siguiente:
   - Nombre distinguido: cn=administrator
   - Contraseña: mycopwd **Nota:** todas las contraseñas que se utilizan en este escenario se incluyen sólo a modo de ejemplo. No deben utilizarse durante la configuración real.
7. Pulse en **Aceptar**.
8. Aparecerán dos carpetas nuevas. Pulse el botón derecho en **Identificadores** y seleccione **Nuevo identificador**.
9. En la página **Nuevo identificador EIM**, entre un identificador en el campo **Identificador**. Repita este paso hasta que todos los usuarios tengan un identificador. MyCo ha añadido los siguientes identificadores:
   - John Smith
   - Sharon Jones
10. Pulse en **Aceptar**.

Ahora que se han creado identificadores EIM únicos para John Smith y Sharon Jones, podemos asociar sus nombres de usuario de OS/400 en iSeries-A e iSeries-B y sus sujetos Kerberos a estos identificadores EIM.

Paso 11: Añadir asociaciones EIM para el nombre de sujeto y los perfiles de usuario del OS/400 al identificador EIM

Para completar esta tareas, el administrador de MyCo ha completado los pasos siguientes:

1. En iSeries-B, expanda **Identificadores**, pulse el botón derecho en **John Smith** y seleccione **Propiedades**. Existirán tres asociaciones para este identificador: el sujeto Kerberos, el perfil de usuario en el iSeries-A y el perfil de usuario para el iSeries-B.
2. Para asociar el sujeto Kerberos con el identificador John Smith:
   a. En la ficha **Asociaciones**, pulse **Añadir**.
   b. En la página **Añadir asociación**, pulse **Examinar** en el campo **Registro** y seleccione `ORDEPT.MYCO.COM`. Éste es el registro de usuario Kerberos que se añadió durante la configuración de EIM.
   c. En el campo **Usuario**, entre `Jsmith`.
   d. En el campo **Tipo de asociación**, seleccione **Origen**.

e. Pulse en **Aceptar**.

3. Para asociar el nombre de usuario del iSeries-A con el identificador John Smith:
   a. En la ficha **Asociaciones**, pulse **Añadir**.
   b. En la página **Añadir asociación**, pulse **Examinar** en el campo **Registro** y seleccione `iSeriesA.ordept.myco.com`. Éste es el registro de usuario del OS/400 para el iSeries-A.
   c. En el campo **Usuario**, entre `Johns`.
   d. En el campo **Tipo de asociación**, seleccione **Destino**.
   e. Pulse en **Aceptar**.
4. Para asociar el nombre de usuario del iSeries-B con el identificador John Smith:
   a. En la ficha **Asociaciones**, pulse **Añadir**.
   b. En la página **Añadir asociación**, pulse **Examinar** en el campo **Registro** y seleccione `iSeriesB.ordept.myco.com`. Éste es el registro de usuario del OS/400 para el iSeries-B.
   c. En el campo **Usuario**, entre `Smithjo`.
   d. En el campo **Tipo de asociación**, seleccione **Destino**.
   e. Pulse en **Aceptar**.
5. Repita los pasos 1-4 para el identificador EIM Sharon Jones.

Ahora debe configurar las aplicaciones iSeries Access for Windows en los PC Jsmith y Sjones de forma que utilicen Kerberos durante la autenticación para el iSeries-A y el iSeries-B.

Desde el PC de Jsmith, configure el iSeries-A y sus aplicaciones de forma que utilicen la autenticación Kerberos completando los pasos siguientes:

1. En el Navigator de iSeries, pulse el botón derecho sobre **iSeries-A** y seleccione **Propiedades**.
2. En la ficha **Conexión**, seleccione **Utilizar nombre de sujeto Kerberos, sin instigación**. Ello permitirá que las conexiones de iSeries Access for Windows utilicen la contraseña y el nombre de sujeto Kerberos para la autenticación.
3. Repita estos pasos para el iSeries-B.
4. Repita estos pasos en el PC de Sjones.

Paso 13: Verificar el servicio de autenticación de red y la configuración de EIM

Ahora ya ha completado todos los pasos de configuración. Para comprobar que el servicio de autenticación de red y EIM se han configurado correctamente, el administrador indicó a Sharon Jones y a John Smith que se conectaran al dominio Windows (R) 2000 iniciando la sesión en sus PC. A continuación les indicó que abrieran el Navigator de iSeries en el iSeries-A. Si no aparece ninguna indicación de inicio de sesión en el iSeries, significa que EIM ha correlacionado satisfactoriamente el sujeto Kerberos con un identificador del dominio. Además de las aplicaciones de iSeries Access for Windows, estas otras aplicaciones dan soporte a la autenticación Kerberos:

- Telnet Server
- iSeries NetServer
- QFileSrv.400
- DRDA (Distributed Relational Database Architecture)

Planificación del servicio de autenticación de red

Para configurar satisfactoriamente el servicio de autenticación de red, debe comprender los requisitos y completar los pasos necesarios de planificación. Este tema proporciona una lista de comprobación de requisitos previos y una hoja de trabajo de planificación que le ayudarán a comprobar que lleva a cabo todos los pasos necesarios. Utilice la lista de comprobación y la hoja de trabajo siguientes para la configuración del servicio de autenticación de red.

Lista de comprobación de requisitos previos	**Respuestas**
¿Su OS/400 es de la versión V5R2 (5722-SS1) o posterior?	
¿Ha instalado el Proveedor de acceso de cifrado (5722-AC3) en sus sistemas iSeries?	
¿Ha instalado iSeries Access for Windows (5722-XE1) en todos los PC de la red y en sus sistemas iSeries?	
¿Ha instalado el subcomponente de Seguridad del Navigator de iSeries en todos los PC de la red y en sus sistemas iSeries?	
¿Ha instalado el subcomponente de Red del Navigator de iSeries en todos los PC de la red y sus sistemas iSeries?	
¿Tiene las autorizaciones especiales: *SECADM, *ALLOBJ y *IOSYSCFG?	
¿Ha instalado alguno de los siguientes programas en el sistema seguro que actuará como un centro de distribución de claves? ¿Cuál? 1. Windows (R) 2000 Server 2. Windows (R) XP Server 3. AIX Server 4. zSeries	
Para Windows (R) 2000 Server y Windows (R) XP Server, ¿Ha instalado en el sistema que se utiliza como el centro de distribución de claves las Herramientas de soporte de Windows que proporcionan la herramienta ktpass?	
¿Están todos los PC de la red configurados en un dominio Windows (R) 2000?	
¿Ha aplicado los arreglos temporales de programa (PTF) más recientes?	
¿Entre la hora del sistema del iSeries y la hora del sistema del KDC no hay más de cinco minutos de diferencia? Si la diferencia es superior, consulte Sincronizar las horas de los sistemas.	

Necesita esta información para configurar el servicio de autenticación de red	**Respuestas**
¿Cuál es el nombre del reino por omisión Kerberos al que pertenecerá el iSeries-A?	
¿Cuál es el KDC para este reino Kerberos por omisión? ¿Cuál es el puerto de escucha del KDC?	
¿Desea configurar un servidor de contraseñas para este reino por omisión? En caso afirmativo, responda a las siguientes preguntas: ¿Cuál es el nombre del servidor de contraseñas para este KDC? ¿Cuál es el puerto de escucha del servidor de contraseñas?	

Necesita esta información para configurar el servicio de autenticación de red	Respuestas
¿Cuál es la contraseña para los sujetos de servicio del iSeries?	
¿Con qué otros reinos interactuará el iSeries?	
Cuál es el nombre de sistema principal del centro de distribución de claves, para cada reino	
¿Qué nombres de sujeto de servicio utilizarán las aplicaciones del iSeries?	

Configuración del servicio de autenticación de red

Antes de configurar el servicio de autenticación de red, deberá haber completado todos los pasos de planificación necesarios. Además, el servicio de autenticación de red asume que usted tiene un centro de distribución de claves (KDC) configurado en un sistema seguro en su red. Actualmente, en el iSeries no existe soporte para el KDC. Microsoft Windows (R) 2000 y Windows (R) XP y z/OS dan soporte a la funcionalidad del KDC. Consulte la documentación apropiada referente a la configuración de Kerberos para el sistema que se utilizará como un KDC.

Es recomendable configurar el KDC antes de configurar el servicio de autenticación de red en el iSeries. Para configurar el servicio de autenticación de red, complete los pasos siguientes:

1. En el Navigator de iSeries, expanda **iSeries-A —>Seguridad**.
2. Pulse el botón derecho sobre **Servicio de autenticación de red** y seleccione **Configurar** para iniciar el asistente para la configuración. **Nota:** tras configurar el servicio de autenticación de red, esta opción será **Volver a configurar**.
3. Consulte la página de **Bienvenida** donde encontrará información sobre los objetos que crea el asistente. Pulse en **Siguiente**.
4. En la página **Especificar la información del reino**, entre el nombre del reino por omisión en el campo **Reino por omisión**. Pulse en **Siguiente**.
5. En la página **Especificar información del KDC**, entre el nombre del centro de distribución de claves para este reino en el campo **KDC** y entre 88 en el campo **Puerto**. Pulse en **Siguiente**.
6. En la página **Especificar información de la contraseña**, seleccione **Sí** o **No** para configurar un servidor de contraseñas. El servidor de contraseñas permite a los sujetos cambiar contraseñas en el KDC. Si selecciona **Sí**, entre el nombre del servidor de contraseñas en el campo **Servidor de contraseñas**. El servidor de contraseñas tiene el puerto por omisión 464. Pulse en **Siguiente**.
7. En la página **Crear entrada de tabla de claves**, seleccione la **Autenticación de Kerberos del iSeries**. Además, también puede crear entradas de tabla de claves para el servidor LDAP y el NetServer del iSeries, si desea que estos servicios utilicen la autenticación de Kerberos. Pulse en **Siguiente**.
8. En la página **Crear entrada de tabla de claves del iSeries**, entre y confirme una contraseña. Pulse en **Siguiente**. **Nota:**se trata de la contraseña que utilizará cuando defina el iSeries para el KDC.
9. En la página **Resumen**, repase los detalles de configuración del servicio de autenticación de red. Pulse en **Finalizar**.

Ya ha configurado el servicio de autenticación de red.

Qué hacer a continuación

Definir el iSeries para el centro de distribución de claves

Tras configurar el servicio de autenticación de red en el iSeries, debe definir el iSeries en el centro de distribución de claves (KDC). El servicio de autenticación de red proporciona un nombre de sujeto iSeries, **krbsvr400**, para el servidor y todas las aplicaciones nativas del iSeries.

Por ejemplo, en nuestros escenarios de configuración, nos hemos referido a un iSeries con el nombre de sistema principal iSeriesA.ordept.myco.com. Para que un cliente obtenga un ticket de servicio para presentar a este iSeries, el sujeto krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM debe definirse para el KDC.

z/OS
Consulte la documentación para el mandato **Kadmin**.

Windows (R) 2000 Server

1. Utilice la herramienta administrativa Active Directory (R) para crear una cuenta de usuario para el iSeries. Especifique un nombre para el iSeries como usuario de Active Directory. Por ejemplo, un nombre válido podría ser iSeriesA.
2. Acceda a las propiedades del usuario de Active Directory que ha creado en el Paso 1. Desde la ficha **Cuenta**, seleccione **Cuenta de confianza para delegación**. Ello permitirá al sujeto de servicio iSeries acceder a otros servicios en nombre de un usuario registrado.
3. Correlacione la cuenta de usuario con el sujeto, utilizando el mandato **ktpass**. Por ejemplo, podría entrar:
   ```
   ktpass -princ krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM -mapuser iSeriesA
   -pass xxxxxx
   ```
   donde `xxxxxx` es la contraseña que ha especificado durante la configuración del servicio de autenticación de red.

Qué hacer a continuación

Crear un directorio de inicio

Crear un directorio de inicio

Tras haber definido el iSeries en el centro de distribución de claves, deberá crear un directorio /home para cada usuario que se conectará al iSeries y a las aplicaciones iSeries. Este directorio contendrá el nombre de la antememoria de credenciales Kerberos del usuario. Para crear un directorio de inicio para un usuario, siga estos pasos:

En un línea de mandatos iSeries, entre

```
CRTDIR '/home/nombre_usuario'
```
donde `nombre_usuario` es el nombre de usuario del iSeries para el usuario.

Qué hacer a continuación:

Verificar la información de dominio TCP/IP

Verificar información de dominio TCP/IP

Tras haber creado un directorio inicial, debe verificar que tiene las entradas de tabla de sistema principal correctas para el servidor.

1. En un línea de mandatos iSeries, entre

   `CFGTCP`
2. Seleccione la Opción 10 (Trabajar con entradas de tabla de sistemas principales TCP/IP).
3. En el campo del nombre de sistema principal, verifique que el nombre de sistema principal totalmente calificado para iSeries A está en minúsculas. Verifique también que el nombre de sistema principal totalmente calificado aparece en primer lugar si hay varias entradas de nombre de sistema principal. Por ejemplo, iSeries A debe tener la entrada de nombre de sistema principal: iseriesa.ordept.myco.com.
4. Una vez haya verificado la entrada de nombre de sistema principal, pulse F3 para regresar al menú principal de Configurar TCP/IP.
5. Seleccione la Opción 12 (Cambiar información de dominio TCP/IP).
6. Verifique que el nombre del sistema aparece en el campo del nombre de sistema principal. Verifique también que el nombre de dominio es correcto. Por ejemplo, el nombre de sistema principal puede ser `iseriesa` y el nombre de dominio puede ser `ordept.myco.com` .

Qué hacer a continuación:

Comprobar la configuración del servicio de autenticación de red

Comprobar la configuración del servicio de autenticación de red

Tras haber verificado la información de dominio correcta, debe comprobar la configuración del servicio de autenticación de red mediante la solicitud de un ticket de otorgación de tickets para el nombre de sujeto de iSeries:

1. En una línea de mandatos, entre `QSH` para iniciar el Intérprete de Qshell.
2. Entre `lista de tabla de claves` para visualizar una lista de los sujetos registrados en el archivo de claves. Por ejemplo, un nombre de sujeto válido podría ser krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM.
3. Entre `kinit -k krbsvr400/sistema.dominio@reino`. Por ejemplo, krbsvr400/iSeriesA.ordept.myco.com@ORDEPT.MYCO.COM sería un nombre de sujeto válido para iSeries. Si tiene éxito, el mandato QSH se visualizará sin errores.
4. Entre `klist` para verificar que el sujeto por omisión es krbsvr400/sistema.dominio@reino.

Qué hacer a continuación:

Configurar EIM (Enterprise Identity Mapping)
Este paso es opcional si está utilizando el servicio de autenticación de red con sus propias aplicaciones. Sin embargo, es recomendable para aplicaciones nativas del iSeries para gestionar múltiples identidades de usuario en una red.

Gestión del servicio de autenticación de red

Tras configurar el servicio de autenticación de red, puede solicitar tickets, trabajar con archivos de claves y administrar las relaciones de confianza del reino. También puede trabajar con archivos de credenciales y efectuar copias de seguridad de archivos de configuración. Los siguientes temas describen cómo completar estas tareas:

Tareas del administrador

A continuación se incluye una breve lista de tareas que puede realizar un administrador en el Navigator de iSeries. Para obtener más información relacionada con las tareas, consulte la ayuda del Navigator de iSeries referida al servicio de autenticación de red. Además de estas tareas, los administradores deben asegurarse de que los usuarios eliminan las credenciales antiguas utilizando el mandato kdestroy.

- Sincronizar las horas de los sistemas
  Para intercambiar tickets entre un iSeries y un KDC, las horas del sistema no deben discrepar en más de cinco minutos. Puede configurar la diferencia horaria máxima desde las propiedades del servicio de autenticación de red. La diferencia horaria máxima por omisión es de 5 minutos o 300 segundos. En este tema se describe cómo sincronizar las horas entre sistemas.
- Añadir reinos
  Este tema describe cómo puede añadir un reino nuevo a la configuración del servicio de autenticación de red.
- Suprimir reinos
  Este tema describe cómo puede eliminar reinos de la configuración del servicio de autenticación de red.
- Añadir un centro de distribución de claves a un reino
  Este tema describe cómo puede añadir un centro de distribución de claves a la configuración actual del servicio de autenticación de red.
- Añadir servidor de contraseñas
  Este tema describe cómo añadir un servidor de contraseñas a la configuración del servicio de autenticación de red de forma que los usuarios puedan cambiar sus contraseñas Kerberos.
- Crear una relación de confianza entre reinos
  Este tema describe cómo crear una relación de confianza entre reinos. Esta función es opcional porque, por omisión, el protocolo Kerberos buscará la confianza en la jerarquía de reinos. Sin embargo, esta función resulta útil si tiene reinos en dominios diferentes y desearía acelerar este proceso.
- Modificar la resolución del sistema principal
  Este tema describe cómo cambiar la resolución del sistema principal para nombres de reino.

- Añadir valores de cifrado
  Este tema describe cómo añadir tipos de cifrado para los tickets de otorgación de tickets (TGT) y el servicio de otorgación de tickets (TGS).

Tareas del usuario de iSeries

El iSeries también puede operar como cliente en una red en la que se ha habilitado el protocolo Kerberos. Los usuarios pueden entrar en el iSeries y efectuar tareas relacionadas con Kerberos mediante el Intérprete de Qshell. Las siguientes tareas utilizan varios mandatos Qshell para realizar tareas habituales para los usuarios de iSeries.

- Crear un directorio de inicio
  Este tema describe cómo crear un directorio de inicio.
-
- Obtención de tickets nuevos de otorgación de tickets
  Este tema describe cómo obtener o renovar un ticket de otorgación de tickets con el mandato Qshell **kinit**.
-
- Cambiar las contraseñas de Kerberos
  Este tema describe cómo cambiar las contraseñas con el mandato Qshell **kpasswd**.
-
- Gestionar archivos de claves
  Este tema describe cómo gestionar archivos de claves con el mandato Qshell **keytab**.
-
- Suprimir las antememorias de credenciales que han caducado
  Este tema describe cómo suprimir las antememorias de credenciales que han caducado guardadas en el cliente con el mandato Qshell **kdestroy**. Es importante que los usuarios supriman periódicamente su antememoria de credenciales.
-
- Visualizar antememoria de credenciales o archivo de claves
  Este tema describe cómo mostrar en forma de lista credenciales y archivos de claves asociados con un usuario con el mandato Qshell **klist**.
-
- Gestionar entradas de servicio Kerberos en directorios LDAP
  Este tema describe cómo gestionar las entradas de servicio Kerberos en los directorios LDAP con el mandato Qshell **ksetup**.

Sincronizar las horas de los sistemas

El servicio de autenticación de red utiliza 5 minutos (300 segundos) como el valor por omisión para el período máximo de tiempo en que pueden discrepar las horas de los sistemas. Puede cambiar la diferencia horaria desde las propiedades del servicio de autenticación de red.

Antes de sincronizar las horas de los sistemas, utilice el valor del sistema QUTCOFFSET para establecer la hora del sistema según su zona horaria. Puede sincronizar estas horas del sistema modificando la hora del KDC o utilizar el valor del sistema QTIME para cambiar la hora del sistema del iSeries. Sin embargo, para mantener sincronizados las horas de los sistemas en una red, debe configurar el SNTP (Simple

Network Time Protocol). El SNTP permite a múltiples sistemas basar su hora en un sólo servidor horario. Para configurar el SNTP, complete los siguientes pasos:

Para configurar el SNTP en un iSeries, entre `CHGNTPA` en una línea de mandatos.

Para configurar el SNTP en sistemas Windows (R), utilice **NET HELP TIME** para visualizar información de configuración para un servidor SNTP.

Añadir reinos

Como administrador de redes, quizás desee añadir un reino nuevo a la configuración del servicio de autenticación de red. Antes de poder añadir un reino a la configuración del iSeries, deberá configurarse el KDC para el reino nuevo. Para poder añadir un reino a la tarea del servicio de autenticación de red del iSeries, necesita el nombre del reino, el nombre del KDC y el puerto de escucha del KDC.

Para añadir un reino al servicio de autenticación de red, siga estos pasos:

1. En el Navigator de iSeries, seleccione **Su servidor iSeries** —> **Seguridad** —> **Servicio de autenticación de red**.
2. Pulse el botón derecho sobre **Reinos** y seleccione **Añadir reino**.
3. En el campo **Reino a añadir**, entre el nombre de sistema principal del reino que desea añadir. Por ejemplo, un nombre de reino válido podría ser: ORDEPT.MYCO.COM.
4. entre el nombre del KDC para el reino que está añadiendo. Por ejemplo, un nombre de KDC válido podría ser: kdc1.ordept.myco.com.
5. Entre el número de puerto en el que el KDC escucha las peticiones. Un número de puerto válido podría ser 1-65535. El puerto por omisión para el KDC es 88.
6. Pulse en **Aceptar**.

Suprimir reinos

Como administrador de redes, quizás desee suprimir un reino de la configuración del servicio de autenticación de red. Los reinos pueden dejar de utilizarse o dejar de ser necesarios en una red. Quizás también necesite eliminar un reino por omisión como recuperación ante algún problema de aplicación nativo de iSeries.

Por ejemplo, si ha configurado el servicio de autenticación de red sin configurar el centro de distribución de claves (KDC) en la red, QFileSvr.400 y DDM (Distributed Data Management) asumirán que está utilizando la autenticación Kerberos. Antes de configurar la autenticación para estos productos, debería suprimir el reino por omisión que ha especificado durante la configuración del servicio de autenticación de red.

Para suprimir un reino para el servicio de autenticación de red, siga los pasos siguientes:

1. En el Navigator de iSeries, expanda **su servidor iSeries** —> **Seguridad** —> **Servicio de autenticación de red** —> **Reinos**.
2. Pulse el botón derecho sobre el nombre del reino que desea suprimir y seleccione **Suprimir**.

3. Pulse en **Aceptar** para confirmar la supresión.

Añadir un centro de distribución de claves a un reino

Como administrador de redes, puede agregar un centro de distribución de claves (KDC) a un reino utilizando el servicio de autenticación de red. Antes de poder añadir el KDC al reino, debe conocer el nombre del KDC y el puerto de escucha.

Para añadir un centro de distribución de claves a un reino, complete estos pasos:

1. En el Navigator de iSeries, expanda **su servidor iSeries** —> **Seguridad** —> **Servicio de autenticación de red** —> **Reinos**.
2. Pulse el botón derecho sobre el nombre del reino del panel de la derecha y seleccione **Propiedades**.
3. En la ficha **General**, entre el nombre del KDC que desea añadir a este reino. El KDC es necesario para todos los reinos. Por ejemplo, kdc2.ordept.myco.com podría ser una entrada válida.
4. Entre el número de puerto en el que el KDC escucha las peticiones. Un número de puerto válido podría ser 1-65535. El puerto por omisión para el KDC es 88.
5. Pulse en **Añadir**. El nuevo KDC aparecerá en la lista **Centro de distribución de claves (KDC) para este reino**.
6. Pulse en **Aceptar**.

Añadir servidor de contraseñas

El servidor de contraseñas permite a los sujetos Kerberos cambiar sus contraseñas. Para añadir un servidor de contraseñas a un reino, complete los pasos siguientes:

1. En el Navigator de iSeries, expanda **su servidor iSeries** —> **Seguridad** —> **Servicio de autenticación de red** —> **Reinos**.
2. Pulse el botón derecho sobre el nombre del reino del panel de la derecha y seleccione **Propiedades**.
3. En la ficha **Servidor de contraseñas**, entre el nombre del servidor de contraseñas. Por ejemplo, un nombre válido para el servidor de contraseñas podría ser: psvr.ordept.myco.com.
4. entre el número del puerto que corresponda al servidor de contraseñas. Un número de puerto válido podría ser 1-65535. El puerto por omisión para el servidor de contraseñas es 464.
5. Pulse en **Añadir**. El nuevo servidor de contraseñas se añadirá a la lista.
6. Pulse en **Aceptar**.

Crear una relación de confianza entre reinos

Al establecer una relación de confianza entre reinos se crea un método abreviado para la autenticación. Esta función es opcional porque, por omisión, el protocolo Kerberos buscará la confianza en la jerarquía de reinos. Esta función resulta útil si tiene reinos en dominios diferentes y desearía acelerar este proceso.

Para configurar la confianza de reinos, los KDC de cada uno de los reinos deben compartir una clave. Para poder crear una relación de confianza, debe configurar los KDC para que confíen entre sí. Para crear una relación de confianza entre reinos, complete los pasos siguientes:

1. En el Navigator de iSeries, expanda **su servidor iSeries** —> **Seguridad** —> **Servicio de autenticación de red** —> **Reino**.
2. Pulse el botón derecho sobre el nombre del reino del panel de la derecha y seleccione **Propiedades**.
3. En la ficha **Reinos de confianza**, entre los nombres de los reinos con los que desea establ ecer una relación de confianza. Por ejemplo, estos podrían ser nombres válidos para la relación de confianza: NY.myco.com and LA.myco.com.
4. Pulse en **Añadir**. De este modo se añadirá la asociación de confianza a la tabla.
5. Pulse en **Aceptar**.

Modificar la resolución del sistema principal

Con el servicio de autenticación de red, puede especificar un servidor LDAP (Directory Services), un DNS (Domain Name System), y correlaciones estáticas que se añaden al archivo de configuración para resolver nombres de sistema principal y nombres de reino. También puede seleccionar los tres métodos para resolver nombres de sistema principal. Si efectivamente selecciona todos estos métodos, el servicio de autenticación de red comprobará en primer lugar el servidor de directorios, a continuación las entradas del DNS y, finalmente, las correlaciones estáticas para resolver los nombres de sistema principal.

Para cambiar la resolución del sistema principal, complete los pasos siguientes:

1. En el Navigator de iSeries, expanda **Su servidor iSeries** —> **Seguridad**.
2. Pulse el botón derecho sobre **Servicio de autenticación de red** y seleccione **Propiedades**.
3. En la página **Resolución del sistema principal**, seleccione **Utilizar búsqueda de LDAP**, **Utilizar búsqueda de DNS**, y/o **Utilizar correlaciones estáticas**.
4. Si selecciona **Utilizar búsqueda de LDAP** como el tipo de resolución del sistema principal, entre el nombre del servidor de directorios y el puerto correspondiente. Por ejemplo, ldapsrv.ordept.myco.com podría ser un nombre válido para el servidor de directorios. Un número de puerto válido podría ser 1-65535. El puerto por omisión para el servidor de directorios es 389.
5. Si selecciona **Utilizar búsqueda de DNS** como el tipo de resolución del sistema principal, debe haber configurado el DNS para la correlación con nombres de reino.
6. Si selecciona **Utilizar correlaciones estáticas** como el tipo de resolución del sistema principal, entre el nombre de reino y su correspondiente nombre DNS. Por ejemplo, el nombre del sistema principal podría ser mypc.mycompanylan.com y el nombre de reino es ORDEPT.MYCO.COM. También puede correlacionar nombres de sistema principal genéricos con un reino específico. Por ejemplo, si todas las máquinas que acaban en myco.lan.com forman parte de ORDEPT.MYCO.COM, podría entrar `myco.lan.com` como el nombre de DNS y ORDEPT.MYCO.COM como el reino. Ello crea una asociación entre el nombre de reino y el nombre DNS en el archivo de configuración. Pulse en **Añadir** para crear una correlación estática entre el nombre de reino y DNS en el archivo de configuración.
7. Tras entrar la información pertinente para el tipo de resolución del sistema principal seleccionado, pulse en **Aceptar**.

Añadir valores de cifrado

Puede seleccionar los tipos de cifrado para tickets de otorgación de tickets (TGT) y servicios de otorgación de tickets (TGS). El cifrado oculta los datos que fluyen en una red logrando que no sean identificables. Un cliente cifraría los datos y el servidor los descrifraría. Para asegurarse de que el cifrado funciona correctamente, debe utilizar el mismo tipo de cifrado que se especifica en KDC o la otra aplicación de comunicación. Si estos tipos de cifrado no concuerda, el cifrado fallará. Puede añadir valores de cifrado TGT y TGS. **Nota:** los valores de cifrado por omisión para el TGT y el TGS son des-cbc-crc y des-cbc-md5. Durante la configuración se establecen valores de cifrado por omisión. Puede añadir a la configuración otros valores de cifrado para tickets completando estos pasos:

1. En el Navigator de iSeries, expanda **Su servidor iSeries** —> **Seguridad**.
2. Pulse el botón derecho sobre **Servicio de autenticación de red** y seleccione **Propiedades**.
3. En la página **Tickets**, seleccione el valor de cifrado de la lista de tipos de cifrado disponibles del ticket de otorgación de tickets o del servicio de otorgación de tickets.
4. Pulse en **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 en que aparecen en la lista. Si falla un tipo de cifrado, se intenta el siguiente de la lista.
5. Pulse en **Aceptar**.

Obtención o renovación de tickets de otorgación de tickets

El mandato **kinit** obtiene o renueva un ticket de otorgación de tickets Kerberos. Si no se especifican opciones de ticket en el mandato **kinit**, se utilizan las opciones del centro de distribución de claves (KDC) especificadas en el archivo de configuración de Kerberos.

Si no se está renovando un ticket existente, la antememoria de credenciales se reinicializa y contiene el nuevo ticket que otorga tickets recibido del KDC. Si en la línea de mandatos no se ha especificado el nombre del sujeto, dicho nombre se obtiene de la antememoria de credenciales. La nueva antememoria de credenciales se convierte en la antememoria de credenciales por omisión a menos que la opción `-c` especifique el nombre de la antememoria.

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 sólo se especifica un número, el valor por omisión son las horas.

Para obtener un ticket que otorga tickets que tenga una vida de 5 horas para el sujeto Jsmith:

en la línea de mandatos Qshell, entre:

```
kinit -l 5h Jsmith
```

O

en un línea de mandatos iSeries, entre

```
call qsys/qkrbkinit parm('-l' '5h' 'Jsmith')
```

Consulte las notas de empleo sobre este mandato Qshell, donde encontrará detalles sobre su utilización y las restricciones.

kinit

Sintaxis

```
kinit [-r tiempo] [-R] [-p] [-f] [-A] [-l tiempo] [-c antememoria] [-k] [-t tabla de
claves] [sujeto]
```

Autorización pública por omisión: *USE

El mandato Qshell **kinit** obtiene o renueva el ticket de otorgación de tickets Kerberos.

Opciones

-r tiempo
El intervalo de tiempo para renovar un ticket. El ticket no puede renovarse tras la expiración de este intervalo. El tiempo de renovación debe ser superior al tiempo final. Si no se ha especificado esta opción, el ticket no puede renovarse (todavía es posible generar un ticket renovable si la vida del ticket solicitado supera la vida máxima del ticket).

-R
Debe renovarse un ticket existente. Cuando se renueva un ticket existente, no 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 puede enviarse. Si no especifica esta opción, el ticket no puede enviarse.

-A
El ticket no incluirá una lista de direcciones de cliente. Si no especifica esta opción, el ticket incluirá la lista de direcciones del sistema principal local. Cuando un ticket inicial contiene una lista de direcciones, puede utilizarse sólo desde una de las direcciones de la lista de direcciones.

-l tiempo

El intervalo de tiempo final del ticket. El ticket no puede utilizarse tras la expiración del intervalo a menos que se haya renovado. Si no especifica esta opción, el intervalo se establece en 10 horas.

-c antememoria
El nombre de la antememoria de credenciales que utilizará el mandato kinit. Si no especifica esta opción, el mandato utilizará la antememoria de credenciales por omisión.

-k
La clave del sujeto del ticket debe obtenerse a partir de la tabla de claves. Si no especifica esta opción, el sistema le solicitará que especifique la contraseña para el sujeto del ticket.

-t tabla de claves
El nombre de la tabla de claves. Si no especifica esta opción pero especifica la opción `-k`, el sistema utiliza la tabla de claves por omisión. La opción `-t` supone la opción `-k`.

sujeto
El sujeto del ticket. Si no especifica el sujeto en la línea de mandatos, el sistema obtiene el sujeto de la antememoria de credenciales.

Autorizaciones

Objeto referido a	Autorización necesaria
Todos los directorios en el nombre de la vía de acceso que precede al archivo de claves si se ha especificado la opción `-t`	*X
Archivo de claves cuando se ha especificado `-t`	*R
Todos los directorios en el nombre de la vía de acceso que precede al archivo de la antememoria de credenciales que se debe utilizar.	*X
Directorio padre del archivo de antememoria que se debe utilizar, si se ha especificado mediante la variable de entorno **KRB5CCNAME** y se está creando el archivo.	*WX
Archivo de la antememoria de credenciales	*RW
Todos los directorios en las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Para permitir que el tiempo de proceso Kerberos encuentre su archivo de la antememoria de credenciales desde cualquier proceso en ejecución, el nombre del archivo de la antememoria normalmente se almacena en el directorio de inicio en un archivo denominado **krb5ccname**. La ubicación de almacenamiento del nombre del archivo de antememoria puede alterarse temporalmente estableciendo la variable de entorno **_EUV_SEC_KRB5CCNAME_FILE**. Para acceder a este archivo, el perfil de usuario debe tener la autorización ***X** para cada directorio en la vía de acceso y la autorización ***R** para el archivo en el que se almacena el nombre del archivo de la antememoria. La primera vez que un usuario crea una antememoria de credenciales, el perfil de usuario debe tener autorización ***WX** para el directorio padre.

Mensajes

- La opción `nombre_opción` necesita un valor.
- `opción_mandato` no es una opción de mandato válida.
- No se permiten opciones durante la renovación o validación de un ticket.
- No se ha podido obtener el nombre de la antememoria de credenciales por omisión.

- No se ha podido resolver la antememoria de credenciales `nombre_archivo`.
- No existe ningún ticket inicial disponible.
- Debe especificarse el nombre del sujeto.
- No se ha podido recuperar el ticket de la antememoria de credenciales `nombre_archivo`.
- El ticket inicial no es renovable.
- La opción `valor_opción` no es válida para la petición `nombre_petición`.
- No se han podido obtener credenciales iniciales.
- No se ha podido analizar el nombre de sujeto.
- No se ha podido resolver la tabla de claves `nombre_archivo`.
- La contraseña no es correcta para `nombre_sujeto`.
- No se ha podido leer la contraseña.
- No se han podido almacenar las credenciales iniciales en la antememoria de credenciales `nombre_archivo`.
- El valor de incremento de tiempo no es válido.

Para obtener un ejemplo de cómo se utiliza este mandato, consulte Obtención o renovación de un ticket de otorgación de tickets.

Visualizar antememoria de credenciales o archivo de claves

El mandato **klist** muestra el contenido de una tabla de claves o antememoria de credenciales Kerberos.

Para mostrar en forma de lista todas las entradas en su antememoria de credenciales por omisión y mostrar los indicadores del boleto:

En un línea de mandatos Qshell, entre

```
klist -f -a
```

O

En un línea de mandatos iSeries, entre

```
call qsys/krbklist parm('-f' '-a')
```

Consulte las notas de empleo sobre este mandato Qshell, donde encontrará detalles sobre su utilización y las restricciones.

klist

Sintaxis

```
klist [-a] [-e] [-c] [-f] [-s] [-k] [-t] [-K] [nombre de archivo]
```
Autorización pública por omisión: *USE

El mandato Qshell **klist** muestra el contenido de una tabla de claves o antememoria de credenciales Kerberos.

Opciones

-a
Muestra todos los tickets de la antememoria de credenciales, inclusive los tickets que han expirado. Si no especifica esta opción, los tickets que han expirado no se incluyen en la lista. Esta opción es válida sólo cuando enumera una antememoria de credenciales.

-e
Muestra la clase de cifrado para el ticket y la clave de la sesión. Esta opción es válida sólo cuando enumera una antememoria de credenciales.

-c
Muestra en modo de lista los tickets de una antememoria de credenciales. Si no se ha especificado la opción `-c` ni la opción `-k`, éste es el valor por omisión. Esta opción es mutuamente excluyente con la opción `-k`.

-f
Muestra los indicadores del ticket, utilizando las siguientes abreviaciones:

Abreviación	Significado
F	Puede enviarse el ticket
f	Ticket enviado
P	El ticket puede ser un proxy
p	Ticket proxy
D	Puede cambiarse la fecha del ticket a una fecha posterior
d	Ticket con fecha posterior
R	Ticket renovable
I	Ticket inicial
i	Ticket no válido
A	Preautenticación utilizada
O	El servidor puede ser un delegado
C	Lista de tránsito verificada por el KDC

Esta opción es válida sólo cuando enumera una antememoria de credenciales.

-s
Suprime la salida de mandatos, pero establece el estado de salida en 0 si se encuentra un ticket de otorgación de tickets válido en la antememoria de credenciales. Esta opción es válida sólo cuando enumera una antememoria de credenciales.

-k
Muestra las entradas de una tabla de claves en forma de lista. Esta opción es mutuamente excluyente con la opción **-c**.

-t
Muestra las indicaciones de la hora para las entradas de la tabla de claves. Esta opción sólo es válida cuando enumera una tabla de claves.

-K
Muestra el valor de la clave de cifrado para cada entrada de la tabla de claves. Esta opción sólo es válida cuando enumera una tabla de claves.

nombre de archivo
Especifica el nombre de la antememoria de credenciales o tabla de claves. Si no se especifica ningún nombre de archivo, se utiliza la tabla de claves o la antememoria de credenciales por omisión.

Autorizaciones

Objeto referido a	Autorización necesaria
Todos los directorios en el nombre de la vía de acceso que precede al archivo si se ha especificado la opción `-k` como tabla de claves	*X
Archivo de claves cuando se ha especificado `-k`	*R
Todos los directorios en el nombre de la vía de acceso que precede al archivo de la antememoria de credenciales si no se ha especificado la opción `-k`	*X
Archivo de la antememoria de credenciales si no se ha especificado la opción `-k`	*R

Para permitir que el tiempo de proceso Kerberos encuentre su archivo de la antememoria de credenciales desde cualquier proceso en ejecución, el nombre del archivo de la antememoria normalmente se almacena en el directorio de inicio en un archivo denominado **krb5ccname**. La ubicación de almacenamiento del nombre del archivo de antememoria puede alterarse temporalmente estableciendo la variable de entorno **_EUV_SEC_KRB5CCNAME_FILE**. Para acceder a este archivo, el perfil de usuario debe tener la autorización ***X** para cada directorio en la vía de acceso y la autorización ***R** para el archivo en el que se almacena el nombre del archivo de la antememoria. La primera vez que un usuario crea una antememoria de credenciales, el perfil de usuario debe tener autorización ***WX** para el directorio padre.

Mensajes

- La opción `nombre_opción` requiere un valor.
- `opción_mandato` no es una opción de mandato válida.
- Las opciones `opción_mandato_uno` y `opción_mandato_dos` no pueden especificarse juntas.
- No se ha encontrado una antememoria de credenciales por omisión.
- No se ha podido resolver la antememoria de credenciales `nombre_archivo`.
- No se ha podido recuperar el nombre del sujeto de la antememoria de credenciales `nombre_archivo`.
- No se ha podido recuperar el ticket de la antememoria de credenciales `nombre_archivo`.
- No se ha podido descodificar el ticket.
- No se ha encontrado la tabla de claves por omisión.
- No se ha podido resolver la tabla de claves `nombre_archivo`.

Para obtener un ejemplo de cómo se utiliza este mandato, consulte Visualizar la antememoria de credenciales o el archivo de claves.

Gestionar archivos de claves

El mandato Keytab se utiliza para añadir o suprimir una clave de una tabla de claves o para visualizar las entradas de una tabla de claves.

Por ejemplo, para añadir una clave para el sujeto de servicio krbsvr400 en el sistema principal kdc1.ordept.myco.com, en el reino ORDEPT.MYCO.COM:

en un línea de mandatos Qshell, entre

```
keytab add krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM
```

O

en un línea de mandatos iSeries, entre

```
call qsys/qkrbkeytab parm('add' 'krbsvr400/kdc1.ordept.myco.com@ORDEPT.MYCO.COM')
```

El sistema le solicitará la contraseña utilizada cuando se definió el servicio en el KDC.

Consulte las notas de empleo sobre este mandato Qshell, donde encontrará detalles sobre su utilización y las restricciones.

keytab

Sintaxis

```
keytab add sujeto [-p contraseña] [-v versión] [-k tabla de claves] keytab delete sujeto
[-v versión] [-k tabla de claves] keytab list [sujeto] [-k tabla de claves]
```
Autorización pública por omisión: *USE

El mandato Qshell **keytab** manipula una tabla de claves.

Opciones

-k
El nombre de la tabla de claves. Si no se ha especificado esta opción, se utiliza la tabla de claves por omisión.

-p
Especificar la contraseña. Si no se especifica esta opción, se solicita a los usuarios que entren la contraseña cuando añadan una entrada a la tabla de claves.

-v
El número de la versión de clave. Si no se ha especificado esta opción, cuando se añade una clave se asigna el siguiente número de versión. Si no se ha especificado esta opción, cuando se suprime una clave se suprimen todas las claves del sujeto.

sujeto
El nombre del sujeto. Si no se ha especificado esta opción, cuando enumera la tabla de claves se muestran todos los sujetos.

Autorizaciones

Objeto referido a	Autorización necesaria
Todos los directorios en el nombre de la vía de acceso que precede al archivo de claves objetivo que se debe abrir.	*X
Directorio padre del archivo de claves objetivo cuando se especifica incorporación, si no existe ya el archivo de claves.	*WX
Archivo de claves cuando se especifica la lista	*R
Archivo de claves objetivo cuando se especifica la incorporación o supresión	*RW
Todos los directorios en las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Mensajes

- Debe especificar *add*, *delete*, *list*, o *merge*.
- La *opción_mandato* no es una opción de mandato válida.
- La *opción_mandato_uno* y la *opción_mandato_dos* no pueden especificarse juntas.
- La opción *opción_valor* no es válida para la petición *nombre_petición*.
- La opción *nombre_opción* necesita un valor.
- No se ha podido analizar el nombre de sujeto.
- Debe especificar el nombre del sujeto.
- No se ha podido leer la contraseña.
- No se ha encontrado la tabla de claves por omisión.
- No se ha podido resolver la tabla de claves *tabla_de_claves*.
- No se ha podido leer la entrada de la tabla de claves *tabla_de_claves*.
- No se ha podido eliminar la entrada de la tabla de claves *tabla_de_claves*.
- No se ha podido añadir la entrada a la tabla de claves *tabla_de_claves*.
- No se han encontrado entradas para el sujeto *nombre_sujeto*.
- 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* para el sujeto *nombre_sujeto*.

Para obtener un ejemplo de cómo se utiliza este mandato, consulte Gestionar archivos de tabla de claves.

Cambiar las contraseñas de Kerberos

El mandato **kpasswd** cambiará la contraseña para el sujeto Kerberos especificado utilizando el servicio de cambio de contraseñas. Debe facilitar la contraseña actual para el sujeto, así como la contraseña nueva. Antes de cambiar la contraseña, el servidor de contraseñas aplicará a la nueva contraseña las reglas aplicables de la política de contraseñas. El servidor de contraseñas se configura durante la instalación y configuración del KDC. Consulte la documentación referente a ese sistema. 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 puede cambiar la contraseña para un sujeto de servicio de otorgación de tickets (krbtgt/realm) con el mandato **kpasswd**.

Para cambiar la contraseña del sujeto por omisión:

En un línea de mandatos Qshell, entre

```
kpasswd
```

O

En un línea de mandatos Qshell, entre

```
call qsys/qkrbkpsswd
```

Para cambiar la contraseña para otro sujeto:

En un línea de mandatos Qshell, entre

```
kpasswd jsmith@ordept.myco.com
```

O

En una línea de mandatos, entre

```
call qsys/qkrbkpsswd parm ('jsmith@ordept.myco.com')
```

Para más detalles sobre el uso de este mandato, consulte las notas de empleo de kpasswd.

kpasswd

Sintaxis

```
kpasswd [-A ] [sujeto]
```
Autorización pública por omisión: *USE

El mandato Qshell kpasswd cambia la contraseña de un sujeto kerberos.

Opciones

-A El ticket inicial utilizado por el mandato kpasswd no incluirá una lista de direcciones cliente. Si no se especifica esta opción, el ticket incluirá la lista de direcciones del sistema principal local. Cuando un ticket inicial contiene una lista de direcciones, puede utilizarse sólo desde una de las direcciones de la lista de direcciones.

sujeto El sujeto cuya contraseña se debe modificar. El sujeto se obtendrá de la antememoria de credenciales por omisión si el sujeto no se especifica en la línea de mandatos.

Mensajes

- El sujeto %3$s no es válido.
- No se ha podido leer la antememoria de credenciales por omisión nombre_archivo.
- No se ha encontrado una antememoria de credenciales por omisión.
- No se ha podido recuperar el ticket de la antememoria de credenciales nombre_archivo.
- No se ha podido leer la contraseña.
- Se ha cancelado el cambio de contraseña.
- La contraseña no es correcta para nombre_sujeto.
- No se ha podido obtener el ticket inicial.
- Ha fallado la petición de cambio de la contraseña.

Para obtener un ejemplo de cómo se utiliza este mandato, consulte Modificar las contraseñas Kerberos.

Supresión de archivos de antememoria de credenciales que han expirado

El mandato **kdestroy** suprime un archivo de antememoria de credenciales Kerberos. Los usuarios deben suprimir periódicamente credenciales anteriores utilizando el mandato kdestroy.

La opción *-e* provoca que el mandato **kdestroy** verifique todos los archivos de la antememoria de credenciales en el directorio de la antememoria por omisión

(**/QIBM/UserData/OS400/NetworkAuthentication/creds**). Se suprime cualquier archivo que contenga sólo tickets caducados que hayan caducado para *incremento_de_tiempo*. *incremento_de_tiempo* se expresa 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 sólo se especifica un número, el valor por omisión son las horas.

Para suprimir su antememoria de credenciales por omisión:
En un línea de mandatos Qshell, entre

```
kdestroy
```

O

En un línea de mandatos iSeries, entre

```
call qsys/qkrbkdstry
```

Para suprimir todos los archivos de la antememoria de credenciales que tienen tickets caducados con una antigüedad superior a un año:

En un línea de mandatos Qshell, entre

```
kdestroy -e 1d
```

O

En un línea de mandatos iSeries, entre

```
call qsys/qkrbkdstry parm ('e' '-1d')
```

Consulte las notas de empleo sobre este mandato Qshell, donde encontrará detalles sobre su utilización y las restricciones.

kdestroy

Sintaxis

```
kdestroy [-c nombre_de_antememoria] [-e incremento_de_tiempo]
```
Autorización pública por omisión: *USE

El mandato Qshell **kdestroy** destruye una antememoria de credenciales Kerberos.

Opciones

-c nombre_de_antememoria
Especifica el nombre de la antememoria de credenciales que se debe destruir. Si no se especifican opciones de mandato, se destruye la antememoria de credenciales por omisión. Esta opción es mutuamente excluyente con la opción `-e`.

-e incremento_de_tiempo
Todos los archivos de la antememoria de credenciales que contienen tickets caducados se borran si dichos tick ets llevan caducados como mínimo el mismo período de tiempo que el valor `incremento_de_tiempo`.

Autorizaciones

Cuando la antememoria de credenciales es de la clase **FILE** (consulte **krb5_cc_resolve()** para obtener más información sobre las clases de antememoria), el comportamiento por omisión consiste en crear el archivo de la antememoria de credenciales en el directorio /QIBM/UserData/OS400/NetworkAuthentication/creds.Puede modificar la posición del archivo de la antememoria de credenciales estableciendo la variable de entorno KRB5CCNAME.

Cuando el archivo de la antememoria de credenciales no se encuentra en el directorio por omisión, se necesitan las siguientes autorizaciones:

Objeto referido a	**Autorización de datos necesaria**	**Autorización de objetos necesaria**
Todos los directorios en el nombre de la vía de acceso que precede al archivo de la antememoria de credenciales	*X	Ninguna
Directorio padre del archivo de la antememoria de credenciales	*WX	Ninguna
Archivo de la antememoria de credenciales	*RW	*OBJEXIST
Todos los directorios en las vías de acceso a los archivos de configuración	*X	Ninguna
Archivos de configuración	*R	Ninguna

Cuando el archivo de la antememoria de credenciales se encuentra en el directorio por omisión, se necesitan las siguientes autorizaciones:

Objeto referido a	**Autorización de datos necesaria**	**Autorización de objetos necesaria**
Todos los directorios del nombre de la vía de acceso	*X	Ninguna
Archivo de la antememoria de credenciales	*RW	Ninguna
Todos los directorios en 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 la antememoria de credenciales desde cualquier proceso en ejecución, el nombre del archivo de la antememoria normalmente se almacena en el directorio de inicio en un archivo denominado krb5ccname. Un usuario que desee utilizar la autenticación Kerberos en el iSeries debe tener definido un directorio de inicio. Por omisión, el directorio de inicio es /home/. Este archivo se utiliza para encontrar la antememoria de credenciales por omisión si no se han especificado opciones de mandato. La posición de almacenamiento del nombre del archivo de antememoria puede alterarse temporalmente estableciendo la variable de entorno _EUV_SEC_KRB5CCNAME_FILE. Para acceder a este archivo, el perfil de usuario debe tener autorización ***X** para todos los directorios de la vía de acceso y autorización ***R** para el archivo donde se almacena el nombre del archivo de la antememoria.

Mensajes

- No se ha podido resolver la antememoria de credenciales *nombre_archivo_antememoria*.
- No se ha podido destruir la antememoria de credenciales *nombre_archivo_antememoria*.
- La función *nombre_función* ha detectado un error.
- No se ha podido recuperar el ticket de la antememoria de credenciales *nombre_archivo*.
- La opción *nombre_opción* necesita un valor.
- *opción_mandato* no es una opción de mandato válida.
- Puede que *opción_mandato_uno* y *opción_mandato_dos* no se hayan especificado juntas.
- No se ha encontrado una antememoria de credenciales por omisión.
- El valor de incremento de tiempo *valor* no es válido.

Para obtener un ejemplo del modo en que se utiliza este mandato, consulte Suprimir archivos caducados de la antememoria de credenciales .

Gestionar entradas de servicio Kerberos en directorios LDAP

El mandato **ksetup** maneja las entradas de servicio Kerberos en los directorios LDAP. Se admiten los siguientes submandatos:

addhost nombre_sistema_principal nombre_reino
Este submandato añade una entrada de sistema principal para el reino especificado. Se utilizará el nombre de sistema principal totalmente calificado de modo que se resuelva correctamente sea cual sea el dominio DNS por omisión en vigor en los clientes Kerberos. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

addkdc nombre_sistema_principal:número_puerto nombre_reino
Este submandato añade una entrada KDC para el reino especificado. Si todavía no existe una entrada de sistema principal, se crea una. Si no se especifica un número de puerto, se establece en 88. Utilice el nombre de sistema principal totalmente calificado de modo que se resuelva correctamente sea cual sea el dominio DNS por omisión en vigor en los clientes Kerberos. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

delhost nombre_sistema_principal nombre_reino
Este submandato suprime una entrada de sistema principal y cualquier especificación KDC asociada del reino especificado. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

delkdc nombre_sistema_principal nombre_reino
Este submandato suprime una entrada KDC para el reino especificado. La propia entrada de sistema principal no se suprime. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

listhost nombre_reino
Este submandato muestra en modo de lista las entradas de sistema principal para un reino. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

listkdc nombre_reino
Este submandato muestra en modo de lista las entradas KDC para un reino. Si no se especifica un nombre de reino, se utiliza el nombre de reino por omisión.

exit
Este submandato finaliza el mandato ksetup.

Ejemplos

Para añadir el sistema principal kdc1.ordept.myco.com al servidor ldapserv.ordept.myco.com como KDC para el reino ORDEPT.MYCO.COM, utilizando el ID de administrador de LDAP Administrator y la contraseña verysecret, siga los pasos siguientes:

En una línea de mandatos Qshell, entre: `ksetup -h ldapserv.ordept.myco.com -n CN=Administrator -p verysecret`

O

1. En un línea de mandatos iSeries, entre:

   ```
   call qsys/qkrbksetup parm('-h' 'ldapserv.ordept.myco.com' '-n' 'CN=Administrator' '-p' 'verysecret')
   ```

2. Cuando se establece contacto satisfactoriamente con el servidor LDAP, se visualiza un indicador de submandatos. Especifique

   ```
   addkdc kdc1.ordept.myco.com ORDEPT.MYCO.COM
   ```

Consulte las notas de empleo sobre este mandato Qshell, donde encontrará detalles sobre su utilización y las restricciones.

ksetup

Sintaxis

`ksetup -h nombre_sistema_principal -n nombre_enlace -p contraseña_enlace -e`
Autorización pública por omisión: *USE

El mandato Qshell **ksetup** maneja entradas de servicio Kerberos en el directorio LDAP para un reino Kerberos.

Opciones

-h
El nombre del sistema principal para el servidor LDAP. Si no especifica esta opción, se utilizará el servidor LDAP especificado en el archivo de configuración Kerberos.

-n
El nombre distinguido que se debe utilizar al enlazarse al servidor LDAP. Si no especifica esta opción, se utiliza la variable de entorno LDAP_BINDDN para obtener el nombre.

-p
El nombre distinguido que se debe utilizar al enlazarse al servidor LDAP. Si no se especifica esta opción, se utiliza la variable de entorno LDAP_BINDPW para obtener la contraseña.

-e
Repetición de cada línea de mandatos para stdout. Es útil cuando stdin se redirige a un archivo.

Autorizaciones

Objeto referido a	Autorización necesaria
Todos los directorios en las vías de acceso a los archivos de configuración	*X
Archivos de configuración	*R

Mensajes

- El submandato `subcommand` 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 pueden especificarse juntas.
- No se ha podido inicializar el cliente LDAP.
- No se ha podido enlazar al servidor LDAP.
- Debe especificarse el nombre del reino.
- Debe especificarse el nombre del sistema principal.
- Demasiados parámetros de posición.
- El sistema principal `sistema_principal` ya existe.
- No se ha definido el dominio raíz `dominio`.
- El nombre de reino `reino` no es válido.
- La función `nombre_función_LDAP` ha detectado un error.
- Almacenamiento disponible insuficiente.
- El nombre de sistema principal `sistema_principal` no es válido.
- El número de puerto `puerto` no es válido.
- No se ha definido el sistema principal `sistema_principal`.
- No se ha definido un KDC para el sistema principal `sistema_principal`.

- No se ha podido obtener el nombre de reino por omisión.

Para obtener un ejemplo de cómo se utiliza este mandato, consulte Gestión de las entradas de servicio Kerberos en directorios LDAP.

Solución de problemas relacionados con el servicio de autenticación de red

Este apartado facilita enlaces a información para la solución de problemas habituales relacionados con el servicio de autenticación de red, EIM (Enterprise Identity Mapping), y aplicaciones nativas de iSeries que dan soporte a la autenticación de Kerberos.

1. Se han completado todos los requisitos previos.
2. Asegúrese de que el usuario tiene un perfil de usuario en el iSeries y un nombre de sujeto en el KDC. En el iSeries, compruebe que el usuario existe abriendo Usuarios y Grupos en el Navigator de iSeries o utilizando `WRKUSRPRF` para una línea de mandatos. En sistemas Windows (R), compruebe que el usuario existe accediendo a la carpeta Usuarios y Sistemas de Active Directory (R).
3. Compruebe si el iSeries contacta con el KDC utilizando el mandato kint del Intérprete de Qshell. Si falla el mandato kinit, verifique si el sujeto de servicio del iSeries ha sido registrado en el KDC. En caso negativo, puede añadir el nombre de sujeto del iSeries al KDC.

Para obtener información sobre determinados mensajes, consulte los temas siguientes:

- Errores y recuperación del servicio de autenticación de red
  Estos errores pueden aparecer durante la ejecución del asistente del servicio de autenticación de red o durante la gestión de propiedades del servicio de autenticación de red en el Navigator de iSeries.
- Errores de conexión de aplicaciones y recuperación
  Este tema aborda los mensajes de error comunes cuando las aplicaciones utilizan el servicio de autenticación de red, EIM y algunas aplicaciones nativas de iSeries, que pueden surgir cuando el iSeries, el servicio o el usuario intenta conectarse al KDC.

Errores y recuperación del servicio de autenticación de red

Estos errores pueden aparecer durante la ejecución del asistente del servicio de autenticación de red o durante la gestión de propiedades del servicio de autenticación de red en el Navigator de iSeries.

Mensaje	Recuperación
KRBWIZ_CONFIG_FILE_FORMAT_ERROR El formato del archivo de configuración del servicio de autenticación de red es erróneo.	Vuelva a configurar el servicio de autenticación de red. Véase Configurar el servicio de autenticación de red para obtener más detalles.

KRBWIZ_CRYPTO_NOT_INSTALLED El producto de cifrado requerido no está instalado en el sistema.	Instale el Proveedor de acceso de cifrado (572-AC3) en el sistema.
KRBWIZ_ERROR_READ_CONFIG_FILE Error al leer el archivo de configuración del servicio de autenticación de red.	Vuelva a configurar el servicio de autenticación de red. Véase Configurar el servicio de autenticación de red para obtener más detalles.
KRBWIZ_ERROR_WRITE_CONFIG_FILE Error al grabar el archivo de configuración del servicio de autenticación de red.	El servicio utilizado para grabar el archivo de configuración no está disponible. Vuelva a intentarlo más tarde.
KRBWIZ_PASSWORD_MISMATCH La contraseña nueva y su confirmación no son iguales.	Vuelva a entrar la contraseña nueva y su confirmación.
KRBWIZ_PORT_ERROR El número de puerto debe estar entre 1 y 65535.	Vuelva a entrar un número de puerto entre 1 y 65535.
KRBWIZ_ERROR_WRITE_KEYTAB Error al grabar el archivo de claves	El servicio utilizado para grabar la tabla de claves no está disponible. Vuelva a intentarlo más tarde.
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 KDC especificado no existe en la lista. Seleccione un KDC de la lista.
KrbPropKDCValueRequired Debe entrarse un nombre de KDC.	Entre un nombre válido para el KDC. El KDC debe configurarse en un sistema seguro en la red.
KrbPropPwdServerRequired Debe entrarse un nombre de servidor de contraseñas.	Entre un nombre válido para el servidor de contraseñas.
KrbPropRealmRequired Debe entrarse un nombre de reino.	Entre el nombre del reino al que pertenece este sistema.
KrbPropRealmToTrustRequired Debe entrarse un nombre para el reino de confianza.	Entre el nombre del reino con el que se esté estableciendo una relación de confianza.
KrbPropRealmValueRequired Debe entrarse un nombre de reino.	Entre un nombre válido para el reino.
CPD3E3F Ha ocurrido el error de servicio de autenticación de red &2.	Consulte la información de recuperación específica que corresponde a este mensaje.

Problemas de conexión de aplicaciones y recuperación

Estos mensajes pueden aparecer cuando las aplicaciones utilizan el servicio de autenticación de red.

Problema	Recuperación
Se recibe este error: No se ha podido obtener el nombre de la antememoria de credenciales por omisión.	Determine si el usuario que ha iniciado la sesión en el iSeries tiene un directorio en el directorio /home. Si no existe el directorio para el usuario, cree un directorio de inicio para la antememoria de credenciales.
CPD3E3F Ha ocurrido el error de servicio de autenticación de red &2.	Consulte la información de recuperación específica que corresponde a este mensaje.
La conexión DRDA/DDM falla en un sistema iSeries previamente conectado.	Compruebe si existe el reino por omisión especificado durante la configuración del servicio de autenticación de red. Si no se ha configurado un centro de distribución de claves (KDC) y un reino por omisión, la configuración del servicio de autenticación de red será incorrecta y fallarán las conexiones DRDA/DDM. Como recuperación de este error, puede llevar a cabo una de estas tareas: 1. Si no está utilizando la autenticación de Kerberos, complete estos pasos: a. Suprima los reinos por omisión especificados en la configuración del servicio de autenticación de red. 2. Si está utilizando la autenticación de Kerberos, complete estos pasos: a. Configure un KDC y un reino por omisión en un sistema seguro en la red. Consulte la documentación correspondiente al sistema. **Nota:** actualmente el iSeries no da soporte al KDC. b. Vuelva a configurar el servicio de autenticación de red especificando el reino por omisión y el KDC que ha creado en el Paso 1. c. Configure (Ver 27) las aplicaciones de iSeries Access for Windows de forma que utilicen la autenticación de Kerberos. Ello configurará la autenticación de Kerberos en todas las aplicaciones de iSeries Access for Windows, inclusive DRDA/DDM.

La conexión QFileSvr.400 falla en un sistema iSeries previamente conectado.	Compruebe si existe el reino por omisión especificado durante la configuración del servicio de autenticación de red. Si no se ha configurado un centro de distribución de claves (KDC) y un reino por omisión, la configuración del servicio de autenticación de red será incorrecta y fallarán las conexiones QFileSvr.400. Como recuperación de este error, puede llevar a cabo una de estas tareas: 1. Si no está utilizando la autenticación de Kerberos, complete estos pasos: a. Suprima los reinos por omisión especificados en la configuración del servicio de autenticación de red. 2. Si está utilizando la autenticación de Kerberos, complete estos pasos: a. Configure un KDC y un reino por omisión en un sistema seguro en la red. Consulte la documentación correspondiente al sistema. **Nota:** actualmente el iSeries no da soporte al KDC. b. Vuelva a configurar el servicio de autenticación de red especificando el reino por omisión y el KDC que ha creado en el Paso 1. c. Configure (Ver 27) las aplicaciones de iSeries Access for Windows de forma que utilicen la autenticación de Kerberos. Ello configurará la autenticación de Kerberos en todas las aplicaciones de iSeries Access for Windows, inclusive DRDA/DDM.
CWBSY1011 No se han encontrado credenciales de cliente Kerberos.	El usuario no posee un ticket de otorgación de tickets (TGT). Este error de conexión surge en un PC cliente cuando un usuario no inicia la sesión en un dominio Windows (R) 2000. Como recuperación de este error, inicie la sesión en el dominio Windows (R) 2000.
Se ha producido un error al verificar los valores de la conexión. El URL no dispone de sistema principal. **Nota:** este error surge cuando se utiliza EIM (Enterprise Identity Mapping).	Como recuperación de este error, complete estos pasos: 1. En el Navigator de iSeries, expanda **su** —> **Red**—>**Servidores**—> **TCP/IP**. 2. Pulse el botón derecho sobre **Directorio** y seleccione **Propiedades**. 3. En la página **General**, compruebe que la contraseña y el nombre distinguido del administrador coinciden con los entrados durante la configuración de EIM.
Se ha producido un error al cambiar la configuración del servidor de directorios local. GLD0232: la configuración no puede contener sufijos que se solapen. **Nota:** este error surge cuando se utiliza EIM (Enterprise Identity Mapping).	Como recuperación de este error, complete estos pasos: 1. En el Navigator de iSeries, expanda **su** —> **Red**—>**Servidores**—> **TCP/IP**. 2. Pulse el botón derecho sobre **Directorio** y seleccione **Propiedades**. 3. En la página **Base de datos/Sufijos**, elimine cualquier entrada **ibm-eimDomainName** y vuelva a configurar EIM.

Se ha producido un error al verificar los valores de la conexión. Se ha producido una excepción al llamar a un programa de iSeries. El programa que se ha llamado es eimConnect. Estos son los detalles: com.ibm.as400.data.PcmlException.
Nota: este error surge cuando se utiliza EIM (Enterprise Identity Mapping).

Como recuperación de este error, complete estos pasos:

1. En el Navigator de iSeries, expanda **su** —> **Red**—>**Servidores**—> **TCP/IP**.
2. Pulse el botón derecho sobre **Directorio** y seleccione **Propiedades**.
3. En la página **Base de datos/Sufijos**, elimine cualquier entrada **ibm-eimDomainName** y vuelva a configurar EIM.

Información relacionada

Especificaciones del protocolo Kerberos

El servicio de autenticación de red Kerberos (V5)

.
El grupo IETF (Internet Engineering Task Force) define formalmente el protocolo Kerberos en RFC 1510.

Kerberos: el protocolo de autenticación de red (V5)

.
La documentación oficial del Massachusetts Institute of Technology sobre el protocolo Kerberos proporciona información sobre programación y describe las características del protocolo.

Especificaciones de la API GSS (Generic Security Services)

Para obtener más información sobre Kerberos y las API GSS, consulte las siguientes fuentes:

API GSS Versión 2, actualización 1

.
El grupo IETF (Internet Engineering Task Force) define formalmente las API GSS en RFC 2743.

API GSS: C-bindings

.
El grupo IETF (Internet Engineering Task Force) especifica los enlaces C de las API GSS en RFC 1509.

El mecanismo de API GSS Kerberos de la versión 5

.
El grupo IETF (Internet Engineering Task Force) define las especificaciones de la API GSS y de Kerberos versión 5 en RFC 1964.

Temas relacionados con el Centro de información

Las API del servicio de autenticación de red
Este tema del Centro de información proporciona una lista de las API del servicio de autenticación de red y descripciones breves de sus funciones.

Las API GSS
Este tema del Centro de información proporciona una lista de las API GSS y descripciones breves de sus funciones.

EIM (Enterprise Identity Mapping)
EIM es un mecanismo para correlacionar una persona o identidad (p.ej. un servicio) con las identidades de usuario apropiadas en varios registros de usuario de la empresa. El iSeries utiliza EIM para permitir a las interfaces del OS/400 autenticar a los usuarios a través del servicio de autenticación de red. El iSeries y las aplicaciones también pueden aceptar tickets Kerberos y utilizar EIM para buscar un ID de usuario en este sistema asociado con el sujeto Kerberos.

Condiciones y conceptos especiales

Los siguientes conceptos y condiciones sólo son válidos para el código del Servicio de autenticación de red, que se incluye en el programa de servicio QKRBGSS de la biblioteca QSYS, en el miembro KRB5 del archivo H de la biblioteca QSYSINC y en los catálogos de mensajes skrbdll.cat y skrbkut.cat que se incluyen en el directorio /QIBM/ProdData/OS400/NetworkAuthentication/.

IBM OTORGA LA LICENCIA DEL CÓDIGO OBJETO DEL SERVICIO DE AUTENTICACIÓN DE RED ″TAL CUAL″, SIN GARANTÍAS DE NINGÚN TIPO, INCLUSIVE, SIN LIMITARSE A ELLO, LAS GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD Y ADECUACIÓN PARA UN FIN DETERMINADO.

IBM NO GARANTIZA QUE EL USO DE DICHO CÓDIGO NO INFRINJA NINGÚN DERECHO DE COPIA, SECRETO COMERCIAL, PATENTE O CUALQUIER OTRO DERECHO DE PROPIEDAD, PROPIEDAD INTELECTUAL O DERECHO CONTRACTUAL DE UNA TERCERA PARTE.

Los colaboradores requieren los siguientes avisos:

Copyright 1985, 1986, 1987, 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995
by the Massachusetts Institute of Technology.
Reservados todos los derechos.

La exportación de este software fuera de los Estados Unidos puede exigir una licencia específica del Gobierno de EE.UU. Es responsabilidad de la persona u organización que tenga en mente la exportación obtener dicha licencia antes de 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 copia conste en todas las copias y que tanto la nota de derechos de copia como la nota referente a este permiso aparezcan en la documentación auxiliar, y que el nombre del M.I.T. no se utilice en anuncios o publicidad relacionados con la distribución del software sin el previo permiso

por escrito específico. El M.I.T. no efectúa ninguna declaración sobre la idoneidad de este software para un fin determinado. Se ofrece ″tal cual″ sin garantías implícitas o explícitas.

Copyright 1994 by the Massachusetts Institute of Technology.
Copyright (c) 1994 CyberSAFE Corporation.
Copyright (c) 1993 Open Computing Security Group
Copyright (c) 1990, 1991 by the Massachusetts Institute of Technology.

Reservados todos los derechos.

La exportación de este software fuera de los Estados Unidos puede exigir una licencia específica del Gobierno de EE.UU. Es responsabilidad de la persona u organización que tenga en mente la exportación obtener dicha licencia antes de 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 copia conste en todas las copias y que tanto la nota de derechos de copia como la nota referente a este permiso aparezcan en la documentación auxiliar, y que el nombre del M.I.T. no se utilice en anuncios o publicidad relacionados con la distribución del software sin el previo permiso por escrito específico. M.I.T., Open Computing Security Group o CyberSAFE Corporation no efectúan ninguna declaración sobre la idoneidad de este software para una finalidad. Se ofrece ″tal cual″ sin garantías implícitas o explícitas.

Copyright 1995, 1996 by Richard P. Basch. Reservados todos los derechos.
Copyright 1995, 1996 by Lehman Brothers, Inc. Reservados todos los derechos.

La exportación de este software fuera de los Estados Unidos puede exigir una licencia específica del Gobierno de EE.UU. Es responsabilidad de la persona u organización que tenga en mente la exportación obtener dicha licencia antes de 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 copia conste en todas las copias y que tanto la nota de derechos de copia como la nota referente a este permiso aparezcan en la documentación auxiliar, y que el nombre de Richard P. Basch, Lehman Brothers y M.I.T. no se utilice en anuncios o publicidad relacionados con la distribución del software sin el previo permiso por escrito específico. Richard P. Basch, Lehman Brothers y M.I.T. no efectúan ninguna declaración sobre la idoneidad de este software para una finalidad. Se ofrece ″tal cual″ sin garantías implícitas o explícitas.

Estas condiciones especiales sólo son válidas para el código del Servicio de autenticación de red tal como se describe más arriba y no son válidas para ninguna otra parte del OS/400 o el Código interno con licencia.

Impreso en España