Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 8: Mantenimiento de soluciones de seguridad en LAN inalámbricas

Actualizado: abril 2, aaaa

Ver todos los temas de la guía de seguridad

En esta página

Introducción

Este capítulo trata los procedimientos operativos relacionados con la administración de la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Este capítulo contiene instrucciones sobre las tareas operativas y de soporte técnico esenciales que necesita llevar a cabo para mantener la infraestructura de seguridad en la red de área local inalámbrica (WLAN), incluidos los servidores del Servicio de autenticación de Internet (IAS), las entidades emisoras de certificados, los puntos de acceso inalámbrico y los clientes WLAN. No obstante, este capítulo no incluye información sobre la administración general de la red o sobre la administración de otros aspectos que no sean servicios de seguridad, como el análisis y la optimización del tráfico en la red.

Principio de la página

Información general

Las secciones más importantes de este capítulo son:

- **Tareas de mantenimiento esenciales:** en esta sección se enumeran las tareas clave que necesita poner en práctica para instalar el sistema de administración (por ejemplo, configurar trabajos de copias de seguridad), y aquéllas que necesita llevar a cabo de forma regular para mantener el sistema (por ejemplo, tareas semanales de reorganización de archivos).
- **Funcionamiento de la infraestructura de WLAN:** esta sección es, ante todo, una sección de referencia donde se detallan los diferentes tipos de tareas que ha de llevar a cabo para mantener la estructura de seguridad de WLAN. Los apartados contienen información sobre tareas operativas estándar, implementación de cambios, tareas de soporte técnico y de optimización.
- **Solución de problemas:** esta sección contiene procedimientos y diagramas de flujo que sirven para solucionar problemas comunes que pueden surgir con la infraestructura de WLAN. Asimismo, incluye descripciones de herramientas y procedimientos útiles destinados a la solución de problemas que permiten habilitar el registro de distintos componentes.
- **Referencias:** en esta sección se enumeran las fuentes de información adicional mencionadas en el texto.

Principio de la página

Requisitos previos del capítulo

Debe estar familiarizado con la administración de Microsoft® Windows® Server™ 2003 o de Windows® 2000 Server. Las siguientes áreas son particularmente importantes:

- Funcionamiento y mantenimiento básicos de Microsoft Windows Server 2003, incluido el uso de herramientas como Visor de sucesos, Administración de equipos y NTBackup.
- IAS.

Descargue la solución completa en

Seguridad en LAN inalámbricas con PEAP y contraseñas

Descargar la solución completa

Guía de defensa en profundidad antivirus

En esta guía

- Servicios de Certificate Server.
- Servicio de directorio Microsoft Active Directory® (incluidas las herramientas y la estructura de Active Directory), administración de usuarios, grupos y otros objetos de Active Directory, así como el uso de la directiva de grupo.
- Conceptos de seguridad del sistema Windows como usuarios, grupos, auditorías, listas de control de acceso, uso de plantillas de seguridad y aplicación de éstas utilizando directivas de grupo o herramientas de línea de comandos.
- LAN inalámbricas y conceptos de red generales.
- Conocimientos de Windows Script Host y de Microsoft Visual Basic® Scripting Edition (VBScript) que ayudarán a comprender y a utilizar las secuencias de comandos que la solución proporciona.

Además, es recomendable que haya leído los siguientes capítulos para adquirir un buen conocimiento de la arquitectura y diseño de la solución:

- Capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas"
- Capítulo 3, "Preparación del entorno"
- Capítulo 4, "Creación de la entidad emisora de certificados de red"
- Capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas"
- Capítulo 6, "Configuración de clientes de LAN inalámbricas"

Principio de la página

Tareas de mantenimiento esenciales

En esta sección se enumeran las tareas clave que debe realizar para que la infraestructura de WLAN funcione satisfactoriamente. Estas tareas se pueden dividir en dos categorías:

- Tareas de configuración iniciales
- Tareas de mantenimiento continuas

En esta sección también se enumeran las herramientas y las tecnologías utilizadas en los procedimientos de este capítulo.

Tareas de configuración iniciales

La siguiente tabla muestra las tareas que se deben realizar para poner en funcionamiento la infraestructura de seguridad de WLAN.

Tabla 8.1. Tareas de configuración iniciales

Nombre de la tarea	Sección
Configuración de la copia de seguridad de IAS	Tareas operativas
Configuración de los tipos de alerta	Supervisión
Habilitación de la supervisión de IAS	Supervisión
Habilitación de la supervisión de la entidad emisora	Supervisión

Tareas de mantenimiento

La siguiente tabla muestra las tareas que se deben realizar con regularidad para mantener el funcionamiento de la infraestructura de seguridad de WLAN de forma adecuada. Puede utilizar esta tabla para planear los recursos necesarios y el programa operativo relacionados con la administración del sistema.

Tabla 8.2. Tareas de mantenimiento

Nombre de la tarea	Frecuencia	Sección
Prueba de las copias de seguridad	6 meses	Tareas operativas

Herramientas y tecnología requeridas

En la tabla siguiente se enumeran las herramientas o tecnologías utilizadas en los procedimientos descritos en este capítulo.

Tabla 8.3. Tecnología requerida

Nombre del elemento	Fuente

Consola de administración (MMC) de usuarios y equipos de Active Directory	Windows Server 2003
MMC de la Entidad emisora de certificados	Windows Server 2003
Certutil.exe	Windows Server 2003
DCDiag.exe	Herramientas de soporte técnico de Windows Server 2003
DSquery.exe	Windows Server 2003
Visor de sucesos	Windows Server 2003
Consola de administración de directivas de grupo	Descarga Web desde Microsoft.com
MSS WLAN Tools	Secuencias de comandos instaladas como parte de esta solución
Netdiag.exe	Herramientas de soporte técnico de Windows Server 2003
Monitor de rendimiento	Windows Server 2003
Estado de la infraestructura de claves públicas	Kit de recursos de Windows Server 2003
Medios extraíbles para la creación de copias de seguridad de entidad emisora raíz	CD-RW o cinta
SchTasks.exe	Windows Server 2003
Editor de texto	Bloc de notas: Windows Server 2003
Copia de seguridad de Windows	Windows Server 2003
Servicio Programador de tareas de Windows	Windows Server 2003

Tabla 8.4. Tecnología recomendada

Nombre del elemento	Fuente
Infraestructura de correo electrónico (para alertas operativas)	Servidor y cliente SMTP/POP3/IMAP, por ejemplo Microsoft Exchange Server y Microsoft Outlook®
Consola de alertas operativas	Microsoft Operations Manager u otro sistema de supervisión de servicios
Distribución de actualizaciones de sistemas operativos	Microsoft Systems Management Server (SMS) o Microsoft Software Update Service (SUS)

Principio de la página

Funcionamiento de la infraestructura de WLAN

Esta sección incluye las tareas principales que necesita llevar a cabo para mantener la infraestructura de seguridad de WLAN.

Tareas operativas

Las tareas operativas abarcan los trabajos que hay que realizar regularmente para mantener el funcionamiento de la infraestructura de WLAN de forma adecuada.

Copias de seguridad de IAS y la entidad emisora de certificados

Debe realizar copias de seguridad de los servidores IAS regularmente, incluido el servidor IAS que ejecuta la entidad emisora de certificados. IAS requiere un procedimiento especial para exportar sus configuraciones a un archivo, del cual se puede realizar después una copia de seguridad normal. Puede realizar copias de seguridad de Servicios de Certificate Server utilizando la copia de seguridad del estado del sistema de Windows, disponible en la herramienta de copias de seguridad de Windows. Deberá establecer procedimientos de creación de copias de seguridad adecuados en todos los servidores en los que se esté ejecutando IAS.

Los dos procedimientos siguientes no se excluyen entre sí, sino que deberá configurar una copia de seguridad tanto de IAS como del servidor.

Configuración de la copia de seguridad de IAS

Ha de crear una carpeta con permisos restringidos a la que se exportará la configuración de IAS cada noche. También ha de crear un trabajo programado que ejecute cada noche la copia de seguridad de IAS (la secuencia de comandos de copia de seguridad no necesita que IAS se encuentre apagado para realizar la copia). Si la copia de seguridad se realiza correctamente, se escribirá un suceso en el registro de aplicaciones de Windows. En caso de error en la copia, se registrará un suceso de error.

Precaución: los archivos de seguridad de IAS incluyen todos los secretos de los clientes RADIUS. Se trata de una información extremadamente confidencial, por lo que debería tener cuidado y almacenar los datos en cuestión de forma segura.

Para configurar la copia de seguridad de IAS

1. Abra un shell de comandos en el servidor utilizando el acceso directo de **MSS WLAN Tools** e introduzca el siguiente comando para crear una carpeta en la que guardar la configuración de IAS:

   md c:\IASBackup

   La configuración de IAS suele ser menor de 100 KB y se puede guardar en la unidad del sistema, tal y como se muestra en el comando.

2. Utilice el siguiente comando para establecer permisos para la carpeta de forma que sólo los administradores y operadores de copias de seguridad puedan leer y modificar el contenido:

   cacls c:\IASBackup /G system:F administrators:F "Backup Operators":C

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea.

3. Pruebe la copia de seguridad con la ayuda del siguiente comando:

   "C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools\msstools.cmd" BackupIAS /path:C:\IASBackup

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea. "**Microsoft WLAN-PEAP Tools**" contiene dos espacios incrustados: uno después de "Microsoft" y otro después de "WLAN-PEAP".

   Nota: si la copia de seguridad se realiza correctamente, se escribirá un suceso en el registro de aplicaciones de Windows y en la pantalla. En caso contrario, se registrarán sucesos de error.

4. Cree una tarea programada que ejecute cada noche la exportación de la configuración de IAS. Por ejemplo, el siguiente comando programa un trabajo para ejecutarlo a las 22:00 horas cada noche:

   SCHTASKS /Create /RU system /SC Daily /TN "IAS Backup" /TR "\"C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools\msstools.cmd\" BackupIAS /path:C:\IASBackup" /ST 22:00

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea. "**Microsoft WLAN-PEAP Tools**" contiene dos espacios incrustados: uno después de "Microsoft" y otro después de "WLAN-PEAP".

   Nota: adjuntar la ruta al archivo de secuencias de comandos msstools.cmd entre barras diagonales inversas (\) garantiza que el shell de comandos de Windows no va a interpretar las comillas dobles ("), ni las va a quitar del comando. El comando que admite y almacena el programador de tareas es el que se muestra en el paso 3.

Realización de copias de seguridad del servidor

Una vez establecida la tarea programada para realizar la copia de seguridad de IAS en el disco, debe configurar también una copia de seguridad regular, en un medio extraíble o en una ubicación de red, del estado del sistema del servidor y de los archivos de la configuración de IAS exportados. La forma más sencilla de llevarlo a cabo es utilizar la herramienta integrada de copias de seguridad de Windows. En caso de usar un sistema de copias de seguridad diferente, debe comprobar si incluye la funcionalidad equivalente a las copias de seguridad del estado del sistema de Windows. Esta información debe reflejarse en la documentación del sistema de copias de seguridad en cuestión. Una copia de seguridad del estado del sistema (o equivalente) es esencial para realizar correctamente copias de seguridad de las claves de Active Directory y del Servicio Certificate Server, así como de las bases de datos de certificados.

Si el software de copias de seguridad no incluye la funcionalidad de copias de seguridad del estado del sistema de Windows, puede efectuar los siguientes pasos:

- Configure la herramienta de copias de seguridad de Windows para que realice una copia de seguridad del estado del sistema en un archivo del servidor (debe asegurarse de que tiene suficiente espacio libre, dado que esta copia ocupará 500 MB o más). Consulte la ayuda en línea de esta herramienta para obtener más detalles sobre este paso.
- Configure el software de copias de seguridad para que copie el archivo de la copia de seguridad del estado del sistema, así como el archivo de la copia de seguridad de IAS descrito en el procedimiento anterior.

Para garantizar que las copias de seguridad son seguras y consistentes, efectúe lo siguiente:

- Programe las distintas operaciones de copia de seguridad de forma que no se superpongan o, de lo contrario, se arriesgará a dañar los datos de las copias.
- Comience las copias de seguridad del estado del sistema y del servidor con al menos 10 minutos de diferencia con respecto a las copias de IAS.
- Si está realizando copias de seguridad del estado del sistema y del archivo del servidor de forma separada, deje que transcurra al menos una hora antes de comenzar con la copia del archivo del servidor para que finalice la copia del estado del sistema.
- Almacene siempre una copia reciente de los datos de la copia de seguridad en una ubicación física distinta a la del servidor del que se ha realizado la copia. Así, podría recuperar el servidor si el equipo informático del sitio se destruyera o si no se pudiera tener acceso a

él.

Precaución: estos datos son confidenciales porque contienen secretos de RADIUS de todos los puntos de acceso en el servidor, de todo el material clave privado de la entidad emisora de certificados y de la base de datos de Active Directory. Debe transportar y almacenar los medios de copias de seguridad con la mayor protección posible, ya que el acceso no autorizado a esta información podría comprometer la seguridad de toda la organización.

Prueba de las copias de seguridad

Para comprobar las copias de seguridad del sistema de forma adecuada, sólo tiene que restaurarlas en un servidor de prueba y comprobar que el servidor restaurado funciona como se espera. La copia de seguridad del estado del sistema se debe restaurar en un sistema con un diseño de disco idéntico al del servidor del que se ha realizado la copia. Por ejemplo, Windows debe estar instalado en la misma ruta tanto en el servidor original como en el de prueba, al tiempo que el diseño de la unidad en la que se almacenan los archivos de Windows (como los archivos de paginación) debe ser igualmente idéntico en ambos.

Importante: para evitar conflictos con el nombre y las direcciones IP entre ambos servidores, el servidor de prueba se debe mantener sin conexión desde el momento en el que comienza la restauración del estado del sistema.

Para restaurar el servidor

1. Prepare un servidor de restauración en el que quiera restaurar las copias de seguridad. En él, tendrá que utilizar la misma edición de Windows Server 2003 que en el servidor original. También debe instalar las secuencias de comandos de la solución en este servidor. Para obtener más información, consulte la sección "Instalación de herramientas de la solución" en el capítulo 3, "Preparación del entorno".
2. Si usa copias de seguridad del estado del sistema y de los archivos por separado, utilice el software de copias de seguridad para restaurar los archivos de las copias de seguridad del estado del sistema y los de la configuración de IAS desde el medio de copia de seguridad al servidor. La configuración de IAS se debe restaurar en la misma ruta: C:\IASBackup.
3. Ejecute la utilidad de copias de seguridad de Windows y seleccione el archivo de la copia de seguridad del estado del sistema restaurado. Deberá pertenecer a un grupo que posea derechos de creación de copias de seguridad y restauración en el equipo (como Operadores de copia de seguridad o Administradores).
4. Haga clic en **Restaurar**.
5. Reinicie el sistema.
6. Una vez reiniciado, compruebe que el funcionamiento es el esperado y que Active Directory y los Servicios de Certificate Server se han iniciado sin errores (probablemente se produzcan errores en el registro de sucesos, dado que el servidor no está conectado a la red).
7. Utilice el acceso directo **MSS WLAN Tools** para abrir el shell de comandos. Para restaurar la configuración de IAS, ejecute el siguiente comando:

   MSSTools RestoreIAS /path:C:\IASBackup

8. Para comprobar que la configuración de IAS se ha restaurado, abra la consola de administración de IAS y compruebe los clientes RADIUS y las carpetas de directivas de acceso remoto.

Supervisión

Esta sección describe la supervisión de los componentes de IAS y de la entidad emisora de certificados de la infraestructura de seguridad de WLAN. No incluye información sobre la supervisión de los puntos de acceso inalámbrico o de otros dispositivos de red, ni ofrece consejos generales sobre la supervisión de servidores de Windows. Para obtener más información sobre la supervisión de servidores de Windows, consulte la sección "Referencias" al final del capítulo.

En gran parte de los procedimientos de esta sección se emplean secuencias de comandos de supervisión automatizadas que se obtienen junto con la solución. Si estas secuencias de comandos detectan un error, desencadenarán una alerta y, en algunos casos, intentarán recuperarse del mismo.

Configuración de los tipos de alerta

Cualquier alerta de las secuencias de comandos de supervisión se puede enviar al registro de aplicaciones de Windows, a uno o más destinatarios de correo electrónico o a ambos. Antes de habilitar las herramientas de supervisión, ha de especificar los tipos de alerta que desea. Además, si ha optado por enviar alertas por correo electrónico, debe proporcionar las direcciones de correo electrónico de los destinatarios y el nombre del servidor de correo al que desea enviar los mensajes.

Para especificar estos parámetros, es preciso modificar el archivo constants.vbs. A continuación se muestran las secciones más importantes de este archivo con los elementos que probablemente desee cambiar en *cursiva*:

```
'Parámetros de alerta
CONST ALERT_EMAIL_ENABLED = FALSE    'establecido en habilitar/deshabilitar correo electrónico
CONST ALERT_EVTLOG_ENABLED = TRUE    'establecido en habilitar/deshabilitar entradas del registro de sucesos
' establecido en lista de destinatarios de alertas de correo electrónico separados por comas
CONST ALERT_EMAIL_RECIPIENTS    = "Admin@woodgrovebank.com,Ops@woodgrovebank.com"
```

```
'servidor SMTP que se va a utilizar (use el nombre DNS o la dirección IP)
CONST ALERT_EMAIL_SMTP     = "mail.woodgrovebank.com"
```

Supervisión de IAS
IAS registrará varios sucesos en el registro del sistema de Windows. Éstos incluyen notificaciones de inicio y de término del servicio (y todos los errores o advertencias asociados), así como notificaciones de intentos de autenticación. Las entradas del registro de solicitud de autenticación se describen en detalle en la sección "Solución de problemas" de este capítulo.

Habilitación de la supervisión de IAS
Esta solución incluye una sencilla secuencia de comandos que supervisa el nivel de respuesta de IAS. La secuencia de comandos comprueba si el proceso de IAS se está ejecutando. Si es así, la secuencia de comandos intenta consultar a IAS empleando la interfaz **Objetos de datos del servidor**. Si alguna de estas comprobaciones presenta errores, la secuencia de comandos emitirá una alerta.

Nota: la secuencia de comandos de supervisión no comprueba que la autenticación RADIUS sea correcta; sólo comprueba el nivel de respuesta general del proceso de IAS. Para comprobar las operaciones de RADIUS de forma integral, necesita un cliente RADIUS para emular los puntos de acceso inalámbrico que transfieren la solicitud del cliente WLAN.

El procedimiento siguiente describe cómo configurar la secuencia de comandos de supervisión para que se ejecute como tarea programada, a fin de que las alertas se emitan de forma automática si IAS deja de responder. No obstante, dado que la secuencia se ejecuta en el mismo servidor, es obvio que no podrá avisarle si se produce un error de carácter general en el servidor. En consecuencia, deberá supervisar también los servidores para asegurarse de que funcionan y responden. Para configurar la ejecución de la secuencia de comandos como una tarea programada en cada servidor IAS, deberá realizar el siguiente procedimiento:

Cada vez que se detecte un error, se enviará una alerta por correo electrónico (si se han configurado las alertas por correo electrónico) y se registrará un suceso en el registro de aplicaciones (consulte la tabla de la sección siguiente para obtener más detalles sobre los tipos de sucesos registrados). A diferencia de la secuencia de comandos de supervisión de la entidad emisora de certificados, no se intentará reiniciar IAS para corregir los problemas. Esto se debe a que IAS debe autenticar clientes WLAN continuamente (cosa que no sucede con la entidad emisora). Permitir que la secuencia de comandos de supervisión reinicie IAS a ciegas puede ocasionar problemas en lugar de resolverlos. En su lugar, permanezca atento a cualquier alerta generada por la secuencia y realice el diagnóstico adecuado de la causa de la alerta antes de intentar resolver el problema manualmente.

Para configurar la supervisión de IAS

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el siguiente comando para programar la ejecución de la secuencia de comandos cada noche a las 1:30 horas (se ejecuta 30 minutos después de la hora para compensar el trabajo de copia de seguridad de IAS).

   SCHTASKS /Create /RU system /SC Hourly /TN "IAS Check" /TR "\"C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools\msstools.cmd\" CheckIAS" /ST 1.30

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea. "**Microsoft WLAN-PEAP Tools**" contiene dos espacios incrustados: uno después de "Microsoft" y otro después de "WLAN-PEAP".

   Nota: adjuntar la ruta al archivo de secuencias de comandos msstools.cmd entre barras diagonales inversas (\) garantiza que el shell de comandos de Windows no va a interpretar las comillas dobles ("), ni las va a quitar del comando. El uso de barras diagonales inversas (\) antes de las comillas (") garantiza que el comando que el programador de tareas admite y almacena es el mostrado en el paso 2.

Sucesos IAS registrados por las secuencias de comandos de MSS
La secuencia de comandos de supervisión y la de copia de seguridad de IAS registran los siguientes tipos de sucesos en el registro de sucesos.

Tabla 8.5. Sucesos IAS devueltos por las secuencias de comandos de herramientas de IAS en esta solución

Suceso IAS	Importancia	Categoría del suceso	Origen del suceso	Id. de suceso
Copia de seguridad de IAS realizada	Copia de seguridad de la configuración de IAS en el archivo realizada correctamente.	Información	Operaciones de IAS	210
Ruta de la copia de seguridad de IAS no válida	Error en la copia de seguridad por haber especificado una ruta de destino no válida	Error	Operaciones de IAS	211
IAS no tiene acceso a la ruta de copia de seguridad	Error en la copia de seguridad porque los archivos no se pudieron escribir en la ruta de destino especificada.	Error	Operaciones de IAS	212
Restauración de IAS realizada	Configuración de IAS correctamente restaurada a	Información	Operaciones de IAS	220

	partir de la configuración guardada			
Error en la restauración de IAS	Error en la restauración de la configuración de IAS	Advertencia	Operaciones de IAS	221
Error en la consulta de directiva de IAS	No se pudo establecer contacto con IAS mediante la interfaz de objetos de datos de servidor. Puede que IAS no se esté ejecutando.	Error	Operaciones de IAS	230
Directivas de IAS no detectadas	IAS no contiene ninguna directiva de acceso remoto. Esto no debería suceder en un servidor IAS configurado de la forma habitual y, probablemente, indique la existencia de otro problema relacionado con IAS o con la red.	Error	Operaciones de IAS	231
IAS no instalado	IAS no está instalado en el equipo.	Error	Operaciones de IAS	232
IAS se ha detenido	El servicio IAS no se estaba ejecutando, pero se inició correctamente.	Advertencia	Operaciones de IAS	233
IAS no se está ejecutando	Error al intentar iniciar el servicio IAS	Error	Operaciones de IAS	234

Supervisión de la entidad emisora de certificados

La entidad emisora de certificados exige relativamente poca atención más allá de la supervisión del estado general del servidor y de la correcta realización de las copias de seguridad. En esta solución, la entidad emisora de certificados sólo es necesaria para tareas relativamente poco comunes como la emisión de certificados para servidores IAS nuevos y la renovación anual de certificados existentes. En definitiva, la entidad emisora de certificados no es un servicio fundamental.

La entidad emisora de certificados publica también una lista de los certificados que el administrador revoca. Esta lista, conocida como lista de revocación de certificados, se publica semanalmente en Active Directory. Dado que la entidad emisora de certificados emite un número pequeño de certificados, la lista de revocación de certificados también será pequeña y, por lo general, estará vacía. A pesar de esto, es importante que se publique en Active Directory de manera regular para que, así, las aplicaciones puedan comprobar el estado de revocación de todo certificado emitido por la entidad emisora. Por ejemplo, la propia entidad emisora de certificados tiene que comprobar el estado de revocación de cualquier certificado que emita antes de enviarlo a quien lo haya solicitado.

La secuencia de comandos de supervisión de la entidad comprueba que ésta está respondiendo a las solicitudes y que hay una lista de revocación de certificados disponible en Active Directory. Si se produce error en cualquiera de estas comprobaciones, la secuencia de comandos intentará reiniciar la entidad emisora de certificados. En caso de que el error se produzca en la lista, intentará igualmente publicar una nueva. Si el error se detecta incluso después de estos intentos de recuperación, se generará una alerta que se enviará por correo electrónico a la cuenta configurada y se escribirá en el registro de sucesos.

Habilitación de la supervisión de la entidad emisora de certificados

El siguiente procedimiento describe cómo configurar la secuencia de comandos de supervisión para que se ejecute como tarea programada de forma que, en caso de error, las alertas se emitan de forma automática y se intente la recuperación. Esta secuencia de comandos ha de ejecutarse sólo en el servidor de la entidad emisora de certificados.

Para configurar la secuencia de comandos de supervisión de la entidad emisora de certificados

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el siguiente comando para programar la ejecución de la secuencia de comandos cada noche a las 1:20 horas (se programa la ejecución a los 20 minutos después de la hora para compensar otras tareas programadas).

   SCHTASKS /Create /RU system /SC Hourly /TN "CA Check" /TR "\"C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools\msstools.cmd\" CheckCA" /ST 01:20

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea.

   Nota: adjuntar la ruta completa del archivo de secuencias de comandos msstools.cmd entre barras diagonales inversas (\) asegura que el shell de comandos de Windows no va a interpretar las comillas dobles ("), ni las va a quitar del comando. La ruta

que el programador de tareas almacena debe adjuntarse entre comillas si incluye espacios incrustados (como en "Archivos de programa"). El uso de una barra diagonal inversa (\) antes de las comillas (") garantiza que la ruta que el programador de tareas almacena se adjunte entre comillas dobles.

Sucesos de la entidad emisora registrados por las secuencias de comandos de MSS
La secuencia de comandos de supervisión de la entidad emisora de certificados registra lo siguiente en el registro de sucesos:

Tabla 8.6. Sucesos de la entidad emisora que las secuencias de comandos de supervisión de la entidad emisora de certificados devuelve en esta solución

Suceso de la entidad emisora	Importancia	Categoría del suceso	Origen del suceso	Id. de suceso
Lista de revocación de certificados caducada	No se puede obtener acceso a una lista de revocación de certificados válida, lo que actualmente provoca una pérdida del servicio.	Error	Operaciones de la entidad emisora	20
Lista de revocación de certificados atrasada	La lista de revocación de certificados aún es válida, pero existe una lista nueva atrasada que debería haberse publicado.	Error	Operaciones de la entidad emisora	21
No se puede recuperar la lista de revocación de certificados de Active Directory	Una lista de revocación de certificados no se encuentra disponible en un punto de distribución de lista de revocación de certificados publicada. Esto puede originar una pérdida de servicio.	Error	Operaciones de la entidad emisora	22
Los Servicios de Certificate Server no responden: Id. de suceso 1: interfaz de cliente sin conexión Id. de suceso 2: interfaz de administrador sin conexión	La interfaz de llamadas a procedimiento remoto (RPC) de los Servicios de Certificate Server está sin conexión y los certificados no pueden emitirse. Es posible que sea necesario reiniciar el servicio.	Error	Operaciones de la entidad emisora	1 y 2
Otros sucesos	Error en la ejecución de la secuencia de comandos de supervisión de la entidad emisora	Error	Operaciones de la entidad emisora	100

Administración de cambios

Las tareas de esta sección hacen referencia a los cambios que posiblemente necesite para configurar la infraestructura de seguridad de WLAN.

Administración de actualizaciones de seguridad de Windows

Tanto las actualizaciones de IAS como las de los Servicios de Certificate Server están incluidas en los paquetes y revisiones de servicios básicos para Windows Server 2003. No necesita actualizar estos componentes por separado.

Debería leer esta guía y seguir las referencias facilitadas en la sección "Actualizaciones de seguridad del servidor" del capítulo 3, "Preparación del entorno".

Administración de cambios en los servidores IAS

En el capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas", se recomendaba designar uno de los servidores IAS como el servidor "maestro", servidor en el que realizaría los cambios en la configuración de IAS (consulte la sección "Implementación de la configuración en varios servidores IAS" del capítulo 5). Estos cambios se replicarían a los otros servidores de la organización mediante exportaciones e importaciones de la base de datos de la configuración de IAS automatizadas; así, se aseguraría la consistencia de la configuración en toda la infraestructura de IAS.

No obstante, el conjunto de clientes RADIUS (los puntos de acceso inalámbrico) configurado en cada IAS no se replica normalmente. Los puntos de acceso admitidos por cada servidor pueden variar sustancialmente y raro sería el caso en que dos servidores IAS tuvieran exactamente el mismo conjunto de clientes. Esto puede suceder, por ejemplo, si tiene dos servidores IAS centrales para atender todos los puntos de acceso inalámbrico de la organización.

Creación de copias de seguridad de la configuración IAS antes de realizar cambios

Aunque haya programado copias de seguridad de los servidores para cada noche, resulta muy conveniente realizar una copia de seguridad manual del IAS antes de realizar cambios en los servidores. Esto le permitirá deshacer cualquier cambio y restaurar el estado del servidor a aquél inmediatamente anterior a los cambios realizados. El siguiente procedimiento se sirve de la secuencia de comandos

de la creación de copias de seguridad para exportar la configuración del servidor, directivas, la configuración del registro y clientes RADIUS.

Para crear copias de seguridad de la configuración de IAS

1. Abra un shell de comandos en el servidor utilizando el acceso directo de **MSS WLAN Tools** e introduzca el siguiente comando para crear una carpeta en la que guardar el archivo de exportación de IAS:

   md c:\IASSaveState

   La configuración de IAS suele ser menor de 100 KB y se puede guardar en la unidad del sistema, tal y como se muestra en el ejemplo. No obstante, se puede utilizar cualquier ruta siempre y cuando se use de forma coherente en este comando y en los posteriores.

2. Utilice el siguiente comando para establecer permisos para la carpeta de forma que sólo los administradores y operadores de copias de seguridad puedan leer y modificar el contenido:

   cacls c:\IASSaveState /G system:F administrators:F "Backup Operators":C

   Es probable que este comando se divida en varias líneas en este documento, pero debe escribirlo como una sola línea.

3. Para exportar la configuración de IAS, ejecute la secuencia de comandos de creación de copias de seguridad mediante el siguiente comando:

   MSSTools BackupIAS /path:C:\IASSaveState

Replicación de la configuración en otros servidores IAS
Debe establecer un procedimiento propio repetitivo para garantizar que la configuración del servidor maestro se replique en el resto de servidores IAS de la organización. Es posible que esto implique ordenar al personal de soporte local que importe la configuración. Lo más normal es que este procedimiento se realice de forma remota copiando los archivos de configuración y utilizando una sesión en el escritorio remoto con el objetivo de ejecutar la secuencia de comandos para importar la configuración.

Para replicar la configuración en otros servidores IAS, siga los procedimientos descritos en la sección "Replicación de la configuración desde el servidor IAS principal" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

Nota: es probable que encuentre útil incrustar un número de versión en el nombre de la directiva de acceso remoto para que sea fácil comprobar que todos los servidores IAS tienen la misma versión de configuración.

Adición de servidores IAS al entorno

Antes de instalar un nuevo servidor IAS, debe identificar los puntos de acceso inalámbrico que configurará como clientes de este servidor. Para ello, siga las instrucciones facilitadas en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". Asimismo, necesitará otro servidor IAS configurado como el servidor RADIUS secundario para proporcionar resistencia a los puntos de acceso en caso de error en el servidor. Si está reconfigurando los puntos de acceso existentes para utilizar este nuevo servidor, deberá planear la migración con detenimiento a fin de evitar trastornos en el servicio para los usuarios durante el cambio de puntos de acceso. Normalmente no se producirán trastornos, siempre y cuando un punto de acceso tenga, al menos, un servidor RADIUS de autenticación activo.

Para instalar IAS en un servidor nuevo

1. Para preparar el servidor, siga las instrucciones del capítulo 3, "Preparación del entorno".

2. Siga las instrucciones de las secciones "Instalación de IAS" y "Registro de IAS en Active Directory" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

3. Para replicar los cambios desde el servidor IAS maestro al servidor nuevo, siga el procedimiento descrito en la sección "Replicación de la configuración desde el servidor IAS principal" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

4. Por último, agregue las entradas de cliente RADIUS para los puntos de acceso a IAS inalámbricos y configure dichos puntos de acceso para utilizar el nuevo servidor IAS.

Adición de puntos de acceso inalámbrico a la red

Para agregar un nuevo punto de acceso inalámbrico, debe completar las dos tareas siguientes:

1. Agregue el punto de acceso como cliente RADIUS al servidor IAS principal y al secundario.

2. Configure el punto de acceso para usar los servidores IAS como servidores RADIUS principal y secundario.

Los servidores IAS elegidos como servidores RADIUS principal y secundario dependerán de la ubicación del punto de acceso en la red. Lo ideal es elegir un servidor IAS principal que esté en la misma LAN que el punto de acceso o que tenga, al menos, una conectividad al punto de acceso confiable. Elija un servidor IAS secundario con una conectividad al punto de acceso confiable. Para obtener más información, consulte las instrucciones facilitadas en la sección "Asignación de puntos de acceso a servidores RADIUS" del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas".

Una vez identificados los servidores IAS adecuados para el punto de acceso, lleve a cabo los siguientes procedimientos , que son los

mismos descritos para agregar un punto de acceso a IAS en el capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

Para agregar un punto de acceso a la red

1. Para agregar el punto de acceso como cliente RADIUS al IAS principal, siga el procedimiento descrito en la sección "Adición de puntos de acceso al servidor IAS principal" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".
2. Para agregar el punto de acceso como cliente RADIUS al IAS secundario, siga el procedimiento descrito en la sección "Importación de puntos de acceso en el servidor IAS secundario" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".
3. Configure el punto de acceso siguiendo las instrucciones proporcionadas en la sección "Configuración de puntos de acceso inalámbrico" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

Eliminación de un punto de acceso inalámbrico

Si está volviendo a ubicar y organizar los sitios, es probable que necesite quitar un punto de acceso inalámbrico de la red. Es recomendable quitar siempre del servidor IAS aquellas entradas de cliente RADIUS que ya no estén en uso.

Para quitar un punto de acceso inalámbrico de la red

1. Identifique los servidores IAS principal y secundario de los que hay que quitar el punto de acceso.
2. Utilice la MMC del **Servicio de autenticación de Internet** para eliminar la entrada del cliente RADIUS del punto de acceso. Compruebe que la IP del cliente RADIUS coincide con la dirección IP del punto de acceso retirado. No tome como referencia el nombre del cliente RADIUS.
3. Repita el paso 2 en el servidor IAS secundario.

Concesión del acceso a WLAN a un usuario o equipo

Si ha seguido la configuración predeterminada de esta solución, todos los usuarios y equipos del dominio en el que haya instalado los servidores IAS tendrán acceso automático a la WLAN. Esto se debe a que los grupos de usuarios y de equipos de dominio son miembros de los grupos de usuarios y de equipos respectivos de la LAN inalámbrica. Estos grupos pertenecen, a su vez, al grupo de acceso a LAN inálambrica, que la directiva de acceso remoto IAS usa para conceder acceso a la WLAN.

Control del acceso para miembros del mismo dominio

Si desea controlar explícitamente qué usuarios y equipos se pueden conectar a la WLAN, deberá recurrir a grupos de seguridad para administrar el acceso. Debe eliminar los grupos de usuarios y equipos de dominio de los respectivos grupos de usuarios y equipos de la LAN inalámbrica para, a continuación, agregar los usuarios y los equipos específicos a los que desee otorgar acceso a WLAN.

Si procede de este modo, modificará la configuración predeterminada de la solución, de forma que WLAN se torna inaccesible para todos, a menos que se conceda acceso explícito mediante la adición al grupo de seguridad. Se trata de un enfoque más prudente que el de "permitir de forma predeterminada" y, por lo general, las organizaciones con necesidades de alta seguridad se decantan por él. También puede resultar útil en los casos en los que sólo un número limitado de personas tiene acceso a la WLAN. Un ejemplo podría ser la fase piloto de una instalación mayor.

Para habilitar el acceso a WLAN de un usuario o un equipo en el mismo dominio

1. Con **Usuarios y equipos de Active Directory**, agregue la cuenta de usuario o de equipo al grupo de usuarios o equipos de LAN inalámbrica.
2. Si está agregando un usuario, pida al usuario que cierre la sesión y la vuelva a iniciar. Si está agregando un equipo, reinícielo.
3. Compruebe que el usuario o el equipo puedan tener acceso a WLAN.

Control del acceso para miembros de otro dominio

Si tiene un bosque con varios dominios, es probable que desee permitir que usuarios y equipos de otros dominios utilicen la WLAN. Para ello, necesita iniciar sesión utilizando una de las cuentas siguientes:

- Un administrador de ambos dominios.
- Una cuenta con permisos para crear grupos en otros dominios y para modificar los miembros del grupo de acceso a WLAN en el dominio principal; es decir, el dominio en el que están instalados los servidores IAS.

Para conceder acceso a WLAN a los usuarios y equipos de otros dominios

1. Inicie sesión con una cuenta que tenga permisos para crear grupos en el dominio al que pertenecen los usuarios y equipos a los que quiere conceder acceso a WLAN (el dominio de destino).
2. Abra **Usuarios y equipos de Active Directory** y céntrese en un controlador de dominio para el dominio de destino.
3. Cree un grupo global de dominio llamado Usuarios de LAN inalámbrica en el dominio de destino.
4. Cree un grupo global de dominio llamado Equipos de LAN inalámbrica en el dominio de destino.

   Inicie sesión con una cuenta que tenga permisos para modificar la pertenencia al grupo de acceso a LAN inalámbrica en el

5. dominio principal. Con **Usuarios y equipos de Active Directory**, busque el grupo de acceso a LAN inalámbrica y ábralo para modificar sus propiedades. Desde la ficha **Pertenencia** de las propiedades del grupo, agregue desde el dominio de destino los grupos Usuarios de LAN inalámbrica y Equipos de LAN inalámbrica como miembros de este grupo.

6. Identifique a los usuarios del dominio de destino que requieren acceso a WLAN. Agregue sus cuentas al grupo Usuarios de LAN inalámbrica de ese dominio. Del mismo modo, agregue las cuentas de equipos necesarias del dominio de destino al grupo Equipos de LAN inalámbrica de dicho dominio. Otra forma consiste en agregar a los Usuarios del dominio y Equipos del dominio a estos grupos para conceder acceso a WLAN a todos los miembros del dominio de destino.

Denegación del acceso a WLAN a un usuario o equipo

La configuración predeterminada de esta solución concede acceso a WLAN a todos los usuarios y equipos del dominio en el que se han instalado los servidores IAS. Este acceso se concede automáticamente porque son miembros de los grupos Usuarios del dominio y Equipos del dominio respectivamente. Esto puede acarrear problemas si necesita bloquear el acceso a WLAN para usuarios o equipos individuales. No debe quitar usuarios o equipos de los grupos de Usuarios del dominio y Equipos del dominio integrados; en vez de ello, utilice una de las siguientes estrategias:

- Si el usuario ha dejado la organización (o, en el caso de un equipo, si se ha perdido o lo han robado), puede deshabilitar la cuenta de dicho usuario o equipo en Active Directory.
- Administre el acceso mediante los permisos de acceso remoto en el objeto de cuenta de usuario o de equipo para permitir o denegar el acceso. Esto se ha analizado brevemente en la sección "Acceso de los usuarios y los equipos a la WLAN" del capítulo 6, "Configuración de clientes de LAN inalámbricas".
- Si desea eliminar el acceso a WLAN de un usuario o equipo pero seguir permitiendo que la cuenta se utilice para el acceso normal al dominio o a otras redes, tendrá que utilizar un modelo WLAN de acceso selectivo, o bien implementar una directiva de acceso remoto "Denegar". La opción elegida dependerá de si desea que el acceso a WLAN se conceda de forma predeterminada, o bien que se deniegue de forma predeterminada y que se conceda sólo a los usuarios especificados.
  - El uso de la pertenencia a un grupo específico para implementar una directiva de acceso selectivo ya se ha descrito anteriormente en el capítulo, en el procedimiento "Concesión del acceso a WLAN a un usuario o equipo". Puede denegar el acceso a WLAN sólo con quitar a un usuario o equipo del grupo de seguridad pertinente.
  - El siguiente procedimiento, "Control del acceso a WLAN mediante una directiva de denegación", describe la creación de una directiva de acceso remoto de IAS para denegar el acceso a los grupos seleccionados.

    Importante: no debe quitar usuarios o equipos de los grupos Usuarios del Dominio o Equipos del dominio respectivamente. Aunque técnicamente es posible, si lo hace impedirá que la cuenta de usuario o equipo funcione correctamente en el uso normal del dominio.

Control del acceso a WLAN mediante una directiva de denegación

Si desea permitir el acceso de forma predeterminada, pero poder denegarlo a usuarios y equipos individuales como excepción, habrá de crear una directiva de acceso remoto "Denegar" en IAS.

Para crear una directiva de acceso remoto de denegación

1. En **Usuarios y equipos de Active Directory**, cree un grupo universal llamado Denegar acceso a LAN inalámbrica.
2. Cree los grupos globales de dominio Denegar usuarios de LAN inalámbrica y Denegar equipos de LAN inalámbrica y agréguelos como miembros del grupo Denegar acceso a LAN inalámbrica.
3. Inicie sesión en el servidor IAS maestro que utiliza para editar la configuración de IAS global, configuración que se replicará más tarde en los otros servidores IAS.
4. En la MMC del **Servicio de autenticación de Internet**, haga clic con el botón secundario en la carpeta **Directivas de acceso remoto** y seleccione **Nueva directiva de acceso remoto**.
5. Seleccione **Configurar una directiva personalizada** y escriba **Denegar acceso a LAN inalámbrica** como nombre de la directiva. Haga clic en **Siguiente** para continuar.
6. Haga clic en **Agregar** para agregar una condición de directiva. Seleccione **Grupos de Windows** de la lista y haga clic en **Agregar**.
7. Haga clic en **Agregar** para agregar un grupo de seguridad. Escriba (o busque) el grupo Denegar acceso a LAN inalámbrica y haga clic en **Aceptar**.
8. Haga clic en **Agregar** para agregar condición de directiva distinta. Seleccione **Tipo de puerto NAS** de la lista y haga clic en **Agregar**.
9. De la lista de **Tipos disponibles**, seleccione **Inalámbrica - IEEE 802.11** y haga clic en **Agregar >>**. A continuación, seleccione **Inalámbrica - Otra** y haga clic en **Agregar >>** para agregarlas a la lista **Tipos seleccionados**. Haga clic en **Aceptar** para concluir y en **Siguiente** para continuar.
10. Seleccione **Denegar permiso de acceso remoto** y haga clic en **Siguiente** para continuar.

11. En la pantalla **Perfil**, haga clic en **Siguiente** para omitirla y, a continuación, haga clic en **Finalizar** para concluir.

12. La directiva **Denegar acceso a LAN inalámbrica** se debe crear al principio de la lista de directivas como prioridad más alta o, al menos, por encima de la directiva Permitir acceso a LAN inalámbrica. Si no es así, haga clic con el botón secundario en el nombre de la directiva y haga clic en **Subir** hasta que ocupe un lugar anterior en la lista al de la directiva **Permitir acceso a LAN inalámbrica**.

13. Utilice los procedimientos descritos anteriormente para replicar la nueva configuración en los otros servidores IAS de la organización.

Se rechazará el acceso a WLAN a todo usuario o equipo que agregue a los grupos Denegar usuarios de LAN inalámbrica o Denegar equipos de LAN inalámbrica. No obstante, esta configuración sólo surtirá efecto la próxima vez que inicie sesión el usuario denegado o cuando se reinicie el equipo denegado.

Tareas de soporte técnico

Esta sección cubre las tareas más comunes que necesita realizar para solucionar los problemas en la infraestructura de seguridad de WLAN. La sección "Solución de problemas" de este capítulo hace referencia a muchas de estas tareas.

Restauración de la configuración de un servidor IAS a partir de copias de seguridad

Las directivas y configuración de IAS se almacenan en la base de datos de configuración de IAS. Éstas se pueden restaurar independientemente del resto de la configuración del sistema. Debe programar la tarea de creación de copias de seguridad de IAS para realizar estas copias cada noche en la carpeta C:\IASBackup. Para obtener más información sobre este tema, consulte el procedimiento "Configuración de la copia de seguridad de IAS" en la sección "Tareas operativas" de este capítulo. Si ha de deshacer los cambios aplicados ese día, puede restaurar la configuración a partir de los archivos de las copias de seguridad (en C:\IASBackup) creados la noche anterior, o a partir de la copia de seguridad de reversión realizada antes de hacer los cambios. Para obtener más detalles, consulte el procedimiento "Creación de copias de seguridad de la configuración IAS antes de realizar cambios" en la sección "Administración de cambios".

Si necesita restaurar una versión anterior de la configuración, ha de recuperar de la copia de seguridad del servidor la configuración de IAS exportada.

Advertencia: este procedimiento restaurará la configuración de IAS completa (incluidos los clientes RADIUS) y sobrescribirá la configuración existente en el servidor. La copia de seguridad que intenta restaurar debe provenir del mismo servidor.

Para restaurar la configuración de IAS

1. Si los archivos de copia de seguridad de la configuración de IAS que desea utilizar no se encuentran en el servidor, deberá restaurarlos a partir de medios de copia de seguridad. Asegúrese de seleccionar en la carpeta IASBackup sólo los archivos que hay que restaurar. No restaure el estado del sistema, a no ser que también desee revertir a una configuración del sistema anterior.

2. Utilice el acceso directo **MSS WLAN Tools** para abrir un shell de comandos. Para restaurar la configuración de IAS, ejecute el siguiente comando:

   msstools RestoreIAS /path:C:\IASBackup

3. Para comprobar que la configuración de IAS se ha restaurado, abra la consola de administración de IAS y compruebe los clientes RADIUS y las carpetas de directivas de acceso remoto.

Si, por cualquier razón, no dispone de ninguna copia de seguridad de este sistema utilizable, puede exportar la configuración desde otro servidor IAS e importarla a éste. Normalmente, los servidores IAS con la misma función comparten los mismos valores de configuración, pero cuentan con un conjunto distinto de clientes RADIUS. Por esta razón, no debe utilizar este procedimiento para restaurar la configuración desde otro servidor. En su lugar, recurra al procedimiento "Replicación de la configuración desde el servidor IAS principal" del capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas".

Importante: debe asegurarse de que el sistema restaurado está actualizado, ya que, dado que se ha restaurado a partir de una copia de seguridad antigua, puede que las revisiones previamente aplicadas se hayan deshecho.

Restauración de la configuración completa del servidor a partir de copias de seguridad

Los procedimientos para restaurar el servidor variarán en función del sistema de copia de seguridad elegido. Los procedimientos que siguen se basan en el supuesto de que ha realizado la copia de seguridad del sistema mediante la creación de una copia de seguridad del estado del sistema de Windows en un archivo, seguida de una copia de seguridad de este archivo y de otros archivos necesarios.

Para restaurar el servidor

1. Según sea el estado del servidor, es posible que necesite preparar el servidor desde el principio, y así, cuando un error grave del hardware ha destruido los discos de sistema del servidor. Si no es el caso, puede realizar la restauración directamente sin reinstalar el sistema operativo.

2. En caso de usar copias de seguridad del estado del sistema y de los archivos por separado, utilice el software de copias de seguridad para restaurar los archivos de las copias de seguridad del estado del sistema y los de la configuración de IAS desde el medio de copia de seguridad al servidor. La configuración de IAS se debe restaurar en la misma ruta, que es C:\IASBackup.

3. Ejecute la utilidad de copias de seguridad de Windows y seleccione el archivo de la copia de seguridad del estado del sistema restaurado. Deberá pertenecer a un grupo que posea derechos de creación de copias de seguridad y restauración en el equipo (como Operadores de copia de seguridad o Administradores).
4. Haga clic en **Restaurar**.
5. Reinicie el sistema.
6. Compruebe que todo funciona según lo esperado y que Active Directory y los Servicios de Certificate Server, si se han instalado, se han iniciado sin errores.
7. Utilice el acceso directo **MSS WLANTools** para abrir un shell de comandos. Para restaurar la configuración de IAS, ejecute el siguiente comando:

   MSSTools RestoreIAS /path:C:\IASBackup
8. Para comprobar que la configuración de IAS se ha restaurado, abra la consola de administración de IAS y compruebe los clientes RADIUS y las carpetas de directivas de acceso remoto.

   Importante: si IAS se está ejecutando en un controlador de dominio, al restaurar una copia de seguridad del estado del sistema, se restaurará en ese servidor la versión de la base de datos de Active Directory de la que se había realizado una copia de seguridad. No obstante, todo cambio realizado en Active Directory con posterioridad a la copia de seguridad se replicará en el servidor restaurado en el siguiente ciclo de replicación de Active Directory.

Tareas de optimización

Esta sección cubre las tareas relevantes para optimizar la ejecución de la infraestructura de IAS.

Determinación de la carga máxima del servidor IAS

En esta sección se ofrece información sobre la posible carga máxima del servidor IAS.

Los problemas de rendimiento en servidores IAS con la configuración y el tamaño correctos son muy poco frecuentes. Los servidores IAS se encuentran bajo una mayor carga durante horas de mayor demanda como, por ejemplo, las mañanas (cuando muchos usuarios inician la sesión a la vez), poco después de una interrupción de la actividad de la red, o bien cuando se produce un error del servidor RADIUS en el que los puntos de acceso inalámbrico conmutan por error a un servidor de copia de seguridad.

La siguiente tabla recoge indicaciones de los requisitos de autenticación WLAN para diversos tamaños de organización.

Tabla 8.7. Requisitos de autenticación WLAN

Número de usuarios de WLAN	Nuevas autenticaciones por segundo	Nuevas autenticaciones por segundo en hora máxima	Reautenticaciones por segundo
100	> 0,1	0,1	0,1
1000	0,1	0,6	1,1
10.000	1,4	5,6	11,1

La columna Nuevas autenticaciones por segundo forma parte de la carga fija; en ella, se supone una media de cuatro autenticaciones nuevas completas, dado que los usuarios se desplazan por los puntos de acceso inalámbrico. La columna Nuevas autenticaciones por segundo en hora máxima señala el tipo de carga que se espera cuando todos los usuarios se deben autenticar en un período de 30 minutos (por ejemplo, al inicio del día). La columna Reautenticaciones por segundo contempla el número de autenticaciones con reconexiones rápidas que tienen lugar cuando IAS obliga a establecer un tiempo de espera de sesión transcurridos 15 minutos. Aunque el tiempo de espera predeterminado en la solución es de 60 minutos, se usa la opción de 15 minutos para ponerse en el peor de los casos. Debe evaluar estas cifras frente a las necesidades de su propia organización para determinar qué tipo de carga necesita admitir.

Las pruebas internas realizadas por Microsoft muestran que IAS puede admitir una carga elevada con un hardware modesto. La carga admitida por IAS se representa mejor con el número de autenticaciones Protocolo de autenticación extensible (EAP) por segundo. La tabla siguiente contempla los resultados de un servidor IAS ejecutado en un servidor Intel Pentium 4 a 2GHz con Windows Server 2003.

Las pruebas se llevaron a cabo con el registro de RADIUS activado (en un disco aparte) y con IAS en un servidor distinto al del controlador de dominio de Active Directory. Por tanto, estas cifras se deben considerar como el peor de los casos. La configuración predeterminada de esta solución presenta el registro desactivado e IAS instalado en el mismo servidor que el controlador de dominio. Ambos elementos mejorarán el rendimiento de la autenticación.

Nota: esta información se ofrece sin garantía alguna de exactitud y sólo se debe utilizar como orientación con objeto de planear la capacidad y no para realizar comparaciones de rendimiento.

Tabla 8.8. Ejemplo de medidas de la capacidad del servidor IAS

Tipo de autenticación	Autenticaciones por segundo

Nuevas autenticaciones con el nuevo protocolo de autenticación extensible protegido (PEAP)	36
Nuevas autenticaciones PEAP con compatibilidad para tarjetas de descarga de TLS/SSL	50
Autenticaciones con reconexión rápida	166

IAS se puede configurar para generar registros de RADIUS basados en el disco que contengan diversos volúmenes de información sobre solicitudes de RADIUS. Si opta por activar el registro de RADIUS, tendrá que considerar los costes generales que supondrá para los servidores, sobre todo, en los subsistemas de discos. El bajo rendimiento del disco actuará como un cuello de botella para el rendimiento de IAS y retrasará las repuestas RADIUS de IAS a los puntos de acceso. Esto conducirá a tiempos de espera del protocolo y a conmutaciones innecesarias de puntos de acceso en servidores RADIUS secundarios. Si espera una carga elevada (puede utilizar las cifras de las tablas anteriores como orientación) y va a activar el registro de RADIUS, se debe asegurar de que IAS está configurado para escribir registros RADIUS en un disco de alto rendimiento distinto del de la unidad del sistema de Windows y del de los archivos de paginación.

La habilitación de las características de seguimiento en IAS de Windows Server 2003 (como se describe en la sección "Habilitación y deshabilitación del seguimiento en el servidor IAS" de este capítulo) también generará carga adicional en los servidores IAS. Estas características pueden ser necesarias de vez en cuando para solucionar problemas relacionados con el acceso a la red, pero no deberían estar habilitadas de forma permanente. No obstante, es posible que desee asegurarse de que los servidores IAS disponen de algún espacio adicional para permitir el seguimiento durante períodos de tiempo determinados y seguir atendiendo la carga de producción.

Otras medidas de optimización

Para obtener más información sobre la optimización de IAS, consulte la sección sobre el diseño de una solución de IAS optimizada en el capítulo dedicado a la implementación de IAS del *Kit de distribución de Microsoft Windows Server 2003*.

Principio de la página

Solución de problemas

Esta sección contiene procedimientos y técnicas que ayudan a diagnosticar y solucionar problemas relacionados con la solución de LAN inalámbrica.

Procedimientos para la solución de problemas

Los siguientes procedimientos facilitan la identificación de las posibles causas de un problema y la acción necesaria para resolverlo. Esta sección se organiza de forma jerárquica. El primer procedimiento, "Determinación del tipo de problema", le indicará uno de varios procedimientos, cada uno de los cuales se desglosa en pasos detallados para la solución del problema. Estos procedimientos, a su vez, pueden apuntar hacia otros procedimientos centrados en un componente particular de la solución.

Cada uno de estos procedimientos se describe en detalle más adelante en este mismo capítulo. Algunos de ellos se presentan en forma gráfica; otros aparecen en tablas o texto por exigir una descripción demasiado extensa para una figura. Alguno de estos procedimientos recurre a la sección "Herramientas y técnicas para la solución de problemas" de este capítulo. Se debe familiarizar con dicha sección para utilizar estos procedimientos de forma eficaz.

Importante: estos procedimientos de diagnóstico no cubren todos los casos. En aquellos casos en los que los pasos de investigación recomendados no le conduzcan al origen del problema, debe volver hacia atrás y seguir otro de los procedimientos de diagnóstico. En algunas ocasiones, no advertirá el alcance completo o la naturaleza de los síntomas, lo que puede conducirle por el camino erróneo. Por ejemplo, es posible que un usuario sea la única persona de una oficina encargada de comunicar un problema que afecta a toda la oficina. Aunque la tabla indique los procedimientos de diagnóstico relacionados con los errores de un único cliente, es probable que otros procedimientos sean más adecuados.

Además, debe consultar los documentos sobre la solución de problemas en WLAN e IAS enumerados al término del capítulo.

Determinación del tipo de problema

Comience por clasificar el tipo de problema que ha surgido con ayuda del diagrama de flujo siguiente. Los rombos representan preguntas o puntos de decisión, mientras que los rectángulos muestran el diagnóstico del problema e indican el nombre del procedimiento que hay que seguir.

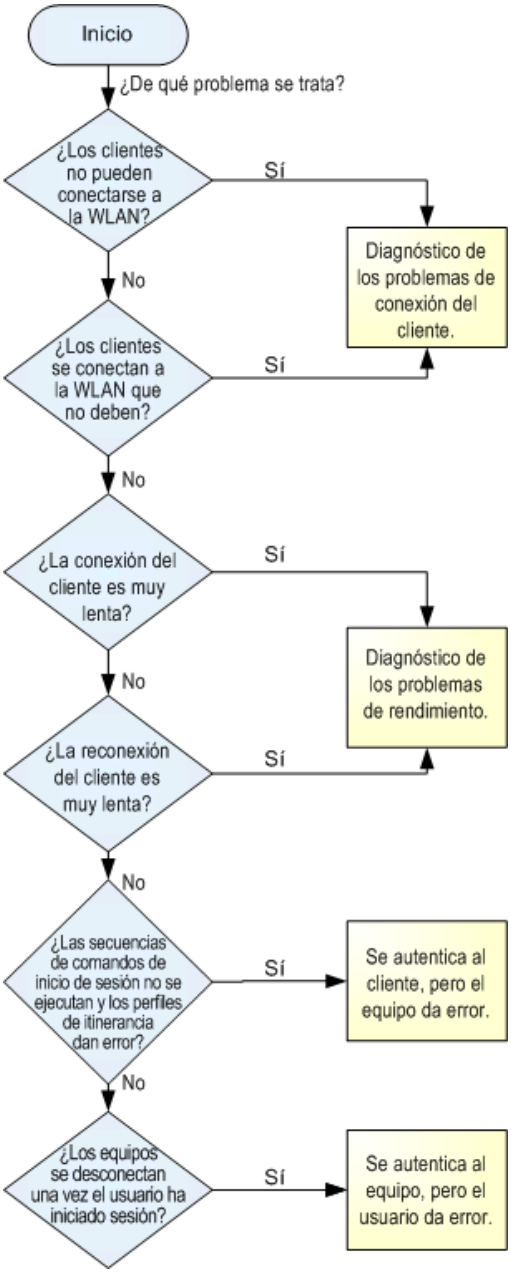

Figura 8.1. Determinación del tipo de problema

Diagnóstico de los problemas de conexión del cliente

La siguiente tabla clasifica los distintos tipos de problemas de conexión basados en el número y en la ubicación de los clientes afectados. La columna Posible(s) problema(s) refleja los factores que pueden producir los síntomas señalados con mayor probabilidad. La columna Procedimientos de diagnóstico que seguir contiene los procedimientos de diagnóstico a los que debe recurrir en primer lugar para diagnosticar el problema. Más adelante podrá encontrar una descripción detallada de cada uno de estos procedimientos.

Tabla 8.9. ¿Quién no puede conectarse a la WLAN?

Síntoma	Posible(s) problema(s)	Procedimientos de diagnóstico que seguir
Un único cliente	Configuración del equipo o cuenta del usuario/equipo	Comprobar cuenta de usuario/equipo Comprobar el equipo cliente
Varios clientes en un sitio	Configuración incorrecta de uno o varios puntos de acceso	Comprobar configuración de puntos de acceso inalámbrico
Todo un sitio (IAS local)	Funcionamiento o configuración incorrecta del	

	servidor IAS en este sitio; problemas de replicación en Active Directory que impiden al controlador de dominio recibir información correcta; funcionamiento incorrecto del servidor IAS asociados a problemas de conectividad de WLAN.	Comprobar Active Directory y Servicios de red Comprobar IAS Comprobar conectividad WAN
Todo un sitio (IAS no local)	Problemas de conectividad con WLAN; problemas de replicación en Active Directory (si se trata del controlador de dominio local).	Comprobar conectividad WAN
Todos los clientes en todos los sitios	Configuración de la organización (objeto de directiva de grupo de la configuración del cliente, grupos con la directiva de acceso remoto, errores en la renovación de certificados).	Comprobar Active Directory y Servicios de red (comprobaciones "Comprobar objetos de directiva de grupo de la configuración de WLAN y "Comprobar grupos de Active Directory"). Comprobar la entidad emisora de certificados Comprobar IAS

Diagnóstico de los problemas de rendimiento

Esta sección se centra en los problemas de rendimiento asociados con la infraestructura de seguridad de WLAN. En este capítulo no se tratan los problemas generales de rendimiento de la red inalámbrica y con cable.

Tabla 8.10. Problemas de rendimiento

Síntoma	Posible solución
Demora en la autenticación que afecta a muchos usuarios	El servidor IAS está muy cargado, compruebe el monitor de rendimiento.
	Autenticación a través de un vínculo WLAN lento (incluso si un IAS local ha comprobado que los puntos de acceso no han producido errores al conectarse con el IAS remoto).
	Las demoras con un servidor Protocolo de configuración dinámica de host (DHCP) al emitir una dirección IP puede afectar al tiempo total de conexión.
Demora en la reautenticación mientras se desplaza entre puntos de acceso	Un retraso de pocos segundos es normal cuando se cambia de punto de acceso.
	Si un cliente se sale del alcance de un punto de acceso (y permanece fuera más de 10 segundos), puede necesitar hasta 60 segundos para que se inicie la reautenticación una vez vuelva a hallarse al alcance de un punto de acceso. Esto ocurre porque, al desconectarse de una WLAN, el cliente WLAN con Windows sólo busca las WLAN disponibles cada 60 segundos.
El rendimiento de la red WLAN es bajo	El origen de este síntoma puede ser la existencia de demasiados clientes que utilizan pocos puntos de acceso, la colocación incorrecta de los puntos de acceso o señales de radio débiles debido a la obstrucción o a una distancia excesiva. Todos estos aspectos pertenecen al diseño de la red WLAN y se encuentran fuera del alcance de este documento. Para recibir algún tipo de consejo, debe consultar a su proveedor o al proveedor de la solución. Para obtener más información, consulte el capítulo sobre la implementación de LAN inalámbricas del *Kit de distribución de Microsoft Windows Server 2003*.

Se autentica al cliente, pero el equipo da error

Esta solución recurre a la autenticación tanto del usuario como del equipo a la WLAN. Las credenciales de dominio del equipo se utilizan para autenticar a la WLAN cuando ningún usuario ha iniciado sesión en el equipo. Cuando un usuario inicia sesión, se utilizan las credenciales de éste para volver a autenticar a la WLAN. Este mecanismo hace posible que el equipo se comunique con la WLAN incluso cuando nadie haya iniciado sesión, al tiempo que permite administrar el equipo de forma remota, descargar la configuración de los objetos de directiva de grupo del servidor, etc.

Cuando un usuario inicia sesión en un equipo WLAN, se produce una pequeña demora mientras el usuario se autentica a la WLAN. Hasta que el usuario está debidamente autorizado para conectarse, la sesión WLAN autenticada del equipo aún se encuentra activa. No obstante, si el equipo no se pudo autenticar, esta demora significa que no existe conectividad con la red al comienzo del inicio de sesión

del usuario.

Esto puede originar una serie de problemas delicados. Por ejemplo, no se cargarán los perfiles de itinerancia del usuario, no se aplicarán algunas configuraciones de objetos de directiva de grupo y no se implementarán las secuencias de comandos de inicio de sesión del usuario ni el software basado en objetos de directiva de grupo (ambos elementos se ejecutan muy pronto en el proceso de inicio de sesión).

Para determinar el origen del error en la autenticación del equipo, debe seguir el procedimiento "Comprobar cuenta de usuario/equipo" descrito más adelante en esta guía.

Se autentica al equipo, pero el usuario da error
A diferencia del caso anterior, este problema se percibe inmediatamente y se pondrá en conocimiento de los usuarios afectados de inmediato. Para determinar el origen del error en la autenticación del usuario, debe seguir el procedimiento "Comprobar cuenta de usuario/equipo".

Procedimientos de diagnóstico
La siguiente sección ofrece una serie de pasos detallados para la solución de problemas a los que se ha hecho mención en secciones anteriores.

Comprobar cuenta de usuario/equipo
El siguiente diagrama de flujo le ayudará a diagnosticar la causa de un error en la autenticación de usuarios o equipos.

Nota: el cuadro con forma de flecha del diagrama de flujo indica que debería consultar el procedimiento "Comprobar el equipo cliente", tal y como se especifica en el cuadro.

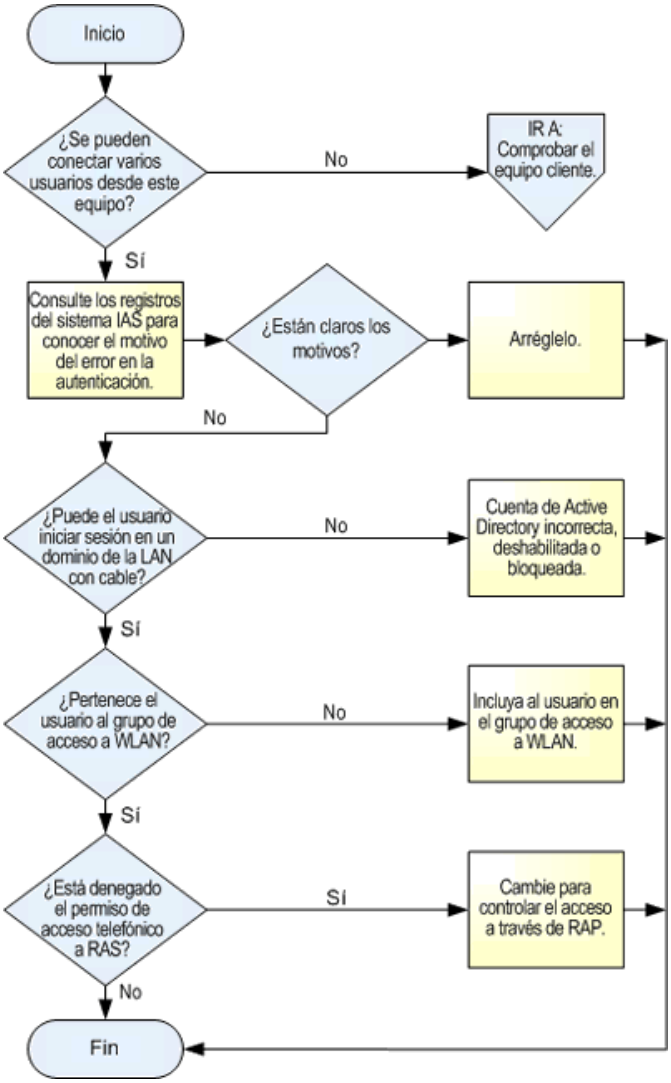

Figura 8.2. Comprobación de la cuenta del usuario o equipo
Vista de imagen a pantalla completa

Comprobar el equipo cliente

El siguiente diagrama de flujo ayuda a diagnosticar los problemas con el equipo cliente.

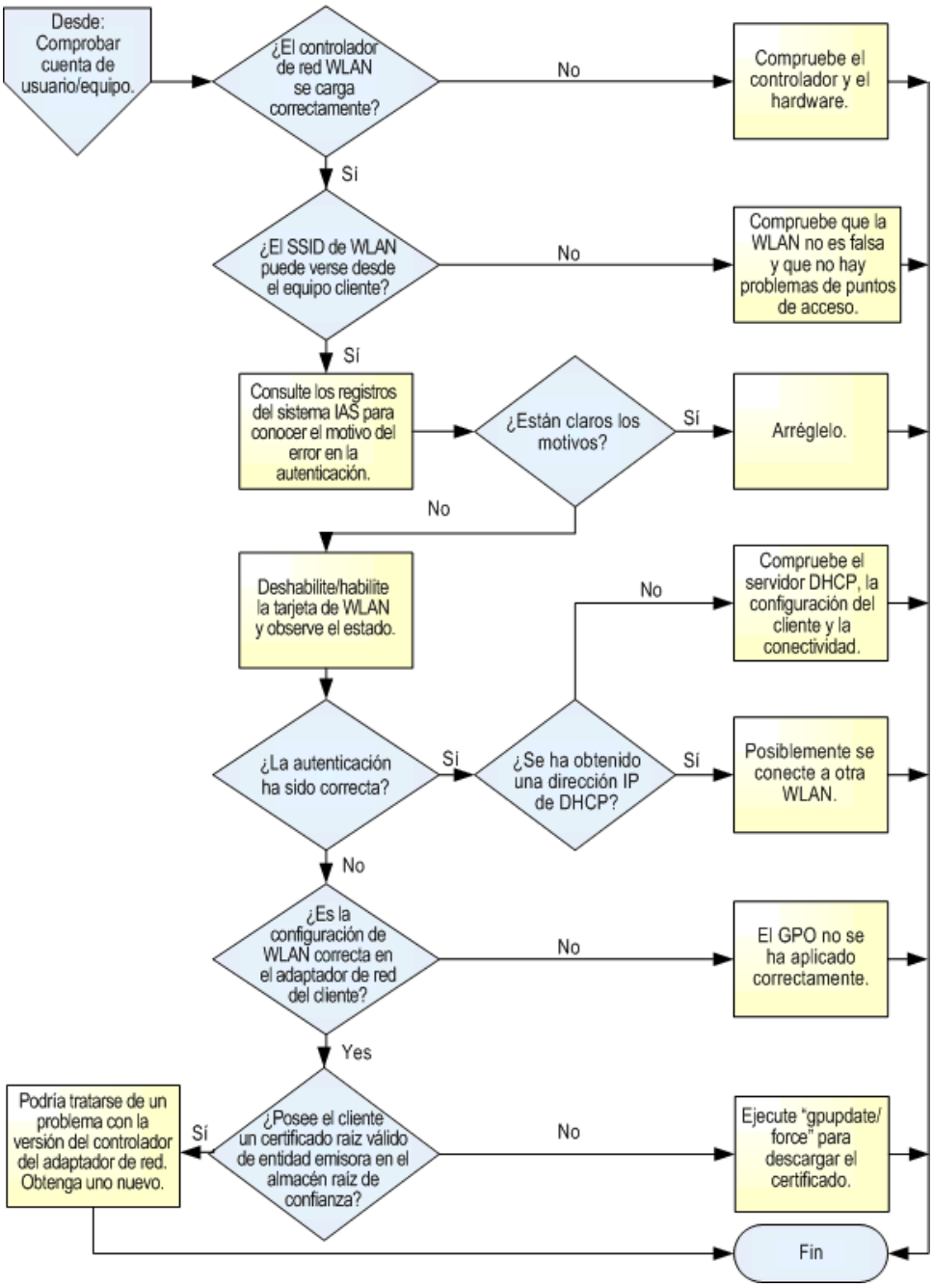

Figura 8.3. Comprobación del equipo cliente
Vista de imagen a pantalla completa

Nota: el cuadro con forma de flecha del diagrama de flujo es un vínculo desde el procedimiento "Comprobar cuenta de usuario/equipo".

El estado de la tarjeta de WLAN (tal y como requiere el paso "Deshabilite/habilite la tarjeta de WLAN y observe el estado" mostrado en el diagrama de flujo) se puede consultar en el panel **Detalles** de la carpeta Conexiones de red (en el **Panel de control**). Cuando habilite la tarjeta, deberá comprobar su estado por medio de las siguientes fases:

- Conexión
- Autenticación
- Adquisición de la dirección IP (a no ser que se asigne estáticamente)

La supervisión del punto en el que surgen errores en el proceso constituye uno de los procedimientos de diagnóstico más útiles.

Comprobar IAS
La siguiente tabla recoge una serie de comprobaciones que se deben realizar si sospecha que un servidor IAS es origen de problemas.

Tabla 8.11. Comprobaciones para el diagnóstico de IAS

Comprobaciones	Detalles
IAS está en ejecución	Abra la MMC de **Administración de equipos** y desplácese a **Servicios**. Asegúrese de que IAS se encuentra en estado de ejecución.
Configuración de red básica de IAS	Ejecute el comando **netdiag** para comprobar si existe algún error en la configuración de red del servidor IAS.
El servidor IAS dispone de un certificado de servidor actual	Abra la MMC **Certificados** y mire en carpeta \Certificados (equipo local)\Personal\Certificados. En esta carpeta, debe encontrar un certificado para el servidor con las siguientes características: -La fecha actual se encuentra dentro del período de validez del certificado. -El nombre alternativo del sujeto coincide con el Sistema de nombres de dominio (DNS) del servidor. -La autenticación del servidor está presente en el Uso de clave extendida. -El emisor del certificado es de confianza (en la ficha **Ruta confiable**). -El certificado no se ha revocado. Consulte la configuración del perfil de la directiva de acceso remoto a IAS, haga clic en la ficha **Autenticación** y consulte la configuración de 802.1X. El certificado del servidor que se acaba de describir debe estar seleccionado.
IAS es miembro del grupo Servidores RAS e IAS del dominio	El servidor necesita ser miembro de este grupo, al que normalmente se agrega cuando IAS se registra en Active Directory.
La directiva de acceso remoto a IAS o la directiva de solicitud de conexión es incorrecta	Compruebe que la configuración de la directiva (y el número de versión, si lo ha incluido) coincide con lo previsto. Si duda, vuelva a implementar la configuración desde el IAS "maestro".
Consulte los sucesos IAS en el registro de sucesos del sistema	Compruebe el registro de sucesos del sistema para comprobar si existe algún suceso de advertencia o de error de IAS. Los errores de autenticación no presentan ningún código de motivo que indique el origen del problema.
Habilite el seguimiento en IAS	Consulte el procedimiento "Habilitación y deshabilitación del seguimiento en el servidor IAS" en la sección "Herramientas y técnicas para la solución de problemas" de este capítulo.
Habilite el seguimiento del cliente	Consulte el procedimiento "Habilitación y deshabilitación del seguimiento en el equipo cliente" en la sección "Herramientas y técnicas para la solución de problemas" de este capítulo.
Habilite el registro SChannel	Para diagnosticar problemas de TLS y los relativos al certificado, habilite el registro SChannel. Para obtener más información, consulte el procedimiento "Habilitación del registro SChannel en el servidor IAS" en la sección "Herramientas y técnicas para la solución de problemas" de este capítulo. También puede habilitar este registro en el equipo cliente para obtener información adicional sobre el diagnóstico desde la perspectiva del cliente.

Comprobar la entidad emisora de certificados
La tabla siguiente contiene una serie de comprobaciones que puede poner en práctica para determinar si el rendimiento de la entidad emisora de certificados es correcto.

Tabla 8.12. Comprobaciones para el diagnóstico de la entidad emisora

Comprobación	Detalle
Los Servicios de Certificate Server están en ejecución	Abra la MMC de **Administración de equipos** y desplácese a **Servicios**. Asegúrese de que los Servicios de Certificate Server están en ejecución.
Compruebe la lista de revocación de certificados, si TLS da error (lo cual aparece en el registro de seguimiento RASTLS o en el registro Schannel) o si la entidad emisora no emite certificados.	Ejecute el comando **msstools CheckCA** en la entidad emisora de certificados para comprobar que existe una lista de revocación de certificados actual publicada y que es accesible. Si encuentra problemas en servidores IAS particulares (o en sitios concretos), consiga la herramienta de estado de infraestructura de claves públicas (del *Kit de recursos de Windows Server 2003*). Se trata de una herramienta de la MMC que le mostrará si el servidor encuentra

	algún problema en el acceso a una lista de revocación de certificados actual o a un certificado de la entidad emisora de certificados.
Si no se ha inscrito ni renovado ningún certificado, consulte el objeto de directiva de grupo de la inscripción automática de certificados.	-Compruebe que el objeto de directiva de grupo de inscripción automática está vinculado a la ubicación correcta, normalmente el dominio. -Compruebe que el objeto de directiva de grupo tiene la plantilla "Equipo" establecida como el tipo de certificado que ha de inscribir (en Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas de claves públicas\Configuración de la solicitud de certificados automática). -Compruebe que el grupo de servidores RAS e IAS dispone de permisos en el objeto de directiva de grupo para **Aplicar directiva y lectura** y que no los anula ningún permiso para denegar (por ejemplo, Usuarios autenticados: denegar lectura).
Plantillas de certificados	La plantilla Equipo se debe asignar a la entidad emisora (compruebe la carpeta de plantillas en la MMC de la **Entidad emisora de certificados**). La plantilla Equipo debe disponer de **permiso para inscribir al grupo Servidores RAS e IAS** (compruebe que ningún permiso para denegar lo anula).
Interfaz de DCOM de entidad emisora de forma remota	Ejecute el comando siguiente desde un servidor IAS remoto para comprobar que DCOM/RPC está funcionando entre el servidor y la entidad emisora de certificados. **certutil -ping-config** *NombredeHostdeEntidadEmisora******NombredeEntidadEmisora* donde *NombredeHostdeEntidadEmisora* es el nombre del equipo del servidor de la entidad emisora y *NombredeEntidadEmisora* es el nombre descriptivo asignado a la entidad emisora de certificados cuando se configura (será el nombre que aparezca en **Emitido por:** de la ficha **General** de cualquier certificado emitido por esta entidad).

Comprobar Active Directory y Servicios de red
La tabla siguiente enumera una serie de comprobaciones que ha de realizar en Active Directory y en otros componentes de red para determinar si están funcionando adecuadamente.

Tabla 8.13. Comprobaciones para el diagnóstico de Active Directory

Comprobación	Detalle
Compruebe la comunicación con Active Directory desde IA	Ejecute el comando **netdiag /test:ldap /test:trust** en el servidor IAS. Este comando también comprobará la existencia de problemas de DNS.
Compruebe los grupos de seguridad de WLAN	Compruebe la pertenencia a los grupos de seguridad utilizados en esta solución para controlar el acceso a WLAN. La pertenencia predeterminada se contempla en la sección "Creación de grupos de seguridad" del capítulo 3, "Preparación del entorno".
Compruebe el objeto de directiva de grupo de la configuración de WLAN del equipo cliente	Compruebe que los valores del objeto de directiva de grupo de la configuración de WLAN son correctos, que el objeto de directiva de grupo está vinculado a la unidad organizativa adecuada (o dominio), y que se le han aplicado los permisos correctos. Consulte la sección "Creación de objetos de directiva de grupo de la configuración de WLAN" del capítulo 6, "Configuración de clientes de LAN inalámbricas".
Compruebe que Active Directory está replicando de forma adecuada	Ejecute el comando **dcdiag /test:replications** desde el servidor IAS en el que ha encontrado problemas. Incluso si IAS no se está ejecutando en un controlador de dominio, la herramienta dcdiag comprobará también el controlador de dominio utilizado por dicho servidor IAS.
Compruebe el servidor DHCP	Compruebe que el servidor DHCP se está ejecutando, que se ha creado un ámbito válido para los clientes WLAN y está activo, y que existe conectividad entre los puntos de acceso inalámbrico y el servidor DHCP. Dicho de forma más precisa, la conectividad es necesaria entre la LAN virtual (VLAN) de los puntos de acceso y el servidor DHCP para permitir que los clientes WLAN adquieran el arrendamiento de una IP).

Comprobar la configuración de los puntos de acceso inalámbrico
La tabla siguiente enumera una serie de comprobaciones que ha de realizar en los puntos de acceso inalámbrico para determinar si

están funcionando adecuadamente.

Tabla 8.14. Comprobaciones para el diagnóstico de los puntos de acceso inalámbrico

Comprobación	Detalle
Compruebe la configuración IP de los puntos de acceso y la conectividad con IAS	Muchos puntos de acceso ofrecen una función para probar la conectividad básica (como el ping). Intente hacer ping a los servidores IAS principal y secundario (otra posibilidad es intentar hacer ping a los puntos de acceso de los servidores IAS principal y secundario).
Compruebe la configuración RADIUS de los puntos de acceso	Compruebe la dirección IP y los valores de los puertos configurados en el punto de acceso para los servidores RADIUS principal y secundario. Asegúrese de que coinciden con la configuración de los servidores IAS.
Compruebe la entrada de cliente RADIUS en el servidor o servidores IAS.	Compruebe que los servidores IAS principal y secundario cuentan con una entrada de cliente RADIUS para este punto de acceso. Si IAS recibe una solicitud RADIUS desde un dispositivo no configurado como cliente, registrará un error en el registro del sistema.
Compruebe el secreto del cliente RADIUS	Puede que sea difícil comprobar visualmente el secreto del cliente RADIUS, puesto que, en algunas ocasiones, no se puede visualizar el secreto RADIUS una vez registrado en el punto de acceso. Si el valor configurado en la entrada de cliente RADIUS de IAS difiere del configurado en el punto de acceso, IAS registrará un error en el registro de sucesos del sistema.
Compruebe la revisión del firmware del punto de acceso	Compruebe que el firmware del punto de acceso está actualizado. Consulte las actualizaciones disponibles en el sitio Web del proveedor.
Compruebe el servidor DHCP	Compruebe que el servidor DHCP se está ejecutando, que se ha creado un ámbito válido para los clientes WLAN y que está activo, y que, asimismo, existe conectividad entre los puntos de acceso inalámbrico y el servidor DHCP. Dicho de forma más precisa, la conectividad es necesaria entre VLAN de los puntos de acceso y el servidor DHCP para permitir que los clientes WLAN adquieran el arrendamiento de una IP.

Comprobar conectividad WAN

El origen de los errores de WLAN puede radicar en problemas de conectividad WAN entre diversos componentes. La tabla siguiente enumera los elementos con más posibilidades de ser la causa de los problemas.

Tabla 8.15. Comprobaciones para el diagnóstico de WAN

Comprobación	Detalle
Autenticación de puntos de acceso inalámbrico a servidores IAS remotos	Pruebe la conectividad simple entre el punto de acceso y los servidores IAS principal y secundario. Para ello, la mayoría de los puntos de acceso disponen de un simple comando **ping** o **traceroute**. Si existen servidores de seguridad o enrutadores filtrando el tráfico entre los sitios en cuestión, debe comprobar que se permite la autenticación RADIUS y el tráfico de información de cuenta (las solicitudes junto con las respuestas en los puertos de Protocolo de datagrama de usuarios (UDP), 1812 y 1813).
Controladores de dominio que replican mediante WAN	Los problemas de replicación entre controladores de dominio pueden aparecer incluso donde hay conectividad IP. Una latencia excesiva puede originar errores en las comunicaciones RPC entre los controladores de dominio. Para comprobarlo, utilice la herramienta dcdiag descrita en la sección "Comprobar Active Directory y Servicios de red" de este capítulo.
Cliente WLAN y servidor DHCP	En los casos en que el servidor DHCP no se encuentre en la misma LAN que los puntos de acceso y que los clientes WLAN autenticados, deberá configurar un agente de retransmisión BOOTP/DHCP para reenviar las solicitudes al servidor DHCP correcto de la red remota.

Herramientas y técnicas para la solución de problemas

En esta sección se describen algunas de las técnicas y herramientas útiles para la solución de problemas.

Comprobación del estado de la carpeta de conexiones de red del cliente

La carpeta Conexiones de red y los iconos de notificación de la bandeja de sistema de Windows XP proporcionan información sobre el estado de la autenticación WLAN.

En la carpeta Conexiones de red (en el **Panel de control**), el texto de estado bajo el adaptador de red inalámbrico describe el estado actual de la conexión. Al resaltar el adaptador, se visualiza información adicional sobre la conexión en el panel **Detalles** de la carpeta Conexiones de red. Al deshabilitar y volver a habilitar el adaptador, se visualiza el estado del adaptador cuando se intenta conectar y autenticar a la WLAN. Esta información puede resultar muy útil cuando se depuran los problemas de conexión del cliente.

Haga clic con el botón secundario en el icono del adaptador y, a continuación, en **Estado** para comprobar la fuerza de la señal WLAN (en la ficha **General**) y los detalles de la dirección IP (en la ficha **Compatibilidad**).

Visualización de los sucesos de autenticación IAS en el registro de sucesos
Los sucesos fallidos o con éxito en la autenticación del cliente (que se graban en el registro de sucesos del sistema en los servidores IAS) pueden resultar útiles para la solución de problemas. El registro de sucesos se habilita de forma predeterminada tanto para las solicitudes de autenticación fallidas como para las satisfactorias. Este parámetro se puede modificar desde la ficha **Servicio** para las propiedades del servidor IAS en la MMC del **Servicio de autenticación de Internet**.

Consultar estos sucesos es útil para solucionar los problemas en la autenticación. En la siguiente tabla se enumeran los tipos de sucesos generados por IAS.

Tabla 8.16. Sucesos de solicitud de autenticación IAS

Suceso IAS	Importancia	Categoría del suceso	Origen del suceso	Id. de suceso
Acceso concedido	Un usuario o equipo se autenticó satisfactoriamente y se le concedió acceso a WLAN.	Información	IAS	1
Acceso denegado	Se denegó un intento de acceso (motivo expuesto en el texto del suceso).	Advertencia	IAS	2
Descartado	El intento de acceso se descartó por agotar el tiempo de espera.	Error	IAS	3

Cada suceso contiene información detallada sobre la solicitud de autenticación. Esta información incluye:

- Nombre de cliente
- Dirección IP e identificador del punto de acceso
- Tipo de cliente (debe ser "Inalámbrica-IEEE 802.11")
- Nombre de la directiva de acceso remoto
- Autenticación y tipo de EAP
- Código y descripción del motivo

Si la autenticación da error, los códigos y descripciones del motivo suelen indicar el problema preciso (aunque a veces el motivo facilitado es ambiguo o engañoso). En la siguiente tabla se exponen los códigos de motivo disponibles.

Tabla 8.17. Códigos de motivo de los sucesos de solicitud de autenticación IAS

Código de motivo	Descripción
00	Correcto
01	Error interno
02	Acceso denegado
03	Solicitud mal formulada
04	Catálogo global no disponible
05	Dominio no disponible
06	Servidor no disponible
07	No existe el dominio
08	No existe el usuario
16	Error en autenticación
17	Error al cambiar contraseña
18	Tipo de autenticación no compatible
32	Sólo usuarios locales
33	Debe cambiar la contraseña

34	Cuenta deshabilitada
35	Cuenta caducada
36	Cuenta bloqueada
37	Horas de inicio de sesión no válidas
38	Restricción de cuenta
48	No coincide ninguna directiva
64	Marcado bloqueado
65	Marcado deshabilitado
66	Tipo de autenticación no válido
67	Estación de llamada no válida
68	Horas de marcado no válidas
69	Estación llamada no válida
70	Tipo de puerto no válido
71	Restricción no válida
80	No hay registros
96	Tiempo de espera de sesión agotado

En algunos casos, la información extraída de las entradas del registro de sucesos no es suficiente para diagnosticar la causa del problema. En estos casos, puede que necesite habilitar el seguimiento en el cliente y en el servidor IAS. En los procedimientos siguientes se describe el modo de hacerlo.

Habilitación y deshabilitación del seguimiento en equipos cliente

Windows admite un seguimiento detallado de la información en la mayoría de los componentes para facilitar el diagnóstico de los problemas que puedan surgir. La habilitación del seguimiento para un componente hace que se escriban los resultados del diagnóstico en los archivos de registro de texto, al tiempo que proporciona más detalles que los registros de sucesos.

Para obtener información pormenorizada sobre el proceso de autenticación WLAN, debe habilitar el seguimiento de EAP a través de los componentes de LAN (EAPOL) y del Servicio de acceso remoto - Seguridad de la capa de transporte (RASTLS) utilizando el comando **netsh**. Una vez habilitado el seguimiento, intente de nuevo el proceso de autenticación y examine los archivos Eapol.log y Rastls.log en busca de algún tipo de indicaciones sobre los problemas (estos archivos se grabarán en la carpeta %Systemroot%\Tracing).

Para habilitar el seguimiento en equipos cliente

- Ejecute los siguientes comandos:

  netsh ras set tracing eapol enabled

  netsh ras set tracing rastls enabled

Para deshabilitar el seguimiento en equipos cliente

- Ejecute los siguientes comandos:

  netsh ras set tracing eapol disabled

  netsh ras set tracing rastls disabled

  Nota: el seguimiento consume una gran cantidad de recursos del sistema y crea archivos de registro que crecen con celeridad. No olvide volver a deshabilitar el seguimiento cuando finalice la tarea de solución de problemas.

Habilitación y deshabilitación del seguimiento en el servidor IAS

La habilitación del seguimiento en IAS funciona de la misma forma que en el equipo cliente.

Puede utilizar el comando **netsh** para habilitar y deshabilitar el seguimiento en una gran variedad de componentes diversos relacionados con la autenticación de red. Los componentes cuya habilitación resulta más útil para el seguimiento de los problemas de autenticación 802.1X basada en PEAP son los siguientes:

- **IASSAM (el archivo Iassam.log de la carpeta %Systemroot%\tracing):** éste es el archivo de seguimiento más utilizado para los problemas de IAS, puesto que describe las funciones relacionadas con el descifrado (traducción entre distintos formatos) de nombres de usuario, el enlace a un controlador de dominio y la comprobación de credenciales. Se trata del "centro" de los archivos de

seguimiento de IAS y suele ser necesario para depurar los problemas relacionados con la autenticación.

- **RASTLS (el archivo Rastls.log de la carpeta %Systemroot%\tracing):** este archivo de seguimiento se utiliza para todas las autenticaciones relacionadas con EAP y PEAP. Este registro contiene la mayor parte de la información vital para la depuración. No obstante, su lectura y comprensión es bastante compleja, de ahí que Microsoft tenga como objetivo publicar documentación que facilite la interpretación de esta información.
- **RASCHAP (el archivo Raschap.log de la carpeta %Systemroot%\tracing):** este archivo de seguimiento se utiliza para todas las operaciones de autenticación de contraseñas basadas en MS-CHAP v2 y otros CHAP.

La habilitación del seguimiento de los componentes IAS que se indican a continuación no suele ser necesaria para solucionar problemas de autenticación 802.1X, pero puede resultar útil para solucionar problemas de otra índole:

- **IASRAD (el archivo Iasrad.log de la carpeta %Systemroot%\tracing):** éste registra todas las operaciones relacionadas con el protocolo RADIUS. Asimismo, describe los puertos en los que el servidor escucha, etc. Puede resultar útil para depurar problemas de compatibilidad de los puntos de acceso inalámbrico.
- **IASSDO (el archivo Iassdo.log de la carpeta %Systemroot%\tracing):** el registro IASSDO contempla transacciones realizadas desde la interfaz de usuario a archivos MDB que almacenan el diccionario y la configuración del servidor. Se trata del registro utilizado para solucionar los problemas de cualquier servicio o los relacionados con la interfaz de usuario.

Para habilitar el seguimiento en el servidor IAS

1. Ejecute el comando **netsh** correspondiente al tipo de información de seguimiento que necesite. Cuando solucione problemas relacionados con la autenticación 802.1X, los registros IASSAM, RASTLS y RASCHAP serán los que contengan la información más útil.

   netsh ras set tracing iassam enabled

   netsh ras set tracing rastls enabled

   netsh ras set tracing raschap enabled

   netsh ras set tracing iasrad enabled

   netsh ras set tracing iassdo enabled

   Otra posibilidad para habilitar el seguimiento de todas las categorías de componentes de red sería la ejecución del siguiente comando:

   netshras set tracing * enabled

Para deshabilitar el seguimiento en el servidor IAS

1. Ejecute uno o varios de los siguientes comandos **netsh** para deshabilitar el seguimiento de las categorías habilitadas en el procedimiento anterior:

   netsh ras set tracing iassam disabled

   netsh ras set tracing rastls disabled

   netsh ras set tracing raschap disabled

   netsh ras set tracing iasrad disabled

   netsh ras set tracing iassdo disabled

   Otra posibilidad para deshabilitar el seguimiento de todas las categorías de componentes de red sería la ejecución del siguiente comando:

   netshras set tracing * disabled

   Nota: dado que el seguimiento consume recursos significativos del sistema, debe utilizarlo con moderación para identificar los problemas de la red. Una vez realizado el seguimiento o identificado el problema, deberá deshabilitar el seguimiento inmediatamente.

De forma predeterminada, los archivos de seguimiento IASSAM y RASTLS están establecidos en sólo 1 MB. Esto puede originar que se sobrescriba información valiosa en los archivos de registro durante grandes cargas. El procedimiento que sigue establece los registros de seguimiento en 10 MB. Cuando un archivo de registro alcanza el límite de 10 MB, se le cambia el nombre (a IASSAM.old y RASTLS.old) y se crea un nuevo archivo de registro. Esto mantiene un máximo de 20 MB de información en el servidor para cada tipo de seguimiento. Puede repetir este procedimiento para cualquier tipo de seguimiento con sólo sustituir el nombre de la categoría del seguimiento (como RASTLS y RASCHAP) por el nombre clave "IASSAM" utilizado en el procedimiento.

Para establecer el archivo de registro de seguimiento IASSAM en 10 MB

1. Inicie Regedit.exe.
2. Desplácese hasta la siguiente clave de Registro:

   HKEY_LOCAL_MACHINE\Software\Microsoft\Tracing

3. Busque la subclave **IASSAM**. Ésta debería tener un valor de Registro **MaxFileSize** (un tipo de **REG_DWORD**). Edite este valor y establezca el valor de los datos como **0xA00000** (ésta es la representación hexadecimal de 10MB: el valor predeterminado sería 0x100000). Si lo desea, puede establecer un valor distinto a 10 MB, si bien los registros comenzarían a ser difíciles de administrar con un tamaño mayor.

   Advertencia: la edición incorrecta del Registro puede dañar el sistema gravemente. Antes de realizar cambios en el Registro, haga copias de seguridad de todos los datos importantes del equipo.

Habilitación del registro SChannel en el servidor IAS

SChannel es un proveedor de compatibilidad de seguridad (SSP) que admite varios protocolos de seguridad de Internet, como capa de sockets seguros (SSL) y seguridad de la capa de transporte (TLS). Si sospecha que existen problemas relacionados con el certificado de servidor IAS o si el registro RASTLS indica que existe algún problema con la creación de la sesión TLS, debe habilitar el registro SChannel tanto en el cliente como en el servidor. Los sucesos se registran en el registro de seguridad.

Siga el mismo procedimiento tanto en el equipo cliente, como en el servidor.

Para habilitar el registro SChannel

1. Inicie Regedit.exe.
2. Desplácese hasta la siguiente clave de Registro:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL

3. Habilite sucesos SChannel detallados mediante la modificación del valor **EventLogging** de **1** (tipo **REG_DWORD**, datos **0x00000001**) a **3** (tipo **REG_DWORD**, datos **0x00000003**).

   Advertencia: la edición incorrecta del Registro puede dañar el sistema gravemente. Antes de realizar cambios en el Registro, debe hacer copias de seguridad de todos los datos importantes del equipo.

Cuando termine de solucionar problemas, asegúrese de deshabilitar el registro Schannel, puesto que consume recursos significativos del sistema e inundará el registro de sucesos con entradas no deseadas.

Herramientas de diagnóstico para el equipo Pocket PC

Windows XP cuenta con varias herramientas de diagnóstico de red. Los equipos Pocket PC, en cambio, disponen de relativamente pocas herramientas integradas en el sistema base. El proveedor del equipo Pocket PC, Microsoft y otras compañías proporcionan diversos tipos de herramientas para facilitar el diagnóstico de los problemas con estos equipos. Algunos ejemplos incluyen:

- **Configuración IP y herramientas de diagnóstico:** herramientas tales como VXUtil o VXIPConfig de Cambridge Software.
- Herramientas de diagnóstico de WLAN facilitadas por el proveedor del equipo Pocket PC.

Principio de la página

Resumen

En este capítulo se han tratado los siguientes elementos necesarios para mantener el estado de la infraestructura de seguridad de WLAN:

- Identificación de las tareas de mantenimiento esenciales.
- Descripción de las tareas operativas, de supervisión, soporte técnico, modificación y optimización relacionadas con este entorno.
- Descripción de los procedimientos y técnicas clave para la solución de problemas.

Principio de la página

Referencias

Esta sección contiene vínculos a otras fuentes de información que sirven como referencia para las instrucciones proporcionadas en este capítulo:

- Para obtener más información sobre la realización de copias de seguridad y la restauración de los servidores Windows, consulte la página "Backing up and restoring data" de Windows Server 2003 en Microsoft.com en:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctasks001.mspx

- Para obtener más información sobre la supervisión y administración, consulte la página "Microsoft Solutions for Management" en Microsoft.com en:

http://www.microsoft.com/technet/itsolutions/techguide/msm/default.mspx

- Para obtener más información sobre la optimización de IAS, consulte la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/deployguide/dnsbk_ias_rziy.mspx

- Para obtener más información sobre la solución de problemas de componentes de red inalámbricos, consulte las siguientes direcciones URL:

  http://support.microsoft.com/default.aspx?scid=313242

  http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifitrbl.mspx

- Para obtener más información sobre la solución de problemas de IAS, consulte la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_ias_tshoot_node.mspx

- Para obtener más información sobre la configuración IP y las herramientas de diagnóstico tales como VXUtil o VXIPConfig, consulte la siguiente dirección URL:

  http://www.cam.com/windowsce.html

(Este artículo contiene referencias a guías de otros productos y vínculos a sitios Web que sólo están disponibles en inglés.)

Principio de la página

Administre su perfil