Latinoamérica

Microsoft TechNet

Capítulo 8: Implementación de la infraestructura de RADIUS

Publicado: octubre 11, aaaa | Actualizado: 24/11/04

En esta página

Introducción

En este capítulo se proporciona una guía detallada para crear una infraestructura de RADIUS (servicio de usuario de acceso telefónico de autenticación remota) para la seguridad de LAN inalámbricas (WLAN) basada en el servicio de autenticación de Internet (IAS) de Microsoft® Windows Server™ 2003. En esta guía se incluye la instalación y configuración de los servidores RADIUS, la preparación del servicio de directorio de Microsoft Active Directory® y la configuración del servidor IAS. La infraestructura de RADIUS se utilizará en el siguiente capítulo para crear una solución LAN inalámbrica completa.

El objetivo de este capítulo es proporcionar la guía de implementación para el diseño de RADIUS descrito en el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas". En el capítulo no se intenta explicar ningún concepto general de RADIUS ni ningún aspecto específico del modo en que IAS implementa el protocolo.

Este capítulo complementa los capítulos de la guía de planeamiento y la guía de operaciones de RADIUS y WLAN. En los capítulos de la guía de planeamiento se explica la lógica subyacente a las decisiones de implementación empleadas en este capítulo y en los capítulos de la guía de operaciones se explican las tareas y procesos necesarios para mantener correctamente la infraestructura de RADIUS. Si todavía no lo ha hecho, es recomendable que lea los capítulos de planeamiento antes de continuar con este capítulo. También debe leer y comprender las implicaciones de los requisitos de asistencia del capítulo de operaciones antes de utilizar la guía de este capítulo para implementar la infraestructura de RADIUS.

Requisitos previos

En esta sección se incluyen listas de comprobación que le ayudarán a establecer la preparación de su organización para implementar la infraestructura de RADIUS. ("Preparación" se emplea aquí con un significado logístico en vez de un sentido empresarial; la motivación empresarial para implementar esta solución se trata en capítulos anteriores de la guía de planeamiento.)

Requisitos previos de conocimientos

Debe estar familiarizado con los conceptos de RADIUS y de IAS en concreto. También se precisan conocimientos de Windows 2000 Server o de Windows Server 2003 en las siguientes áreas:

- Instalación del sistema operativo Microsoft Windows®.
- Conceptos de Active Directory (incluidas las estructuras y herramientas de Active Directory, manipulación de usuarios, grupos y otros objetos de Active Directory, así como el uso de la directiva de grupo).
- Seguridad del sistema de Windows, conceptos de seguridad como usuarios, grupos y auditoría, listas de

control de acceso (ACL), uso de plantillas de seguridad y aplicación de plantillas de seguridad mediante Directiva de grupo o herramientas de la línea de comandos.

- Comprensión de las secuencias de comandos de archivos por lotes. El conocimiento de Windows Scripting Host y el lenguaje Microsoft Visual Basic® Scripting Edition (VBScript) le ayudará a sacar el máximo provecho de las secuencias de comandos suministradas, pero no es esencial.

Antes de leer este capítulo, también debe haber leído el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas" y disponer de un conocimiento exhaustivo de la arquitectura y el diseño de la solución.

Requisitos previos organizativos

Debe consultar a otros miembros de la organización que puedan tener necesidad de participar en la implementación de esta solución, como:

- Patrocinadores empresariales.
- Personal de seguridad y auditoría.
- Personal de ingeniería, administración y operaciones de Active Directory.
- Personal de ingeniería, administración y operaciones de DNS (sistema de nombres de dominio) y redes.

Requisitos previos de la infraestructura de TI

En este capítulo se supone lo siguiente en relación con la infraestructura de TI existente:

- Existe una infraestructura de dominios de Active Directory de Windows Server 2003 implementada. Todos los usuarios de la infraestructura de RADIUS de esta solución deben ser miembros de dominios del mismo bosque de Active Directory.

  Nota: para obtener más información acerca de la compatibilidad con versiones anteriores de Microsoft Windows, consulte el apéndice A, "Matriz de compatibilidad de versiones de Windows".

- En esta solución no se incluye orientación para la integración en una infraestructura de RADIUS existente; no obstante, esto no impide la implementación en una infraestructura de RADIUS existente.
- Disponibilidad de hardware de servidor capaz de ejecutar IAS de Windows Server 2003. Como parte de la guía se proporciona una configuración sugerida.
- Están disponibles licencias, medios de instalación y claves de producto de Windows Server 2003 Standard Edition y Enterprise Edition.

Descripción general del capítulo

En la siguiente figura se muestra el proceso de crear la infraestructura de RADIUS tal como se describe en este capítulo.

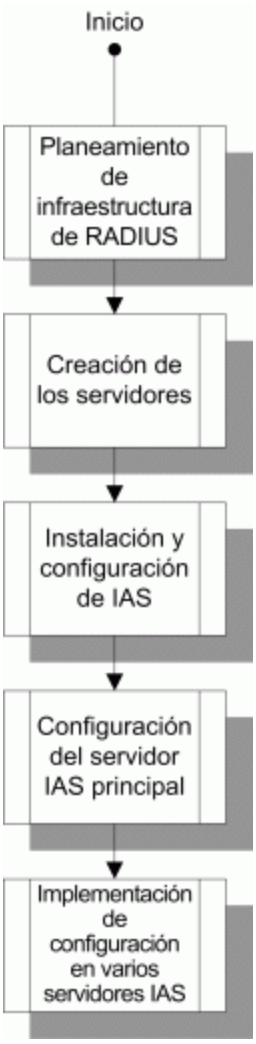

Figura 8.1 Diagrama del proceso de creación de la infraestructura de RADIUS

Estos pasos están reflejados en la organización del capítulo y se describen en la siguiente lista. Cada uno consta de tareas de instalación o configuración y uno o varios procedimientos de comprobación, por lo que puede comprobar lo que acaba de hacer antes de continuar con el paso siguiente.

- **Hoja de planeamiento de IAS**. Se enumera la información de configuración empleada en este capítulo para instalar y configurar IAS. Se incluye una tabla de información que debe proporcionar antes de empezar la implementación.
- **Creación de los servidores**. Se describe la selección y configuración de hardware, la instalación de Windows Server 2003 y la instalación de componentes opcionales. También se describe la creación de los grupos de seguridad de administración de Active Directory, el modo de configurar los permisos correctos para delegar tareas de administración y la implementación de seguridad de nivel de sistema operativo mediante la aplicación de plantillas de seguridad. Las plantillas utilizadas proceden de la *Guía de seguridad de Windows Server 2003*. Al final del capítulo se puede encontrar información acerca de cómo obtener esta guía. En esta sección también se indican algunas tareas comunes para realizar la instalación básica de los servidores.
- **Instalación y configuración de IAS**. Se describen los pasos de preparación, la instalación de software y la

configuración de IAS, incluida la creación y protección de directorios de datos de IAS.

- **Configuración del servidor IAS principal** Se describe la configuración del servidor IAS principal que se utilizará como plantilla de configuración para servidores IAS adicionales de funciones similares en el entorno. También se explica la exportación de la configuración de IAS para utilizarla en otros servidores IAS. Este procedimiento se volverá a utilizar en capítulos posteriores después de haber efectuado una configuración más exhaustiva.
- **Configuración del servidor IAS secundario**. Se describe la configuración del servidor IAS secundario que se unirá al principal en un par de servidores RADIUS para obtener resistencia a errores y equilibrio de carga. También se describe el modo de importar la configuración de IAS principal para la implementación automática. Este procedimiento se volverá a utilizar en capítulos posteriores después de haber efectuado una configuración más exhaustiva.
- **Configuración de servidores IAS de sucursal**. Se describe la configuración un servidor IAS de sucursal opcional que se puede utilizar como ejemplo de entornos distribuidos y cómo importar la configuración de IAS principal para la implementación automática. Este procedimiento se volverá a utilizar en capítulos posteriores después de haber efectuado una configuración más exhaustiva.

Principio de la página

Hoja de trabajo de planeamiento de infraestructura de RADIUS

En las tablas siguientes se indican los parámetros de configuración utilizados en esta solución. Utilícelas como lista de comprobación cuando tome decisiones de planeamiento.

Muchos de los parámetros de estas tablas se configuran manualmente y forman parte de los procedimientos que se describen en este capítulo. Otros se establecen mediante una secuencia de comandos que se ejecuta como parte de uno de los procedimientos o se les hace referencia en una secuencia de comandos para completar otra configuración o tarea operativa.

Nota: las secuencias de comandos utilizadas en la guía de generación se describen más detalladamente en el archivo Léame.txt que se incluye con las mismas.

Elementos de configuración definidos por el usuario

En la siguiente tabla se enumeran parámetros específicos de organización tomados de la compañía ficticia Woodgrove Bank. Asegúrese de que ha recopilado, o tomado decisiones sobre valores equivalentes para su organización, todos estos elementos antes de iniciar el procedimiento de instalación. Los valores ficticios que se muestran aquí se utilizan en todo el capítulo en los comandos de muestra proporcionados. Debe sustituir estos valores por los adecuados para su organización. Los lugares en los que debe utilizar sus propios valores se muestran en cursiva.

Tabla 8.1: Elementos de configuración definidos por el usuario

Elemento de configuración	Configuración
Nombre DNS del dominio raíz del bosque de Active Directory	*woodgrovebank.com*
Nombre NetBIOS (servicio básico de entrada y salida de red) del dominio	*WOODGROVEBANK*
Nombre del servidor IAS principal	*HQ-IAS-01*
Nombre del servidor IAS secundario	*HQ-IAS-02*
Nombre del servidor IAS secundario	*BO-IAS-03*

Elementos de configuración recomendados por la solución

La configuración especificada en esta tabla no se debe cambiar en instalaciones concretas, a menos que existan necesidades específicas y sea necesario utilizar valores diferentes a los del diseño de la solución. Los

parámetros del diseño se pueden cambiar, si es consciente de que, al hacerlo, se dejará de utilizar la solución probada. Asegúrese de que comprende todas las implicaciones del cambio de una configuración y sus dependencias antes de alterar uno de estos valores en los procedimientos de configuración o en las secuencias de comandos suministradas.

Tabla 8.2: Elementos de configuración que recomienda la solución

Elemento de configuración	Configuración
[Cuentas] Nombre completo del grupo administrativo que controla la configuración de IAS	Administradores IAS
[Cuentas] Nombre del grupo administrativo que controla la configuración de IAS en versiones anteriores a Windows 2000	Administradores IAS
[Cuentas] Nombre completo del grupo que revisa los registros de solicitudes de autenticación y de cuentas de IAS con fines de seguridad	Auditores de seguridad IAS
[Cuentas] Nombre del grupo que revisa los registros de peticiones contables y las autenticaciones de IAS con fines de seguridad en versiones anteriores a Windows 2000	Auditores de seguridad IAS
[Secuencias de comandos] Ruta para las secuencias de comandos de instalación	C:\MSSScripts
[Secuencias de comandos] Archivo por lotes de exportación de configuración de IAS	IASExport.bat
[Secuencias de comandos] Archivo por lotes de importación de configuración de IAS	IASImport.bat
[Secuencias de comandos] Archivo por lotes de exportación de configuración de cliente RADIUS de IAS	IASClientExport.bat
[Secuencias de comandos] Archivo por lotes de importación de configuración de cliente RADIUS de IAS	IASClientImport.bat
[Config] Ruta para archivos de copia de seguridad de la configuración	D:\IASConfig
[Registros de solicitudes] Ubicación de los registros de solicitudes de autenticación y auditoría IAS	D:\IASLogs
[Registros de solicitudes] Nombre compartido de los registros de solicitudes RADIUS	IASLogs

Preparación para IAS

La solución incluye dos servidores IAS ubicados centralmente y configurados como servidores RADIUS para el control de acceso a LAN inalámbricas. También incluye un servidor IAS opcional de sucursal configurado como servidor RADIUS para entornos que requieren una infraestructura distribuida. Para obtener más información acerca de la situación de servidores IAS, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Antes de instalar IAS, debe realizar varias tareas de preparación, como:

- Configuración del hardware del servidor.
- Instalación del sistema operativo del servidor.
- Preparación de Active Directory.
- Realización de tareas de consolidación de la seguridad del servidor.

Principio de la página

Creación de los servidores

En las secciones siguientes se describen los pasos necesarios para crear los servidores. Aunque la creación de cada servidor puede llevarse a cabo de forma independiente, es importante que se realicen todos los pasos en todos los servidores.

Especificación del hardware del servidor

Debe seleccionar el hardware del servidor para IAS de la Lista de compatibilidad de hardware (HCL) de Windows Server 2003. La selección del hardware de servidor de la HCL de Windows Server 2003 contribuye a evitar los problemas de confiabilidad y compatibilidad que puedan surgir con el hardware que no se haya probado o con controladores de dispositivos escritos de manera inadecuada. Puede encontrar más información acerca de la HCL de Windows Server 2003 en la sección "Información adicional" al final de este capítulo.

Especificaciones de hardware de servidor probadas

Las especificaciones de hardware siguientes se utilizaron para probar esta solución en un entorno de laboratorio. Estas especificaciones de hardware se incluyen sólo de referencia y no son obligatorias. Para ver una explicación más extensa de los requisitos de hardware de servidor IAS, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Tabla 8.3: Especificaciones de hardware de servidor probadas

Recurso	Requisito
CPU	CPU dual a 850 MHz o superior.
Memoria	512 MB.
Interfaces de red	Dos tarjetas de interfaz de red (NIC) independientes, unidas para obtener mayor resistencia.
Almacenamiento en disco	Controlador RAID (matriz redundante de discos independientes) IDE (electrónica integrada de dispositivos) o SCSI (interfaz estándar de equipos pequeños). 2 x 9 GB (SCSI o IDE) configurados como volumen RAID 1 (unidad C). 2 x 18 GB (SCSI o IDE) configurados como volumen RAID 1 (unidad D). Medios de almacenamiento local extraíbles (CD-RW o cinta para copia de seguridad) si no existe un servicio de copia de seguridad de red. Unidad de disco de 1,44 MB para la transferencia de datos.

Preparación del hardware

Complete toda la configuración de hardware de acuerdo con las recomendaciones del proveedor. Estas configuraciones pueden incluir la aplicación del BIOS (sistema básico de entrada y salida) más reciente, así como de las actualizaciones de firmware del proveedor.

Utilice el software de administración del controlador de disco incluido con el hardware para crear los volúmenes RAID 1 del esquema de la tabla anterior.

Instalación de Windows Server 2003

En esta sección se describe detalladamente la instalación de Windows Server 2003 en los servidores IAS. Muchas organizaciones disponen de un proceso de instalación de servidores automatizado. Puede utilizarlo para crear servidores siempre que se puedan incluir en los servidores creados los parámetros empleados en el procedimiento siguiente. Para obtener información acerca de si utilizar Windows Server 2003 Standard Edition o

Windows Server 2003 Enterprise Edition, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Para instalar Windows Server 2003 en uno de los servidores IAS, realice los pasos siguientes.

Para instalar Windows Server 2003

1. Compruebe que el CD-ROM se haya establecido como dispositivo de inicio en la configuración del BIOS del servidor. Reinicie el equipo con el CD de Windows Server 2003 en la unidad de CD-ROM.
2. Cree una partición en el volumen principal, formatéela como sistema de archivos NTFS y seleccione la opción para instalar Windows en dicha partición.
3. Seleccione la configuración regional adecuada.
4. Escriba el nombre y la información de la empresa en la que se va a registrar Windows.
5. Escriba una contraseña segura para la cuenta del administrador local (con un mínimo de 10 caracteres, combinando caracteres alfabéticos en mayúscula y minúscula, numéricos y signos de puntuación).
6. Cuando se le solicite, escriba el nombre del equipo (sustituya este valor por el nombre de su equipo):
   - IAS principal: *HQ-IAS-01*
   - IAS secundario: *HQ-IAS-02*
   - IAS de sucursal: BO-IAS-03
7. Cuando se le pida, seleccione la opción para unirse a un dominio. Escriba el nombre del dominio de Active Directory al que se van a unir los servidores: ***WOODGROVEBANK*** (sustituya este valor por el nombre del dominio en que va a instalar el servidor RADIUS). Cuando se le pida, escriba las credenciales del usuario que está autorizado para unir equipos a este dominio.

   Nota: para un dominio de bosques múltiples, normalmente los servidores IAS se instalarán en el dominio raíz del bosque para optimizar el funcionamiento de Kerberos. Aunque esta configuración no es fundamental, se supone en esta solución.
8. No instale ningún componente opcional.

   El equipo se reiniciará al final del proceso de instalación principal. Siga con los pasos siguientes.
9. Instale los Service Pack actuales, actualizaciones críticas y otras actualizaciones necesarias.
10. Reasigne la letra R a la unidad CD-ROM/DVD.
11. Cree una partición en el segundo volumen del disco duro, asígnele la letra de unidad D y dele formato con NTFS.
12. Active esta copia de Windows.

Configuración de la red

Los servidores IAS tienen una única interfaz de red (aunque esta configuración se puede implementar uniendo dos NIC físicas para obtener una mayor resistencia). La interfaz de red se debe configurar con una dirección fija del Protocolo Internet (IP) y otros parámetros de configuración de IP (como puerta de enlace predeterminada y configuración de DNS), tal como corresponda a la red.

Comprobación de la instalación

Debe comprobar que la instalación del sistema operativo ha finalizado correctamente y que los parámetros configurados son los esperados.

Para ver la configuración del sistema actual

1. Ejecute el programa systeminfo en un símbolo del sistema.
2. Compruebe los elementos siguientes del resultado de la información del sistema (se han omitido algunos detalles del resultado en aras de la brevedad):

   Nombre de host: *HQ-IAS-01*

   Nombre del sistema operativo: Microsoft® Windows® Server 2003, Enterprise Edition

   ...

   Configuración del sistema operativo: Servidor miembro

   Propiedad de: *SuNombre*

   Organización registrada: *NombreDeLaOrganización*

   ...

   Directorio de Windows: C:\WINDOWS

   Directorio de sistema: C:\WINDOWS\System32

   Dispositivo de inicio: \Device\HarddiskVolume1

   Configuración regional del sistema: *ConfiguraciónRegionalDelSistema*

   Idioma: *SuIdioma*

   Zona horaria: *SuZonaHoraria*

   ...

   Dominio: woodgrovebank.com

   Servidor de inicio de sesión: *NombreDelControladorDeDominio*

   Revisión(es): X revisión(es) instaladas.

   [01]: Qxxxxxx

   ...

   [nn]: Qnnnnnn

   Tarjeta(s) de red: 1 Tarjetas de interfaz de red instaladas.

   [01]: *ModeloYProveedorDeTarjetaDeRed*

   Nombre de conexión: Conexión de área local

   DHCP habilitado: No

   Direcciones IP

   [01]: xxx.xxx.xxx.xxx
3. Si estos valores no son los que esperaba, debe volver a configurar el servidor mediante el Panel de control o volver a realizar la instalación.

Instalación de secuencias de comandos de configuración en los servidores

Con la solución se proporciona una serie de secuencias de comandos y archivos de configuración auxiliares que ayudan a simplificar algunos aspectos de su configuración y funcionamiento. Debe instalarlos en todos los servidores. Algunas de estas secuencias de comandos se necesitarán para las operaciones descritas en el

capítulo 12, "Administración de la infraestructura de seguridad de RADIUS y LAN inalámbrica", de modo que no debe eliminarlas una vez finalizada la instalación del servidor RADIUS.

Para instalar las secuencias de comandos de instalación en todos los servidores

1. Cree una carpeta denominada **C:\MSSScripts**.
2. Copie las secuencias de comandos del medio de distribución en esta carpeta.

Comprobación de los Service Pack y las actualizaciones de seguridad

En este punto, debe volver a comprobar la lista de los Service Pack y actualizaciones de seguridad instalados. Utilice una herramienta como Microsoft Baseline Security Analyzer (MBSA) para realizar la comprobación y obtener las actualizaciones necesarias. Después de las pruebas adecuadas, instálelas en los servidores.

Para obtener más información acerca de MBSA, consulte la sección "Información adicional" al final de este capítulo.

Instalación de software adicional

En esta sección se describe la instalación del software adicional que puedan requerir los servidores IAS.

CAPICOM

Se requiere CAPICOM 2.0 en los servidores RADIUS para algunas de las secuencias de comandos de configuración y administración proporcionadas con esta solución. Para obtener información acerca de dónde encontrar la versión más reciente de CAPICOM, consulte la sección "Información adicional" al final de este capítulo.

Siga las instrucciones del archivo ejecutable autoextraíble para instalar y registrar la biblioteca de vínculos dinámicos (DLL) CAPICOM antes de continuar con esta guía.

Comprobación de la conectividad de la red y Active Directory

IAS depende en gran medida de la correcta configuración y conectividad de la red con Active Directory. Por lo tanto, debe considerar la ejecución de diagnósticos de red en el servidor antes de implementar IAS.

Para realizar diagnósticos de red con la utilidad Netdiag.exe de las herramientas de soporte de Windows Server 2003, que se pueden encontrar en el CD de Windows Server 2003. Netdiag.exe se puede extraer mediante la ejecución del comando siguiente:

```
expand r:\support\tools\support.cab –f:netdiag.exe c:\mssscripts
```

Al finalizar, escriba el siguiente comando para ejecutar la utilidad:

```
C:\mssscripts\netdiag.exe
```

Asegúrese de investigar los errores o advertencias que se muestren.

Comprobación del nivel de funcionalidad de dominio

El modelo preferido para controlar el acceso de red consiste en utilizar el valor de configuración **Controlar acceso a través de la directiva de acceso remoto** en las cuentas de usuario de Active Directory. El valor de configuración **Controlar acceso a través de la directiva de acceso remoto** sólo se encuentra disponible si Active Directory se ejecuta en modo nativo de Windows 2000 o posteriores. Por lo tanto, debe comprobar el nivel de funcionalidad de dominio antes de implementar la directiva de acceso remoto (RAP) en IAS.

Para comprobar el nivel de funcionalidad de dominio, lea las propiedades del dominio desde la herramienta Dominios y confianzas de Active Directory. Si el dominio de destino para IAS está configurado en modo mixto de Windows 2000, póngase en contacto con los administradores de Active Directory correspondientes para planear la migración al modo nativo.

Para obtener más información acerca de este tema, consulte la sección "Información adicional" al final de este capítulo.

Configuración de grupos de seguridad de Active Directory

IAS forma parte de la infraestructura de seguridad de la red. En consecuencia, el acceso a la configuración de IAS y archivos de registro se debe controlar estrictamente. Para implementar los controles de acceso necesarios, se utiliza una combinación de grupos globales de Active Directory y grupos locales de Windows Server 2003.

Creación de grupos de administración de IAS
Ejecute la secuencia de comandos siguiente como administrador del dominio para crear grupos de seguridad de administración de IAS:

Cscript //job:CreateIASGroups C:\MSSScripts\IAS_Tools.wsf

Esta secuencia de comandos crea los grupos de seguridad siguientes como grupos globales de dominio:

- Administradores IAS
- Auditores de seguridad IAS

En un bosque con múltiples dominios, estos grupos deben crearse en el mismo dominio que los servidores IAS.

Nota: las organizaciones con administradores ubicados en múltiples dominios deben considerar el uso de grupos universales en vez de los grupos globales creados aquí. La secuencia de comandos que crea grupos de seguridad se puede modificar fácilmente mediante la sintaxis empleada para crear el grupo Directiva de acceso remoto - Acceso inalámbrico en el capítulo siguiente (consulte "Creación de los grupos de Active Directory necesarios para el acceso a WLAN" en el capítulo 9).

Configuración del grupo de administradores de IAS
IAS es un componente principal del sistema operativo Windows Server 2003 y se requiere la pertenencia al grupo de seguridad Administradores local para realizar las tareas de configuración de IAS.

Debe agregar el grupo global de dominio de administradores de IAS al grupo Administradores local en cada servidor IAS. Si IAS está instalado en un controlador de dominio, debe agregar los administradores de IAS al grupo Administradores del dominio que utilice el complemento Usuarios y equipos de Active Directory de Microsoft Management Console (MMC).

Advertencia: agregar grupos al grupo de dominio Administradores integrado tiene graves consecuencias de seguridad. Para obtener más información acerca de la situación de IAS en controladores de dominio, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

Debe asignar los grupos Administradores de IAS y Auditores de seguridad de IAS con las cuentas del personal de administración adecuado. Para obtener una descripción completa del modo en que estos grupos se asignan a las funciones administrativas de IAS, consulte la descripción del planeamiento de permisos administrativos en el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

En los procedimientos de configuración del resto de este capítulo se requiere el uso de cuentas que sean miembros del grupo Administradores de IAS.

Protección de Windows Server 2003 para IAS
Debe adoptar las medidas adicionales que sean necesarias para proteger los servidores IAS del acceso no autorizado. Los servidores IAS constituyen una parte fundamental de la infraestructura de seguridad y se deben tratar con la misma consideración que los servidores de seguridad y otras infraestructuras de acceso de seguridad.

Seguridad física
Debe alojar los servidores IAS en una ubicación donde el acceso físico se controle estrictamente. Estos servidores deben estar en línea continuamente. Por este motivo, deben situarse en ubicaciones que dispongan de servicios habituales en las salas de servidores, como control de temperatura, filtrado de aire y capacidad de extinción de fuego.

La ubicación de los servidores debe estar tan libre como sea posible de riesgos externos que puedan perjudicar al servidor, como fuego e inundaciones.

También es igualmente importante controlar el acceso físico a copias de seguridad, documentación y otros datos

de configuración, así como garantizar su seguridad física. Esta información debe almacenarse en una ubicación distinta de la de los servidores.

Aplicación de configuración de seguridad de sistema a los servidores

Los servidores IAS se protegen mediante la función de servidor IAS definida en la *Guía de seguridad de Windows Server 2003*. En la sección "Información adicional", al final de este capítulo, hay disponible más información sobre esta guía y la ubicación para descargar las plantillas de seguridad.

Debido a que los servidores IAS son miembros de un dominio, la configuración de directivas de seguridad se aplica mediante una directiva de grupo basada en dominio. Para aplicar la configuración de seguridad, debe crear una estructura adecuada de unidades organizativas (UO) que contenga los objetos de equipo del servidor IAS y una estructura de objetos de directiva de grupo (GPO). Debe crear dos GPO para los servidores IAS que se ejecutan en servidores dedicados (es decir, no instalados en controladores de dominio):

- Cliente empresarial: Línea de base de servidores miembro
- Cliente empresarial: Servicio de autenticación de Internet

Después de consultar el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas", puede optar por ejecutar algunos o todos los servicios en controladores de dominio. Debido a la complejidad de la consolidación de controladores de dominio, en este documento no se proporcionan instrucciones sobre el modo de aplicar plantillas de seguridad de controlador de dominio. En la *Guía de seguridad de Windows Server 2003* se incluye una plantilla para controladores de dominio, que efectúa un bloqueo similar al de la directiva de línea de base de servidores miembro. Debe aplicar la plantilla de seguridad para controladores de dominio a los controladores de dominio existentes después de leer detenidamente la *Guía de seguridad de Windows Server 2003* y evaluar las posibles consecuencias en los clientes y aplicaciones de dominio.

Si utiliza la plantilla de seguridad Cliente empresarial: Controlador de dominio en los servidores IAS y de controlador de dominio combinados, también tiene que aplicar la plantilla de seguridad Cliente empresarial: Servidor IAS a dichos equipos. Esta plantilla aplica una configuración adicional que habilita el servicio IAS. (El servicio IAS está deshabilitado en la plantilla Cliente empresarial: Controlador de dominio.) Para aplicar esta plantilla, debe crear un GPO adicional para aplicarlo en una nueva unidad organizativa secundaria situada debajo de la UO Controladores de dominio:

- Cliente empresarial: IAS en Controladores de dominio

Debe seguir el siguiente procedimiento para importar la plantilla Cliente empresarial: Servidores IAS en este GPO. En este procedimiento se describe cómo crear las unidades organizativas y los GPO. Los nombres de GPO y UO son sólo ejemplos. El procedimiento debe adaptarse a los estándares de UO y GPO del dominio.

Para crear las UO y GPO de los servidores IAS

1. Obtenga las siguientes plantillas de seguridad de la *Guía de seguridad de Windows Server 2003*:
   - Cliente empresarial: Dominio
   - Cliente empresarial: Línea de base de servidores miembro
   - Cliente empresarial: Servidor IAS
   - Cliente empresarial: Controlador de dominio
2. Inicie sesión como miembro de los administradores de dominio o como usuario con derechos de creación de las unidades organizativas descritas en el paso 4. Para crear GPO, tiene que ser miembro de los administradores de dominio o del grupo de propietarios del creador de directivas de grupo.
3. Abra el complemento MMC Usuarios y equipos de Active Directory.
4. Cree la siguiente estructura de UO:

woodgrovebank.com

- Servidores miembro

- IAS

- Controladores de dominio

- Controladores de dominio con IAS

Advertencia: los pasos del 5 al 7 aplican directivas de domino que configuran directivas de cuenta locales en todos los equipos del dominio. Debe examinar la configuración de la plantilla de seguridad Cliente empresarial: Dominio. En vez de aplicarla a todo el dominio, puede crear este GPO vinculado a la UO de IAS de modo que su alcance esté restringido únicamente a los servidores IAS.

5. Abra las propiedades del contenedor de dominio. En la ficha **Directiva de grupo**, haga clic en **Nuevo** para crear un nuevo GPO y asígnele el nombre **Directiva de dominio**.

6. Edite el GPO y desplácese hasta Configuración del equipo\Configuración de Windows\Configuración de seguridad. Haga clic con el botón secundario del mouse en la carpeta **Configuración de seguridad** y, a continuación, haga clic en **Importar**. Busque el archivo Enterprise Client – Domain.inf y selecciónelo como plantilla para importar.

7. Cierre el GPO.

8. Repita los tres pasos anteriores para la combinación de OU, GPO y plantillas de seguridad que se muestran en la siguiente tabla. (Estos tres GPO sólo afectan a los servidores IAS, por lo que la advertencia anterior no se aplica aquí.)

Tabla 8.4: Objetos de directiva de grupo y ubicación

UO	GPO	Plantilla de seguridad
Servidores miembro	Cliente empresarial: Línea de base de servidores miembro	Enterprise Client – Member Server Baseline.inf
IAS	Cliente empresarial: Servicio de autenticación de Internet	Enterprise Client – IAS Server.inf
Controladores de dominio con IAS	Cliente empresarial: IAS en Controladores de dominio (opcional si IAS se encuentra en un controlador de dominio)	Enterprise Client – IAS Server.inf

Después de crear los GPO e importar las plantillas, debe personalizar la configuración de los GPO y aplicarlos a los equipos servidores IAS, como se describe en el procedimiento siguiente.

Para personalizar y aplicar el GPO Cliente empresarial: Servicio de autenticación de Internet

1. Desde Usuarios y equipos de Active Directory, edite el GPO Cliente empresarial: Servicio de autenticación de Internet. En Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad, cambie los siguientes elementos de acuerdo con los estándares de seguridad de la organización:

   - Cuentas: cambiar el nombre de la cuenta del administrador: *NuevoNombreDelAdministrador*
   - Cuentas: cambiar el nombre de la cuenta de invitado: *NuevoNombreDelInvitado*
   - Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión:

TextoDelAvisoLegal

- Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión: *TítuloDelAvisoLegal*

2. En la asignación de directivas locales y derechos de usuario, agregue los siguientes grupos locales y de dominio al derecho **Permitir el inicio de sesión local**:
   - (local) *Administradores*
   - (local) *Operadores de copia de seguridad*
   - (dominio) Auditores de seguridad de IAS
3. Abra las propiedades de los siguientes servicios en la carpeta de servicios del sistema y haga clic en **Definir esta configuración de la directiva en la plantilla**. Acepte los permisos predeterminados haciendo clic en **Aceptar**. Establezca el valor **Seleccionar el modo de inicio del servicio** en **Automático**
   - Almacenamiento de medios extraíbles
   - Instantáneas de volumen
   - MS Software Shadow Copy Provider
   - Programador de tareas

   Nota: estos servicios están deshabilitados en la plantilla de seguridad de línea de base de servidores miembro, pero NTBackup.exe requiere los tres primeros. Algunas secuencias de comandos operativas requieren el servicio del Programador de tareas.
4. Traslade la cuenta de equipo del servidor IAS a la UO de IAS.
5. En el servidor IAS, ejecute el comando gpupdate para aplicar la configuración del objeto de directiva de grupo al equipo.

   Nota: en la *Guía de seguridad de Windows Server* 2003 se incluyen explicaciones más detalladas de estas configuraciones de seguridad. Consulte la sección "Información adicional" al final de este capítulo para obtener información acerca de cómo obtener esta guía.

Para personalizar y aplicar el GPO Cliente empresarial: IAS en Controladores de dominio

1. Desde Usuarios y equipos de Active Directory, edite el GPO Cliente empresarial: IAS en Controladores de dominio. En Configuración del equipo\Configuración de Windows\Configuración de seguridad\Directivas locales\Opciones de seguridad, cambie los siguientes elementos de acuerdo con los estándares de seguridad de la organización:
   - Cuentas: cambiar el nombre de la cuenta del administrador: *NuevoNombreDelAdministrador*
   - Cuentas: cambiar el nombre de la cuenta de invitado: *NuevoNombreDelInvitado*
   - Inicio de sesión interactivo: texto del mensaje para los usuarios que intentan iniciar una sesión: *TextoDelAvisoLegal*
   - Inicio de sesión interactivo: título del mensaje para los usuarios que intentan iniciar una sesión: *TítuloDelAvisoLegal*
2. En la asignación de directivas locales y derechos de usuario, agregue los siguientes grupos locales y de dominio al derecho **Permitir el inicio de sesión local**:
   - (Integrado) *Administradores*

- (Integrado) *Operadores de copia de seguridad*
- (dominio) Auditores de seguridad de IAS

3. Abra las propiedades de los siguientes servicios en la carpeta de servicios del sistema y haga clic en **Definir esta configuración de la directiva en la plantilla**. Acepte los permisos predeterminados haciendo clic en **Aceptar**. Establezca el valor **Seleccionar el modo de inicio del servicio** en **Automático**.
   - Almacenamiento de medios extraíbles
   - Instantáneas de volumen
   - MS Software Shadow Copy Provider
   - Programador de tareas

   Nota: estos servicios están deshabilitados en la plantilla de seguridad de la línea base de servidores miembro, pero se necesitan los tres primeros para ejecutar NTBackup.exe. Algunas secuencias de comandos operativas requieren el servicio del Programador de tareas.
4. Traslade la cuenta de equipo del servidor IAS a los controladores de dominio con UO de IAS.
5. En el servidor IAS, ejecute el comando gpupdate para aplicar la configuración del objeto de directiva de grupo al equipo.

   Nota: en la *Guía de seguridad de Windows Server* 2003 se incluyen explicaciones más detalladas de estas configuraciones de seguridad. Consulte la sección "Información adicional" al final de este capítulo para obtener información acerca de cómo obtener esta guía.

Comprobación de la configuración de seguridad

Para comprobar la correcta aplicación de la configuración de seguridad, lleve a cabo los pasos del siguiente procedimiento.

Para comprobar la configuración de seguridad del servidor IAS

1. Compruebe en el registro de sucesos de la aplicación si aparecen sucesos del origen SceCli. Debe aparecer el suceso con Id. 1704 detrás del comando **gpupdate**. El texto del suceso debe ser:

   Se ha aplicado correctamente la directiva de seguridad en los objetos de directiva de grupo.
2. Reinicie el servidor y compruebe que se inician todos los servicios deseados y que no se registran errores en el registro de sucesos.
3. Debe poder iniciar sesión y ver el texto del aviso legal.

Configuración de seguridad de Servicios de Terminal Server

Debe utilizar Servicios de Terminal Server para la modificación programada de las contraseñas (secretos de RADIUS) empleadas por los clientes RADIUS. El cifrado de tráfico de Servicios de Terminal Server protege los secretos de RADIUS a medida que pasan por la red.

Importante: si se utiliza otro método para definir o modificar los secretos de cliente de RADIUS a través de la red (como el uso de telnet o de otra herramienta simple de ejecución remota), asegúrese de que se utilice seguridad del protocolo Internet (IPsec) u otra tecnología adecuada para proteger la información en tránsito.

Debe establecerse la siguiente configuración de Servicios de Terminal Server en los GPO Cliente empresarial: IAS en Controladores de dominio y Cliente empresarial: Servicio de autenticación de Internet que se apliquen a los servidores IAS.

Tabla 8.5: Configuración para Configuración de equipo\Plantillas administrativas\Componentes de Windows\Servicios de Terminal Server

Ruta de acceso	Directiva	Configuración
	Denegar el cierre de sesión a un administrador con una sesión iniciada en la consola	Habilitada
	No permitir a los administradores locales personalizar permisos	Habilitada
	Establece reglas para el control remoto de sesiones de usuario de Servicios de Terminal Server	Control remoto no permitido
Redirección de datos cliente-servidor	Permitir redirección de zona horaria	Deshabilitado
	No permitir redirección del portapapeles	Habilitada
	Permitir redirección de audio	Deshabilitado
	No permitir redirección de puertos COM	Habilitada
	No permitir redirección de impresoras de cliente	Habilitada
	No permitir redirección de puertos LPT	Habilitada
	No permitir redirección de unidad	Habilitada
	No establecer impresora predeterminada de cliente como impresora predeterminada para una sesión	Habilitada
Cifrado y seguridad	Establecer el nivel de cifrado de conexión de cliente	Alta
	Pedir siempre al cliente la contraseña al conectarse	Habilitada
Cifrado y seguridad\Seguridad de llamada a procedimiento remoto	Servidor seguro (requerir seguridad)	Habilitada
Sesiones	Establece un tiempo límite para sesiones desconectadas	10 minutos
	Permitir reconexiones sólo desde el cliente original	Habilitada

Cualquier grupo de seguridad o cuenta de dominio que requiera el acceso de Servicios de Terminal Server a los servidores IAS debe agregarse al grupo local de usuarios de escritorio remoto (a menos que ya sea un miembro del grupo de administradores locales).

Otras tareas de configuración de Windows

Existen otras tareas de configuración según la infraestructura y los estándares de la organización. Por ejemplo:

- Habilitación de copias de seguridad o instalación de agentes de copia de seguridad.

- Configuración de las opciones del Protocolo simple de administración de redes (SNMP) o del Instrumental de administración de Windows (WMI).
- Instalación de agentes de administración como los componentes de cliente de Microsoft Operations Manager (MOM) o Microsoft Systems Management Server (SMS).
- Instalación de software antivirus.
- Instalación de agentes de detección de intrusiones.

Debe comprobar estos elementos a medida que se instalan.

Principio de la página

Instalación y configuración de IAS

Esta solución incluye dos servidores IAS ubicados centralmente que actúan como servidores RADIUS para la autenticación de usuarios y la autorización de acceso a la red. La solución también incluye un servidor IAS de sucursal para entornos que requieran autenticación y autorización distribuidas de acceso a la red. Para obtener más información acerca de la situación de servidores IAS, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".

En la siguiente sección se describen las tareas para instalar IAS en los servidores. Es importante que efectúe todos los pasos de instalación y configuración en todos los servidores IAS.

Instalación de componentes de software de IAS

IAS se instala con el administrador de componentes opcionales de Windows (al que se puede tener acceso mediante **Agregar o quitar componentes** del Panel de control). En la tabla siguiente se enumeran los componentes que se deben instalar. La sangría refleja la relación jerárquica entre los componentes, como se verían en el asistente del administrador de componentes opcionales. Los componentes que no están seleccionados no se muestran en la tabla.

Tabla 8.6 Componentes de IAS para instalar

Componente opcional que se instalará	Estado de instalación
Servicios de red	Seleccionado
Servicio de autenticación de Internet	Seleccionado

Nota: se necesitará el medio de instalación de Windows Server 2003 para completar la instalación.

Para instalar componentes de IAS

- Ejecute el administrador de componentes opcionales en cada servidor IAS para automatizar la instalación de IAS; el siguiente comando realiza esta tarea:

  sysocmgr /i:sysoc.inf /u:C:\MSSScripts\OC_AddIAS.txt

Registro de IAS en Active Directory

Los servidores IAS se deben registrar en cada dominio. Esto significa convertir la cuenta de equipo del servidor IAS en miembro del grupo de seguridad Servidores IAS y RAS en cada dominio para el que sea necesario efectuar la autenticación. La pertenencia a este grupo garantiza que los servidores IAS tengan permiso para leer las propiedades de acceso remoto de las cuentas de usuario y equipo del dominio.

Los objetos de cuenta de equipo de los servidores IAS se pueden colocar en este grupo mediante el complemento de MMC Usuarios y equipos de Active Directory o el comando Netshell (**netsh**).

Para registrar IAS en servidores en el dominio predeterminado con el comando netsh

1. Inicie sesión en cada servidor IAS con una cuenta que tenga privilegios de administrador de dominio para el dominio.
2. Abra un símbolo del sistema y escriba:

   netsh ras add registeredserver

Para registrar IAS en dominios distintos del predeterminado con el comando netsh

1. Inicie sesión en cada servidor IAS con una cuenta que tenga privilegios de administrador de dominio para el dominio de destino.
2. Abra un símbolo del sistema, escriba lo siguiente y reemplace *NombreDeDominio* por el nombre del dominio en el que se registrará el servidor IAS:

   netsh ras add registeredserver domain = *NombreDeDominio*

   Nota: también puede agregar el objeto de equipo del servidor IAS al grupo de seguridad Servidores IAS y RAS mediante el complemento de Microsoft Management Console (MMC) Usuarios y equipos de Active Directory.

Creación y protección de directorios de datos de IAS

Debe crear directorios de datos en las unidades de datos de los servidores IAS para almacenar los datos de configuración y registro de IAS. En un símbolo del sistema, realice el procedimiento siguiente en cada servidor IAS para crear y proteger los directorios de datos de IAS. También puede utilizar la secuencia de comandos por lotes que se proporciona para automatizar este procedimiento.

Para crear y proteger directorios de datos de IAS

- Ejecute los comandos siguientes, sustituyendo WOODGROVEBANK por el nombre NetBIOS del dominio:
  - md D:\IASConfig
  - md D:\IASLogs
  - cacls D:\IASConfig /G system:F administrators:F "Backup Operators":C
  - cacls D:\IASLogs /G system:F administrators:F "Backup Operators":C "WOODGROVEBANK\IAS Security Auditors":C

También debe compartir el directorio D:\IASLogs con los auditores de seguridad IAS para que puedan tener acceso a los datos de registro de petición RADIUS de forma remota.

Para compartir el directorio de registro IAS de forma segura

- Ejecute el comando siguiente, sustituyendo WOODGROVEBANK por el nombre NetBIOS del dominio:

  net share IASLogs=D:\IASLogs /GRANT:"WOODGROVEBANK\IAS Security Auditors",CHANGE

Se ha creado un archivo por lotes opcional que contiene los comandos anteriores, pero debe editarse para incluir el nombre NetBIOS correcto del dominio.

Para editar y ejecutar el archivo por lotes para crear, proteger y compartir los directorios de datos de IAS

1. Utilice el bloc de notas para editar el archivo C:\MSSScripts\IAS_Data.BAT y sustituya WOODGROVEBANK por el nombre NetBIOS del dominio.
2. Ejecute el archivo por lotes ejecutando el comando siguiente en un símbolo del sistema:

   C:\MSSScripts\IAS_Data.BAT

Principio de la página

Configuración del servidor IAS principal

Debe seleccionar uno de los servidores IAS del entorno como servidor principal. Configurará este servidor antes que los demás servidores IAS y servirá de plantilla para configurar las opciones de los servidores IAS posteriores.

Configuración del registro de solicitudes de autenticación y de cuentas

De forma predeterminada, IAS no registra solicitudes de autenticación y de cuentas de RADIUS. Si es posible, deben habilitarse ambos tipos de registros de solicitudes para asegurarse de que los sucesos de seguridad se registren y puedan investigarse más adelante. Además, es posible que la organización tenga que utilizar los datos de las cuentas para la facturación.

Nota: el registro de solicitudes de RADIUS influye en el rendimiento del servidor y requiere procesos para garantizar que los registros no llenan los discos de datos. Consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas", y el capítulo 3, "Administración de la infraestructura de seguridad de LAN inalámbrica y RADIUS", para obtener información acerca de cómo archivar y eliminar archivos de registro.

Para configurar el registro de autenticación y de cuentas en servidores IAS

1. Utilice el complemento Servicio de autenticación de Internet de MMC para seleccionar **Registro de acceso remoto** y, a continuación, ver las propiedades del método de registro del **Archivo local**.
2. Seleccione las solicitudes **Cuentas** (por ejemplo, inicio o detención de cuentas) y las solicitudes **Autenticación** (por ejemplo, acceso-aceptación o acceso-denegación).

   Nota: esta guía no habilita el registro de solicitudes de estado periódicas. Sin embargo, es posible que lo necesite para realizar un seguimiento preciso de la información de sesión de red de los usuarios. Para obtener más información, consulte el capítulo 5, "Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas".
3. Compruebe que se define el directorio D:\IASLogs como directorio de los archivos de registro y que se selecciona el formato **Base de datos compatible**.

El uso del formato **Base de datos compatible** permite importar los registros de solicitudes directamente en bases de datos como Microsoft Access y Microsoft SQL Server™ 2000, lo que facilita las consultas y la generación de informes a partir de los datos.

Configuración de IAS para el acceso a la LAN inalámbrica y otras aplicaciones de red

Ahora ha configurado las opciones básicas de IAS. En el resto del capítulo se describe el modo de replicar la configuración del primer servidor IAS a los servidores posteriores. Antes de replicar esta configuración debe configurar las directivas de acceso remoto y otras opciones específicas de la aplicación. En el capítulo 9, "Implementación de la seguridad de LAN inalámbricas", se describe el modo de configurar IAS para LAN inalámbricas. Después de configurar el primer servidor puede volver a este capítulo y seguir los procedimientos para replicar la configuración IAS en otros servidores.

Principio de la página

Implementación de la configuración en varios servidores IAS

Puede utilizar el comando **netsh** para exportar parte de la configuración de IAS a archivos de texto. Las áreas de configuración siguientes pueden exportarse individualmente:

- Configuración de servidor
- Configuración de registro
- Directivas de acceso remoto

- Directivas de solicitud de conexión
- Clientes RADIUS
- Configuración completa

Estos archivos de texto pueden utilizarse para transferir la configuración común a varios servidores IAS para garantizar una configuración coherente y acelerar la implementación. Las secciones de configuración siguientes pueden ser comunes para los servidores con funciones similares:

- Configuración del servidor
- Configuración de registro
- Directiva de acceso remoto
- Directivas de solicitud de conexión

Los elementos anteriores sólo deben configurarse en el servidor IAS principal. A continuación, utilice el comando **netsh** para exportarlos a archivos de texto. Después, estos archivos de texto pueden importarse a otros servidores IAS con una función similar. Este proceso garantiza que los archivos de texto de configuración común estén sincronizados en todos los servidores.

Cada servidor IAS contiene la configuración de clientes RADIUS con información confidencial compartida que normalmente es única para cada servidor. Por lo tanto, se debe realizar la configuración y copia de seguridad de dicha información en cada servidor de forma independiente.

Advertencia: con el comando **netsh** para realizar un volcado completo se crea un archivo de texto de configuración con información confidencial RADIUS compartida de gran importancia. En esta guía se muestra el modo de implementar la configuración y realizar la copia de seguridad sin utilizar un volcado completo de la configuración de IAS. Si decide utilizar los archivos de texto de configuración de volcado completo, asegúrese de administrarlos y almacenarlos con gran confidencialidad. La información de dichos archivos permitiría a cualquier persona obtener acceso a la red.

En las siguientes secciones se describe el procedimiento para transferir la configuración desde el servidor IAS principal a servidores IAS adicionales con una función similar. Puede replicar la configuración en esta fase, pero hasta el momento se han efectuado cambios mínimos en la configuración de los servidores IAS. Debe volver a efectuar este procedimiento de replicación después de que se hayan realizado cambios importantes en la configuración de IAS en el capítulo siguiente, como la creación de la directiva de acceso a la red y la incorporación de clientes RADIUS.

Exportación de la configuración del servidor IAS principal

La exportación de la configuración del servidor IAS principal es necesaria para transferir dicha configuración a otros servidores IAS utilizados en esta solución.

Los archivos por lotes pueden automatizar la exportación de áreas de configuración de IAS comunes para la copia de seguridad y como ayuda en la implementación de la configuración de IAS en varios servidores IAS con la misma función. Al crear archivos por lotes para la implementación de la configuración, incluya sólo configuraciones portátiles en servidores IAS:

- Configuración del servidor
- Configuración de registro
- Directiva de acceso remoto
- Directivas de solicitud de conexión

Para exportar la configuración común del servidor IAS principal

- Escriba el comando siguiente en un símbolo del sistema:

C:\MSSScripts\IASExport.bat

Este archivo por lotes contiene una serie de comandos **netsh** que exportan la información de configuración común a archivos de texto de configuración del directorio D:\IASConfig.

Carga de la configuración de copia de seguridad desde el servidor principal

IAS utiliza el comando **netsh** para transferir el estado de configuración de un servidor a otro. Este proceso acelera la implementación y reduce las posibilidades de error durante las implementaciones de varios servidores. Los archivos de texto de estado de configuración del servidor IAS principal creados anteriormente se pueden utilizar ahora para cargar la configuración en el servidor IAS secundarios y en los de sucursal.

Para cargar los archivos de texto de configuración exportados, desde el servidor IAS principal en los demás servidores IAS, debe seguir estos pasos.

Para cargar la configuración común del servidor IAS principal en otros servidores IAS

1. Copie todos los archivos de configuración desde el directorio D:\IASConfig del servidor IAS principal en el directorio D:\IASConfig de los demás servidores IAS.
2. Utilice el siguiente archivo por lotes para cargar la configuración de los archivos de texto de configuración del servidor IAS principal:

   C:\MSSScripts\IASImport.bat

Principio de la página

Resumen

Si ha realizado todos los procedimientos de este capítulo, debe haber completado las siguientes tareas:

- Instalado y configurado las opciones básicas de un servidor IAS principal.
- Instalado y configurado un servidor IAS secundario.
- Instalado y configurado un servidor IAS opcional de sucursal.
- Configurado grupos administrativos para administrar los servidores IAS.

Ahora ya está preparado para configurar valores específicos para WLAN, tema que se trata en el capítulo "Implementación de la seguridad de LAN inalámbricas". Es posible que tenga que volver a la parte final de este capítulo para replicar la configuración de IAS que se configurará en el siguiente capítulo.

También debe leer ahora las partes correspondientes del capítulo 12, "Administración de la infraestructura de seguridad de LAN inalámbrica y RADIUS", que contiene información fundamental para mantener el funcionamiento de la infraestructura de RADIUS de forma segura y confiable.

Información adicional

- CAPICOM se puede descargar del Centro de descarga de Microsoft en www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6. No obstante, busque "CAPICOM" en el sitio del Centro de descarga para asegurarse de que obtiene la versión más reciente.
- El artículo "Managing Remote Access on a Per-Group Basis Using Windows 2000 Remote Access Policies" está disponible en www.microsoft.com/windows2000/techinfo/administration/management/pgremote.asp.
- La *Guía de seguridad de Windows Server 2003* se puede descargar de http://go.microsoft.com/fwlink/?LinkId=14846.
- El capítulo "Servicio de autenticación de Internet" de la *Referencia técnica de Windows Server 2003*. Esta guía se puede encontrar en http://go.microsoft.com/fwlink/?LinkId=4630.

- El capítulo "Implementación de IAS" del *Kit de implementación de Windows Server 2003* se puede encontrar en: http://go.microsoft.com/fwlink/?LinkId=4716.
- La calificación de hardware para el programa de logotipo de Windows se describe en "FAQ for Windows Logo Program for Hardware" en www.microsoft.com/whdc/winlogo/logofaq.mspx.
- El artículo "Microsoft Baseline Security Analyzer V1.2" está disponible en www.microsoft.com/technet/security/tools/mbsahome.mspx.
- Las tecnologías WLAN 802.1X se describen en el artículo "Windows XP Wireless Deployment Technology and Component Overview" en www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx

Principio de la página

Administre su perfil