Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 3: Preparación del entorno

Actualizado: abril 3, aaaa

Ver todos los temas de guía de seguridad

En esta página

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

Información general

Este capítulo ayuda a preparar el entorno de tecnología de la información (TI) para implementar la infraestructura de seguridad para su red de área local inalámbrica (WLAN). Las principales tareas para preparar el entorno incluyen:

- Preparar el dominio del servicio de directorio Microsoft® Active Directory® creando grupos de seguridad necesarios.
- Preparar sus servidores para instalar el Servicio de autenticación de Internet (IAS) y los Servicios de Certificate Server. Esta tarea también incluye las tres subtareas siguientes:
  - Aplicar configuración de seguridad a los servidores.
  - Instalar herramientas necesarias en los servidores.
  - Actualizar los servidores para garantizar que no tienen vulnerabilidades de seguridad.

Principio de la página

Requisitos previos del capítulo

Antes de continuar, debe tener un buen conocimiento de la arquitectura y el diseño de esta solución que se describe en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". Además, debe estar familiarizado con la instalación y administración de Microsoft Windows® 2000 Server o Microsoft Windows Server™ 2003. También puede ser útil el conocimiento de los siguientes temas:

- Conceptos de Active Directory, incluyendo estructura y herramientas de administración, administración de usuarios, grupos y otros objetos de Active Directory y utilización de la directiva de grupo.

  Temas relacionados con la seguridad del sistema Windows, incluyendo conceptos de seguridad como usuario

- y grupos, auditoría de las listas de control de acceso (ACL) y aplicación de configuración de seguridad mediante la directiva de grupo.
- Lenguaje Windows Scripting Host y Microsoft Visual Basic® Scripting Edition (VBScript).

Principio de la página

Requisitos previos y supuestos de la infraestructura de TI

Este capítulo y los siguientes de esta guía se basan en los siguientes supuestos sobre infraestructura de TI, aunque algunos se pueden implementar como parte de esta solución. Muchos de estos supuestos no son requisitos rígidos; en esta guía se indica dónde hay configuraciones alternativas válidas.

- Un bosque de Active Directory con controladores de dominio Windows 2000 Server o Windows Server 2003, con todos los usuarios de WLAN como miembros de un dominio en el mismo bosque.

  Nota: los controladores de dominio en los que se instalan IAS y los Servicios de Certificate Server deben ejecutar Windows Server 2003.
- Dos o más servidores ejecutando Windows Server 2003, Standard Edition (Windows Server 2003, Enterprise Edition también es compatible) en los que se instalan componentes de la solución.
- Estos servidores tienen capacidad suficiente para ejecutar IAS y Servicios de Certificate Server, además de cualquier servicio y aplicación existente. Los Servicios de Certificate Server se instalan sólo en el servidor principal.
- IAS se instalará en controladores de dominio existentes. Esto es opcional ya que puede instalar IAS en un servidor miembro de dominio.
- Los Servicios de Certificate Server se instalarán en un controlador de dominio. De forma opcional, puede instalar Servicios de Certificate Server en un servidor miembro de dominio.
- Tiene acceso al medio de instalación de Windows Server 2003.
- El dominio en el que se instalará IAS se está ejecutando en el modo nativo de Windows 2000. Esto es opcional.
- Una infraestructura LAN inalámbrica instalada o planeada que conste de varios puntos de acceso inalámbrico. El diseño de la infraestructura de WLAN y los temas relacionados, como la colocación de los puntos de acceso inalámbrico y la selección de canal no se tratan en esta guía.
- Se asume que la organización en su totalidad tiene menos de 50 puntos de acceso.
- Una o más sucursales sin controladores de dominio local (y sin servidores IAS) pero con clientes que necesitan conexiones a la WLAN.

Aunque la solución se ha creado para este perfil específico, el diseño básico se puede adaptar a muchas otras configuraciones, como sucursales con controladores de dominio local o la instalación en bosques de varios dominios. El impacto de las configuraciones alternativas válidas, cuando sea aplicable, se describe en esta guía.

Principio de la página

Preparación de la implementación

Permisos necesarios

Para llevar a cabo los procedimientos indicados en este capítulo debe utilizar una cuenta miembro del grupo Administradores para el dominio que contiene los servidores. De forma predeterminada, la cuenta de administrador integrada del dominio es miembro del grupo Administradores, aunque puede utilizar cualquier otra cuenta que pertenezca al grupo.

Nota: esta guía se basa en la suposición de que está instalando Servicios de Certificate Server e IAS en un controlador de dominio. Si los está instalando en servidores que no son controladores de dominio, la cuenta que

utilice sólo necesitará ser miembro del grupo Administradores local en cada uno de los servidores.

Herramientas necesarias

Necesita las siguientes herramientas para llevar a cabo los procedimientos descritos en este capítulo:

Tabla 3.1. Herramientas necesarias

Herramienta	Descripción	Fuente
Secuencias de comandos de solución WLAN	Conjunto de secuencias de comandos y herramientas proporcionado con esta solución.	Los detalles de instalación se proporcionan en este capítulo.
Consola de administración de directivas de grupo	Herramienta de administración avanzada de objetos de directiva de grupo que permite importarlos y exportarlos.	Se puede descargar del sitio Microsoft.com. Los detalles de instalación se proporcionan en este capítulo.
CAPICOM	Biblioteca del sistema que permite ejecutar secuencias de comandos de operaciones de certificado y seguridad.	Se puede descargar del sitio Microsoft.com. Los detalles de instalación se proporcionan en este capítulo.
DSACLs.exe	Herramienta de línea de comandos, que permite establecer permisos en los objetos de Active Directory.	CD de instalación de Windows Server 2003. Los detalles de instalación se proporcionan en este capítulo.
Usuarios y equipos de Active Directory	Herramienta de Microsoft Management Console (MMC) utilizada para administrar usuarios, grupos, equipos y otros objetos de Active Directory.	Instalado como parte de Windows Server 2003.

Principio de la página

Instalación de herramientas de la solución

Con esta guía se proporcionan una serie de secuencias de comandos y herramientas para ayudar a simplificar la configuración y el funcionamiento de esta solución. Debe instalar estas secuencias de comandos y herramientas en cada uno de los servidores IAS. Algunas de estas secuencias de comandos son necesarias durante las operaciones en curso (como se describe en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas"), por lo que no debe eliminarlas después de completar la instalación. De forma predeterminada, las secuencias de comandos se encuentran ubicadas en la carpeta en C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools.

Para instalar las secuencias de comandos y las herramientas en cada servidor

1. Copie el archivo **PEAPWLAN.msi** proporcionado con la solución en el servidor.
2. En el **Explorador de Windows**, haga doble clic en el archivo **PEAPWLAN.msi** y, a continuación, haga clic en **Siguiente** para iniciar la instalación.
3. Si desea instalar las secuencias de comandos en una ubicación que no sea la predeterminada C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools, especifíquela.
   Se le preguntará si desea instalar las secuencias de comandos para una sola cuenta o para todos los usuarios. Haga clic en **Todos los usuarios** y en **Siguiente** para continuar y, a continuación, vuelva a

hacer clic en **Siguiente** de nuevo para confirmar.

4. Tras completar la instalación, aparece el archivo **Tools Readme**. Este archivo contiene una renuncia importante y una breve descripción de las secuencias de comandos que se han instalado. Debe leerlo antes de continuar. Haga clic en **Siguiente** para continuar y, a continuación, haga clic en **Finalizar** para completar la instalación.

Para permitir un mejor acceso a estas secuencias de comandos, puede crear un acceso directo para abrir un shell de comandos en la carpeta donde se almacenan las secuencias de comandos.

Para crear un acceso directo a MSS WLANS Tools

1. Desde el **Explorador de Windows** desplácese a la carpeta **MSS WLAN Tools**, cuya ubicación predeterminada es C:\Archivos de programa\Microsoft\Microsoft WLAN-PEAP Tools.
2. Haga doble clic en el archivo de secuencia de comandos por lotes **CreateShortcut.cmd**. Esto crea un acceso directo denominado MSS WLAN Tools en el escritorio.
3. Puede que desee mover o copiar este acceso directo a su menú **Inicio**.

Utilización de las secuencias de comandos

Las secuencias de comandos se escriben en Windows Scripting Host utilizando lenguaje VBScript. Todas las secuencias de comandos funcionan de manera similar. Se deben ejecutar utilizando los dos archivos por lotes (MSSSetup.cmd y MSSTools.cmd) en lugar de ejecutarlos directamente. Los archivos por lotes simplifican la sintaxis de las secuencias de comandos.

La mayoría de las secuencias de comandos toman un solo parámetro que especifica la función que se va a realizar. Algunas secuencias de comandos toman parámetros adicionales (se explican en la guía). Las secuencias de comandos se ejecutan desde la carpeta en que se instalaron, es decir, desde un shell de comandos con el directorio de trabajo actual establecido en la carpeta de instalación de herramientas.

Las secuencias de comandos producen los siguientes tipos de resultados:

- Cuadros de mensaje que muestran información o texto de alerta, solicitud de decisión o solicitud de entrada de datos.
- Información de progreso detallada enviada a una ventana desplegable mientras la secuencia de comando se ejecuta. Si la secuencia de comandos encuentra un error, muestra información de error en la ventana. Cuando la ejecución de la secuencia de comandos se completa, se le solicita que cierre la ventana o que la deje abierta para una inspección posterior (por ejemplo, puede que desee mantener la ventana abierta para investigar errores).
- Para muchas tareas, la información de progreso detallada también se escribe en un archivo de registro (% systemroot%\debug\ MSSWLAN-Setup.log). Su finalidad es la de utilizarlo en la resolución de problemas y la auditoría de instalación. Todas las tareas de instalación y configuración, así como la exportación e importación de la configuración de IAS se archivan en este registro. Por razones de seguridad, las tareas que crean los secretos de RADIUS (contraseñas) para los puntos de acceso inalámbrico no se registran.

Principio de la página

Configuración de la infraestructura de directorio y de red

Configuración de la red

Debe conectar los componentes a la red como se muestra en la siguiente ilustración o según los requisitos específicos de su red.

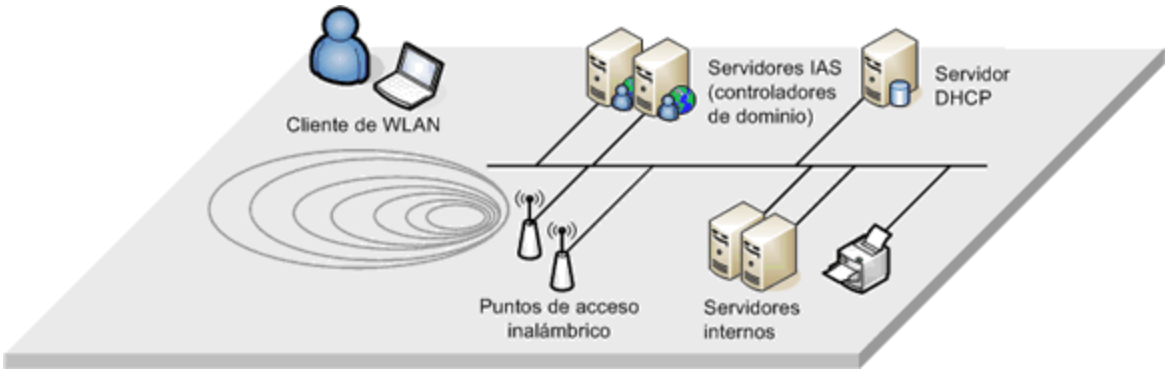

Figura 3.1 Configuraciones simples de red WLAN
Vista de imagen a pantalla completa

Esta ilustración muestra la configuración más simple posible, donde los servidores IAS, los puntos de acceso y el resto de su red interna se conectan a la misma LAN. En instalaciones de mayor tamaño, la red está, normalmente, segmentada en varias LAN virtuales (VLAN) que se conectan mediante enrutadores o conmutadores de nivel 3. La configuración precisa cambiará considerablemente dependiendo de los requisitos individuales de la organización. La descripción detallada de este tema no entra en el ámbito de esta guía.

Para obtener más información sobre la configuración de la red para una infraestructura de WLAN, consulte el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Windows Server 2003*.

Configuración de la red IP

La solución es, en gran parte, independiente de la distribución de la subred y la VLAN. Como se describe en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas", puede elegir tener sus clientes inalámbricos en una VLAN diferente del resto de la red. Sin embargo, esta solución sólo se ha probado para el caso más simple, es decir, para un sitio determinado, los clientes inalámbricos se colocan en la misma LAN que el resto de la red y comparten la misma subred IP.

Si elige tener sus clientes inalámbricos en una VLAN independiente, debe asignar una subred IP independiente para los clientes inalámbricos y enlazar la VLAN inalámbrica al resto de su red mediante un enrutador o un conmutador de nivel 3. Para entornos más complejos, hay ventajas en configurar subredes independientes para sus clientes WLAN en cada sitio físico. Estas ventajas incluyen:

- Puede mantener ámbitos de protocolo de configuración dinámica de host (DHCP) independientes para clientes con cable e inalámbricos; esto permite establecer un período de concesión mucho más corto para clientes WLAN.
- Si tiene un entorno enrutado con varias subredes en el mismo sitio, la asignación de una sola subred para todos los clientes WLAN en ese sitio permite a esos clientes desplazarse por los puntos de acceso manteniendo la misma dirección IP.
- Puede utilizar la subred de WLAN para definir un sitio de Active Directory y asociar la configuración de directiva de grupo con ese sitio. Sin embargo, no puede utilizar este mecanismo para aplicar la configuración de cliente WLAN del objeto de directiva de grupo descrita en el capítulo 6 "Configuración de clientes de LAN inalámbricas", ya que esta configuración necesita aplicarse a los clientes antes de que puedan conectarse correctamente a la WLAN.

DHCP

La información de direcciones IP y red IP necesita asignarse a los clientes WLAN. Esta solución utiliza el servicio DHCP de Windows para ello; así, debe haber un servicio DHCP para que lo utilicen los clientes WLAN.

Necesita asignar un ámbito DHCP independiente para cada subred donde implementará los clientes. Por ejemplo, si cuenta con dos sitios independientes con una conexión de red de área extensa (WAN) enrutada entre ellos, debe crear un ámbito DHCP para cada subred. Si va a asignar subredes independientes para sus clientes WLAN y LAN con cable, necesitará configurar un ámbito independiente para cada subred de WLAN.

Además, si ha enrutado conexiones entre sus puntos de conexión y sus servidores DHCP, necesitará configurar agentes de retransmisión DHCP en los enrutadores o instalar el agente de retransmisión DHCP de Windows en un servidor de la misma subred que los puntos de acceso.

Para una mayor disponibilidad, deberá considerar la utilización de una configuración DHCP resistente con ámbitos divididos, DHCP agrupados o configuraciones DHCP en espera. Para obtener más información sobre este tema, consulte el capítulo sobre implementación de DHCP del *Kit de distribución de Windows Server 2003*.

DNS

Active Directory depende de un servicio de sistema de nombres de dominio (DNS) que debe funcionar correctamente. Esta solución se basa en el supuesto de que tal servicio está en vigor y operativo. Tendrá instalado DNS como parte del proceso de instalación de Active Directory o lo tendrá configurado por separado.

Active Directory

Esta solución se ha diseñado y probado utilizando la siguiente configuración de Active Directory:

- Un bosque Active Directory de un solo dominio.
- Los controladores de dominio de Windows Server 2003 (recién instalados, no los actualizados desde los controladores de dominio de Windows 2000).
- Un nivel funcional de dominio del modo nativo de Windows 2000.

En muchos casos, es posible utilizar otras configuraciones de Active Directory, por ejemplo, mediante varios dominios o controladores de dominio de Windows 2000. En el texto se ofrece información adicional sobre la utilización de estas configuraciones, allí donde son compatibles con Microsoft. Sin embargo, estas configuraciones alternativas no forman parte de la solución principal probada.

Requisitos para todas las versiones de Active Directory

Un dominio en modo nativo permite crear grupos de seguridad universal de Active Directory. La utilización de grupos universales facilita la administración de directivas de acceso a redes de varios dominios. Sin embargo, para implementaciones de dominio único, esta configuración no tiene relevancia. Los comandos de instalación comprueban si el dominio está o no en modo nativo. Si el dominio está en modo nativo, la secuencia de comandos utilizará grupos universales pero, en caso contrario, sólo utilizará grupos globales.

Active Directory debe tener un esquema de Windows Server 2003. Es necesario para admitir la configuración de objetos de directiva de grupo de directivas de red inalámbrica. No hay necesidad de un nivel de funcionalidad de bosque Active Directory específico. En esta solución, se asume el nivel de funcionalidad de bosque de Windows 2000 predeterminado.

Para obtener más información sobre los conceptos de modo de dominio y bosque, consulte las referencias al final de este capítulo.

Utilización de los controladores de dominio de Windows 2000

En esta solución, IAS y los Servicios de Certificate Server se instalan en los sistemas de Windows Server 2003. No se ofrecen instrucciones para utilizar las versiones de Windows 2000 de estos componentes. Si está utilizando los controladores de dominio de Windows 2000 y no está pensando en actualizar ninguno a Windows Server 2003 debe actualizar el esquema al nivel de Windows 2003. Para obtener más información sobre la actualización del esquema, consulte la referencia al final de este capítulo.

Si esta solución se va a utilizar en un dominio o bosque utilizando controladores de dominio Windows 2000, debe asegurarse de que esos controladores de dominio tienen aplicado el Windows 2000 Service Pack 3 (SP3) o posterior. El Service Pack es necesario para asegurar que los controladores de dominio admiten firmas de protocolo ligero de acceso a directorios (LDAP). Ésta es una mejora de seguridad necesaria para los clientes de Windows XP y de entidad emisora de Windows Server 2003 que utilizan inscripción automática de certificados.

Comprobación de la seguridad de las directivas de cuenta de dominio

Esta solución se basa en contraseñas de usuario y equipo para autenticar usuarios y equipos para la WLAN. Por esta razón, es muy importante que no permita la utilización de contraseñas en blanco o poco seguras. Las

contraseñas fácilmente predecibles facilitarán a un atacante la entrada a la WLAN. Ya que se utilizan las mismas contraseñas para autenticar al usuario o al equipo en el dominio, esto proporcionará también acceso al atacante a todos los recursos de red.

La forma más fácil de eliminar las contraseñas no seguras es establecer directivas de contraseñas seguras en el objeto de directiva de grupo de la directiva de dominio predeterminada. También debe aplicar una caducidad periódica para las contraseñas, una vigencia mínima de la contraseña y una comprobación del historial de la contraseña (para asegurarse de que los usuarios no utilizan de nuevo la misma).

Advertencia: debe advertir a los usuarios y administradores antes de cambiar la directiva de contraseña de dominio. Para evitar la frustración y la confusión entre los usuarios, es buena idea informarles inicialmente sobre la nueva directiva de contraseñas que planea adoptar, junto con instrucciones sobre la elección de contraseñas seguras.

Para ver las prácticas recomendadas para la directiva de contraseña de dominio, consulte la *Guía de seguridad de Windows Server 2003*. Al final de este capítulo se ofrece referencia para este documento.

Creación de grupos de seguridad

Utilice el procedimiento que se ofrece más adelante en esta sección para crear grupos de seguridad en Active Directory que utilizará con esta solución. Los grupos creados se enumeran en la tabla siguiente y, donde se indica, se muestran sus miembros. De forma predeterminada, estos grupos se crean en el contenedor de usuarios.

Tabla 3.2. Miembros y grupos de seguridad

Grupo de seguridad	Finalidad	Tipo de grupo	Miembros
Usuarios de LAN inalámbrica	Especifica qué usuarios pueden autenticarse en la WLAN.	Global	Usuarios de dominio
Equipos de LAN inalámbrica	Especifica qué equipos pueden autenticarse en la WLAN.	Global	Equipos de dominio
Acceso a LAN inalámbrica	Este grupo se utiliza en la directiva de acceso de RADIUS para controlar el acceso a la WLAN.	Universal	Usuarios de LAN inalámbrica Equipos de LAN inalámbrica.
Configuración del equipo de LAN inalámbrica	Especifica qué equipos reciben configuración de WLAN de la directiva de grupo.	Dominio local	Equipos de LAN inalámbrica.

Para crear y llenar los grupos de seguridad

1. Abra un shell de comandos con el acceso directo **MSS WLAN Tools**.
2. En el símbolo del sistema, escriba *MSSSetup CreateWLANGroups* y, a continuación, presione **ENTRAR**.

   Importante: si ha movido los grupos de usuarios del dominio y de equipos del dominio de sus ubicaciones predeterminadas en el contenedor de usuarios, no se agregarán a los grupos de usuarios de LAN inalámbrica y equipos de LAN inalámbrica respectivamente. En ese caso, debe agregarlos a esos grupos de forma manual.

   Nota: si instala esta solución en un dominio de modo mixto, el grupo de acceso a la LAN inalámbrica se creará como un grupo global de dominio en lugar de un grupo universal. Esto indica que necesita crear uno de estos grupos en cada dominio si va a instalar esta solución en un bosque de varios dominios (esta tarea se describe en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas").

Si va a instalar esta solución en varios dominios, necesita crear los grupos globales de usuarios de LAN inalámbrica y equipos de LAN inalámbrica en cada dominio y agregarlos al grupo de acceso de LAN inalámbrica. También necesita crear un grupo local de dominio de configuración del equipo de LAN inalámbrica en cada dominio en el que tenga clientes WLAN y agregar el grupo universal de equipos de LAN inalámbrica como miembro.

Principio de la página

Preparación de los servidores

Esta sección cubre la configuración específica de servidor. Necesita realizar la mayoría de los procedimientos siguientes para cada servidor que desee instalar como servidor IAS. El procedimiento de la sección sobre configuración de seguridad del servidor es la única excepción porque, aunque la configuración de seguridad se aplique a cada servidor, este procedimiento sólo se debe ejecutar una vez por dominio. La configuración se aplica automáticamente a otros servidores del dominio.

Sistemas operativos compatibles

Esta solución se ha creado y probado utilizando Windows Server 2003, Standard Edition para todos los componentes de servidor. Sin embargo, las secuencias de comandos de la instalación y la guía son las mismas para Windows Server 2003, Enterprise Edition.

Debería leer la sección "Uso de Windows Server Standard o Enterprise Edition" del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas" antes de decidir si necesita utilizar Windows Server 2003, Enterprise Edition o no. La utilización de Windows Server 2003, Standard Edition limita la funcionalidad de los Servicios de Certificate Server y el número de puntos de acceso inalámbrico que puede admitir IAS que podrían (ambos o uno de los dos) no ser aceptados en grandes organizaciones.

Esta solución no se ha diseñado para admitir versiones anteriores de Windows Server y no se ha probado con ninguna de ellas. Estas versiones de Windows Server 2000 de IAS y Servicios de Certificate Server pueden funcionar para algunas o todas las funciones de servidor de esta solución, pero las instrucciones para ello quedan fuera del ámbito de esta documentación.

Directrices del hardware

El primer servidor que instale ejecutará los Servicios de Certificate Server así como IAS. Los Servicios de Certificate Server necesitan recursos mínimos en esta solución. Sin embargo, debería asegurar que la carga que IAS coloca en el servidor no afecta negativamente al rendimiento de sus funciones de controlador de dominio. Esto sólo suele ocurrir en las implementaciones de IAS más amplias. Si fuera necesario, debería agregar un controlador de dominio adicional al mismo sitio de Active Directory como compensación.

Si piensa activar el registro de RADIUS, deberá asignar un disco físico independiente para los registros.

Tabla 3.3. Hardware mínimo recomendado para el servidor IAS

Elemento	Requisito
CPU	Procesador a 733 MHz o superior
Memoria	256 MB
Interfaces de red	Adaptador único de red
Almacenamiento en disco	Controladora RAID SCSI o IDE 2 x 18 GB (SCSI) o 2 x 20 GB (IDE) configurado como volumen RAID 1 Almacenamiento local de medios extraíbles (CD-RW o cinta para copia de seguridad), si no hay ningún servicio de copia de seguridad en red. Unidad de disco de 1,44 MB para transferencia de datos.

Debería leer la sección "Requisitos del software y del hardware de IAS" del capítulo 2 "Planeamiento de la implementación de seguridad en LAN inalámbricas", para obtener más detalles sobre los requisitos de rendimiento de hardware.

Obtención e instalación de software compatible

Esta sección enumera el software adicional necesario en sus servidores. También describe cómo obtener e instalar el software.

Consola de administración de directivas de grupo

La consola de administración de directiva de grupo (GPMC) se utiliza para instalar y configurar los objetos de directiva de grupo utilizados por la solución. La GPMC sólo necesita instalarse en el primer servidor en el que se instala IAS, su instalación en servidores IAS posteriores es opcional.

Nota: la instalación de la GPMC cambia ligeramente la interfaz de usuario de los usuarios y equipos de Active Directory en el servidor en el que se ha instalado la GPMC. Para obtener más información sobre la utilización de la GPMC y descargas, consulte la referencia al final de este capítulo.

Para instalar la consola de administración de directivas de grupo

1. Descargue el archivo de instalación **Gpmc.msi** del Centro de descargas de Microsoft.
2. Asegúrese de que ha iniciado sesión como miembro del grupo de administradores de dominio (o el grupo de administradores locales del equipo en el que va a instalar la GPMC, si no lo va a instalar en un controlador de dominio).
3. En el **Explorador de Windows** haga doble clic en el archivo de instalación **Gpmc.msi**.
4. Siga las indicaciones del asistente para instalar la GPMC; acepte todas las opciones predeterminadas.

   Importante: debe instalar la GPMC en la carpeta de Archivos de programa (aunque no importa la unidad que esté activada). También debe utilizar la carpeta de instalación predeterminada —GPMC— de Archivos de programa (si cambia el nombre de la carpeta, debe actualizar el nombre de la carpeta utilizada para instalar la GPMC en el archivo Constants.txt). Los procedimientos posteriores utilizan algunas de las herramientas instaladas por la GPMC y si lo instala en cualquier otro lugar no podrán encontrar las herramientas de GPMC.

Herramientas de soporte técnico de Windows Server 2003

Los procedimientos y las secuencias de comandos de configuración de esta solución utilizan algunas de las herramientas de soporte técnico de Windows. Debe instalarlas desde el disco de instalación de Windows Server 2003. Las secuencias de comandos de configuración e instalación de entidades emisoras las necesitan, así que debe instalarlas en el servidor en el que se van a instalar los Servicios de Certificate Server. No son necesarias, sin embargo, en los otros servidores aunque puede que desee instalarlas.

Para instalar las herramientas de soporte técnico de Windows Server 2003

1. Asegúrese de que ha iniciado sesión como miembro del grupo de administradores de dominio (o el grupo de administradores locales del equipo en el que está instalando las herramientas de soporte técnico, si no lo está instalando en un controlador de dominio).
2. Inserte el **CD** de **instalación de Windows Server 2003** (o conéctese a la fuente de instalación si va a instalar desde la red o desde otros discos).
3. Desde el **Explorador de Windows**, desplácese a la unidad de discos de instalación (unidad de CD o de disquete) y, a continuación, al archivo **\support\tools\supptools.msi**. Haga doble clic en el archivo para empezar la instalación.
4. Siga las indicaciones del asistente para instalar las herramientas de soporte y acepte el contrato de

licencia y la carpeta de instalación predeterminada.

CAPICOM

CAPICOM es una interfaz convertible en secuencias de comandos en un conjunto de funciones de seguridad de Windows conocido como CryptoAPI (CAPI). CAPICOM es necesario para las secuencias de comandos de control de estado de los Servicios de Certificate Server y para crear los secretos de RADIUS utilizados para autenticar los puntos de acceso inalámbrico. Debe instalar la versión 2.0 o posterior de CAPICOM en todos los servidores IAS de su organización.

Puede encontrar la última versión de CAPICOM 2.0 en el Centro de descargas de Microsoft (consulte la sección "Referencias" al final de este capítulo).

El archivo de distribución de CAPICOM no contiene una instalación automática; por ello debe utilizar la secuencia de comandos por lotes InstCAPICOM.cmd (suministrada con esta solución). Si desea llevar a cabo estos pasos de forma manual, puede copiar los comandos de la secuencia de comandos por lotes.

Para instalar CAPICOM

1. Descargue el archivo de distribución de **CAPICOM**, **CCR2INST.exe**, del Centro de descargas de Microsoft y cópielo en una carpeta temporal del servidor.
2. Asegúrese de que ha iniciado sesión como miembro del grupo de administradores de dominio (o el grupo de administradores locales del equipo en el que está instalando CAPICOM, si no lo está instalando en un controlador de dominio).
3. Abra un shell de comandos con el acceso directo **MSS WLAN Tools**.
4. En el símbolo del sistema, escriba:

   InstCAPICOM [d:]PathtoCCDistFile\CCR2INST.EXE y, a continuación, presione **ENTRAR**.

   Nota: sustituya *[d:]RutaArchivoDistribuciónCAPICOM* con la ruta completa (incluyendo la letra de la unidad, si es una distinta) de la carpeta en la que copió el archivo de distribución de CAPICOM.

Microsoft Baseline Security Analyzer (MBSA)

Esta herramienta es necesaria para comprobar que las actualizaciones de seguridad del sistema operativo son actuales y detectar posibles problemas con la configuración de seguridad de los servidores. Necesita utilizar la versión 1.1.1 o posterior de MBSA para explorar los sistemas de Windows Server 2003. Puede encontrar la última versión de MBSA en el Centro de descargas de Microsoft.

Para instalar MBSA

1. Descargue el archivo de instalación **mbsasetup.msi** del Centro de descargas de Microsoft.
2. Asegúrese de que ha iniciado sesión como miembro del grupo de administradores de dominio (o el grupo de administradores locales del equipo en el que está instalando MBSA, si no lo va a instalar en un controlador de dominio).
3. En el **Explorador de Windows**, desplácese al archivo **mbsasetup.msi** y haga doble clic en él.
4. Siga las indicaciones del asistente para instalar el MBSA; acepte todas las opciones predeterminadas.

Configuración de seguridad del servidor

En esta sección se describe cómo aplicar directivas de seguridad y otras medidas de seguridad a Windows Server 2003 antes de instalar IAS y Servicios de Certificate Server.

Esta solución está diseñada para instalarse en servidores existentes (normalmente controladores de dominio). La configuración de seguridad utilizada en esta sección es intencionadamente conservadora por el peligro que representa un conflicto entre la configuración de seguridad y los servicios y las aplicaciones instaladas que pueden estar ejecutándose en el servidor.

Utilización de la Guía de Seguridad de Windows Server 2003

Windows Server 2003 cuenta con una configuración de seguridad predeterminada segura. Para la mayoría de las organizaciones, esta configuración ofrece una buena protección para su sistema si se combina con un proceso de mantenimiento de actualizaciones efectivo (para obtener más detalles sobre el mantenimiento de actualizaciones, consulte la sección "Actualizaciones de seguridad del servidor" que aparece más adelante en este capítulo). Sin embargo, también debe tener en cuenta las recomendaciones descritas en la *Guía de seguridad de Windows Server 2003*. Esta guía define configuraciones de seguridad adecuadas para distintas funciones de servidor.

Los servidores utilizados en esta solución realizan varias funciones de servidor definidas en la *Guía de seguridad*; las funciones de controlador de dominio y de servidor de RADIUS para la mayoría de los servidores y, en el caso del servidor principal, también realiza la función de entidad emisora de certificados. Para cada función, la guía define una plantilla de seguridad con todas las configuraciones de seguridad adecuadas para esa función. Para un servidor con varias funciones, deberá aplicar una combinación de las plantillas de seguridad que correspondan a cada una de las funciones independientes del servidor. En sus servidores, también puede tener otros servicios de infraestructura como DNS, DHCP y el servicio de nombres de Internet de Windows (WINS), en cuyo caso necesita incluir las plantillas de seguridad adecuadas a estas funciones. Para obtener instrucciones sobre cómo llevarlo a cabo, consulte la *Guía de seguridad de Windows Server 2003*.

Advertencia: las plantillas de configuración de seguridad de la *Guía de seguridad de Windows Server 2003* desactivan específicamente un número de servicios que no son necesarios para las funciones de servidor definidas. Si dispone de cualquier otra aplicación o servicio en los servidores, debe probarlos para asegurarse de que las plantillas de seguridad no desactivan servicios ni cambian ninguna configuración de seguridad de la que dependen sus aplicaciones o servicios. Las instrucciones para combinar funciones y cambiar configuraciones para albergar otras aplicaciones también se incluyen en la *Guía de seguridad de Windows Server 2003*.

Aplicación de la configuración de seguridad

Al contrario que la mayoría de los otros procedimientos de la sección "Preparación de los servidores" de este capítulo, este procedimiento no necesita llevarse a cabo en cada servidor. En su lugar, las configuraciones se importan en un objeto de directiva de grupo de Active Directory y, a continuación, se aplican de forma global a todos los servidores.

Sólo hay dos tipos de configuraciones de seguridad aplicadas en esta solución. El primer tipo se aplica para configurar todos los servicios necesarios para iniciar automáticamente (en caso de que otra directiva de seguridad aplicada al equipo lo detenga o lo desactive). El segundo tipo se aplica para cambiar la directiva de auditoría de forma que los errores de auditoría para sucesos comunes (como inicio de sesión) también se guarden en el registro de seguridad.

La tabla siguiente muestra los servicios configurados para iniciarse automáticamente.

Tabla 3.4. Servicios de Windows activados por directiva

Servicio	Configuración de directiva
Servicios de Certificate Server	Automático
Servicio de autenticación de Internet	Automático
Proveedor de instantáneas de software de Microsoft	Automático
Almacenamiento de medios extraíbles	Automático
Programador de tareas	Automático
Instantáneas de volumen	Automático

La tabla siguiente muestra las categorías de auditoría donde se activa la auditoría de errores además de la auditoría de aciertos predeterminada.

Tabla 3.5. Configuración de directiva de auditoría

Directiva de auditoría	Valor de configuración
Auditar sucesos de inicio de sesión de cuenta	Acierto/Error (sólo Acierto como valor predeterminado)
Auditar sucesos de administración de cuentas	Acierto/Error (sólo Acierto como valor predeterminado)
Auditar sucesos de inicio de sesión	Acierto/Error (sólo Acierto como valor predeterminado)
Auditar sucesos de cambio de directivas	Acierto/Error (sólo Acierto como valor predeterminado)

La habilitación de los valores de configuración de auditoría contemplados en la tabla aumentará los requisitos de almacenamiento para el registro de seguridad. Debe asegurarse de que se han establecido tamaños adecuados para los registros de sucesos en los controladores de dominio. El tamaño predeterminado para los registros de sucesos en Windows Server 2003 es más que adecuado, pero Windows 2000 utilizaba tamaños predeterminados que solían ser demasiado pequeños para un uso práctico (esta configuración puede ser aún efectiva si ha actualizado desde Windows 2000). En el capítulo 5, "Creación de la infraestructura de seguridad de LAN inalámbricas", comprobará cómo los servidores IAS están configurados para registrar todas las conexiones WLAN, sean correctas o erróneas, en el registro del sistema de Windows. Debe asegurarse de que se han establecido tamaños adecuados para los registros de seguridad y de sistema en los controladores de todos los dominios. Windows Server 2003 utiliza 16 MB para los registros del sistema y de la aplicación y 128 MB para los registros de seguridad: estos valores son adecuados para esta solución.

Importación del objeto de directiva de grupo de la configuración de seguridad
El siguiente procedimiento importa la configuración descrita en la sección anterior en el dominio, pero no la aplica a ningún servidor.

Para instalar en su dominio el objeto de directiva de grupo de la configuración de seguridad

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. En el símbolo del sistema, escriba el siguiente comando para importar en el dominio el objeto de directiva de grupo llamado Directivas de seguridad del servidor IAS:

   MSSSetup ImportSecurityGPO, y, a continuación, presione **ENTRAR**.

Aplicación de la configuración de seguridad en los controladores de todos los dominios
En este procedimiento, la configuración de seguridad se aplica a los controladores de todos los dominios (con o sin IAS instalado). No debería provocar ningún efecto adverso en las funciones de los controladores de dominio o en cualquier otra aplicación o servicio que se ejecute en ellos, puesto que el objeto de directiva de grupo no tiene ningún parámetro que deshabilite funcionalidades. Si no desea aplicar esta configuración a los controladores de su dominio, consulte el procedimiento que sigue inmediatamente a éste.

Para aplicar la configuración a los controladores de todos los dominios, necesita vincular el objeto de directiva de grupo importado a la unidad organizativa de controladores de dominio. El objeto de directiva de grupo se vincula manualmente debido al riesgo de sobrescribir los valores de este objeto ya configurados en su dominio.

Para aplicar la configuración de seguridad en los controladores de todos los dominios

1. Para iniciar la **consola de administración de directiva de grupo**, haga clic en **Inicio**, **Todos los programas**, **Herramientas administrativas** y, a continuación, en **Administración de directiva de grupo**.
2. Desplácese hasta la unidad organizativa de los **controladores de dominio** en el panel izquierdo y haga

clic sobre ella.

Esta unidad debe aparecer justo debajo del objeto dominio.

3. Haga clic con el botón secundario en el nombre de la unidad organizativa y, a continuación, en **Vincular objeto de directiva de grupo existente**.

4. En la lista de objetos, haga clic en **Directivas de seguridad del servidor IAS** y, a continuación, haga clic en **Aceptar** para volver a la ventana principal de la consola.

5. En el panel derecho, asegúrese de que la ficha **Objetos de directiva de grupo vinculados** está seleccionada; a continuación, haga clic en el objeto de directiva de grupo **Directivas de seguridad del servidor IAS**.

6. Haga clic en el símbolo con doble flecha hacia arriba que se encuentra justo a la izquierda de esta lista para mover este objeto a la prioridad más alta.

   Esto garantiza que los servicios requeridos permanecerán habilitados independientemente de otras directivas de seguridad aplicadas a los controladores de dominio.

7. Cierre la **consola de administración de directiva de grupo**.

   La configuración de seguridad se aplicará a los servidores en el siguiente intervalo de actualización de objetos de directiva de grupo (el intervalo de actualización predeterminado es de cinco minutos para los controladores de dominio).

Aplicación de la configuración de seguridad sólo en los servidores IAS
Si no desea que la configuración de seguridad se aplique a los controladores de todos los dominios (o si ha optado por no instalar IAS en los controladores de dominio), puede crear una unidad organizativa aparte para los servidores IAS y, a continuación, aplicar a ésta el objeto de directiva de grupo. Si no está instalando IAS en los controladores de dominio, debe crear la unidad organizativa de los servidores IAS en alguna otra parte del dominio.

Para aplicar la configuración de seguridad sólo a los servidores IAS

1. Para iniciar la **consola de administración de directiva de grupo**, haga clic en **Inicio**, **Todos los programas**, **Herramientas administrativas** y, a continuación, en **Administración de directiva de grupo**.

2. Desplácese hasta la unidad organizativa de los **controladores de dominio** en el panel izquierdo y haga clic sobre ella.

   Esta unidad organizativa se encuentra justo debajo de la raíz del dominio.

3. Cree una nueva unidad organizativa de nivel secundario debajo de esta unidad. Para ello, haga clic con el botón secundario en el nombre de la unidad organizativa de **controladores de dominio** y, a continuación, seleccione **Nueva unidad organizativa** del menú emergente.

4. Escriba un nombre para la unidad cuando se le solicite, por ejemplo, *Servidores IAS*.

5. Haga clic con el botón secundario en esta unidad organizativa y, a continuación, en **Vincular objeto de directiva de grupo existente**.

6. En la lista de objetos, seleccione **Directivas de seguridad del servidor IAS** y, a continuación, haga clic en **Aceptar** para volver a la ventana principal de la consola.

7. Cierre la **consola de administración de directiva de grupo**.

8. Mueva el objeto equipo de cada controlador de dominio combinado y el servidor IAS desde la unidad organizativa de **controladores de dominio** hasta la nueva unidad organizativa de nivel secundario.

   La configuración de seguridad se aplicará a los servidores en el siguiente intervalo de actualización de

objetos de directiva de grupo (el intervalo de actualización predeterminado es de 5 minutos para los controladores de dominio y de 90 minutos para otros equipos).

Nota: si va a instalar servidores IAS en varios dominios, necesita volver a instalar y vincular los objetos de directiva de grupo para cada dominio del bosque.

Comprobación de la configuración de seguridad
Para comprobar que se ha aplicado la configuración de seguridad

1. Desde un shell de comandos, en el símbolo de sistema, escriba:

   *gpupdate /force*y, a continuación, presione **ENTRAR**.

2. En el registro de **sucesos de aplicación**, compruebe los sucesos de origen **SceCli** (puede tardar unos segundos en aparecer). Debe aparecer registrada una Id. de suceso 1704. El texto del suceso debe ser:

   Se ha aplicado satisfactoriamente la directiva de seguridad en los objetos de directiva de grupo.

Actualizaciones de seguridad del servidor

A diferencia de la configuración de seguridad del objeto de directiva de grupo, es necesario comprobar y aplicar las actualizaciones de seguridad en cada servidor. Si tiene que administrar pocos servidores, puede utilizar procedimientos manuales. Si tiene muchos servidores y aún no dispone de un sistema de mantenimiento actualizado automático, la comprobación y aplicación manuales de actualizaciones en todos los servidores puede ser una tarea extremadamente tediosa. En cambio, debe considerar automatizar la aplicación de actualizaciones de seguridad mediante Microsoft Software Update Service (SUS) o Microsoft Systems Management Server (SMS) 2003. Para obtener más información sobre su uso, consulte la *Microsoft Guide to Security Patch Management*.

Comprobación de actualizaciones de seguridad actuales

Existen dos formas de comprobar la versión de las actualizaciones de seguridad de su servidor, en concreto Windows Update y Microsoft Baseline Security Analyzer (MBSA). Existen también otras herramientas, que realizan funciones similares, facilitadas por proveedores distintos a Microsoft.

Windows Update
Windows Update es un servicio en línea diseñado principalmente para su uso por parte de pequeñas empresas y de usuarios en casa, aunque no existe ninguna restricción sobre los usuarios del servicio. Dado que Windows Update exige estar conectado a Internet, no debe utilizar este servicio sin proteger el servidor con un servidor de seguridad.

Para obtener más información sobre Windows Update, consulte las referencias al final de este capítulo.

Microsoft Baseline Security Analyzer
MBSA es una herramienta de evaluación de seguridad que comprueba la existencia de problemas de seguridad en el sistema, incluidas las actualizaciones que faltan. Para obtener más información sobre MBSA, consulte las referencias al final de este capítulo.

Para comprobar las actualizaciones de seguridad instaladas con MBSA

1. Si su servidor no tiene conectividad con Internet, debe obtener cada vez la versión actual de la base de datos de seguridad de MBSA antes de ejecutar la comprobación. Se trata de un archivo XML, **msecure.xm.**, que se puede descargar de la URL facilitada al final de este capítulo. Copie este archivo a la carpeta en la que ha instalado MBSA (la carpeta predeterminada es C:\Archivos de programa\Microsoft Baseline Security Analyzer).

2. Para comprobar el estado de actualización actual del servidor, escriba en el símbolo del sistema:

   Mbsacli /hf -v y, a continuación, presione **ENTRAR**.

3. Anote las actualizaciones de seguridad que faltan. Éstas se muestran como sigue:

* WINDOWS SERVER 2003, STANDARD EDITION GOLD

Nota MS03-030 819696

Para obtener una explicación pormenorizada, consulte Q306460.

4. Puede obtener la actualización de seguridad asociada a cada actualización de seguridad que le falte con la ayuda de su explorador Web, el cual le dará acceso al artículo de Microsoft Knowledge Base relacionado. Escriba la siguiente dirección URL en el explorador:

   http://support.microsoft.com/default.aspx?kbid=XXXXXX

   Nota: debe reemplazar XXXXXX con el número o números del artículo de Microsoft Knowledge Base enumerado(s) en los resultados de MBSA (por ejemplo, 819696 en el ejemplo anterior).

5. Instale cada actualización según las instrucciones del artículo de Microsoft Knowledge Base.

Utilización de MBSA para comprobar otros problemas de seguridad

Además de para comprobar que las actualizaciones de seguridad sean las últimas, debe utilizar MBSA para comprobar en el servidor otros problemas potenciales de seguridad. Para ello, ejecute la versión gráfica (desde el menú **Inicio**), explore el servidor y actúe según las advertencias.

En concreto, debe prestar atención a las cuentas de usuario detectadas con contraseñas en blanco, inseguras o sin límite de validez. No obstante, no modifique la configuración de ninguna cuenta integrada como krbtgt.

A menos que cambie la configuración predeterminada de la zona de seguridad de Internet Explorer, puede hacer caso omiso a las advertencias de MBSA sobre configuraciones no estándar. La configuración predeterminada de Windows Server 2003 es más segura que la configuración de las zonas de Internet Explorer que está comprobando MBSA.

El procedimiento expuesto en este capítulo sólo cubre la ejecución de MBSA para explorar el equipo local. El procedimiento para ejecutarlo y explorar los equipos de la red está fuera del alcance de estas instrucciones. Para obtener más detalles sobre el uso de MBSA, consulte la referencia al final del capítulo.

Administración e instalación de actualizaciones en los servidores

La cobertura total de la administración de actualizaciones automáticas continuas está fuera del alcance de estas instrucciones. No obstante, debe ser consciente de las tres formas principales que existen para la administración continua de las actualizaciones del sistema mediante la tecnología Microsoft.

AutoUpdate

AutoUpdate es un servido integrado en los servidores y clientes Windows que permite que cada equipo compruebe y descargue toda revisión de seguridad importante conforme son publicadas por Microsoft. Dispone de la opción para que las actualizaciones se instalen de manera automática. Esto requiere que cada equipo tenga acceso al Web (HTTP). En esta ocasión, también debe tener la precaución de contar con la protección de un servidor de seguridad adecuado para cada dispositivo (consulte la sección "Windows Update").

Para obtener más información sobre AutoUpdate, consulte las referencias al final de este capítulo.

Software Update Service

Software Update Service (SUS) perfecciona el servicio de AutoUpdate. Elimina la necesidad de que cada equipo esté conectado a Internet mediante la centralización de la comprobación de actualizaciones y la descarga de la funcionalidad en un equipo central o en varios. El administrador puede entonces aprobar o rechazar las actualizaciones descargadas en el servidor o servidores SUS. Todos los equipos de la organización recuperan todas las actualizaciones aprobadas. Estos equipos utilizan el servicio AutoUpdate para comprobar y descargar las actualizaciones desde el servidor o servidores SUS, en lugar de hacerlo desde el sitio Web de Windows Update.

Para obtener instrucciones sobre cómo implementar SUS, consulte *Patch Management Using Microsoft Software Update Services*. La dirección URL del mismo se proporciona al final de este capítulo.

Administración de las actualizaciones con Microsoft Systems Management Server

Con Microsoft SMS 2003, puede automatizar completamente la distribución de los Service Pack, las

actualizaciones de seguridad y las de software. SMS 2000 con el Software Update Services Feature Pack integra las características de SUS con las capacidades más amplias de SMS. Tanto SMS 2000 como SMS 2003 incluyen la capacidad de programar las exploraciones de MBSA de todos los equipos de la organización. Si desea obtener más información acerca del uso de SMS, consulte los siguientes documentos:

- *Patch Management Using Microsoft Systems Management Server 2003*
- *Patch Management Using Microsoft Systems Management Server 2.0*

Las direcciones URL de estos documentos se proporcionan al final del capítulo.

Principio de la página

Resumen

Este capítulo ha ofrecido instrucciones sobre la preparación de la red, de Active Directory, de los controladores de dominio y de otros elementos del entorno para instalar una infraestructura de WLAN segura. Las secuencias de comandos utilizadas para configurar esta solución se instalaron junto con una serie de herramientas de soporte técnico. Los grupos de seguridad utilizados por la solución se crearon en el dominio y la configuración de seguridad se importó y aplicó a los servidores. Por último, la versión de las actualizaciones de seguridad en los servidores se examinó y se corrigió si procedía.

El capítulo siguiente versa sobre la instalación de los Servicios de Certificate Server en el servidor principal instalado para crear la entidad emisora de certificados de red.

Principio de la página

Referencias

Esta sección ofrece referencias a otra información complementaria importante u otro material informativo de relevancia para el contenido de este capítulo.

- El capítulo sobre las LAN inálámbricas del Kit de distribución de Microsoft Windows Server 2003 se puede consultar en la siguiente dirección URL:

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

- Para obtener más información sobre los niveles funcionales de dominio en Active Directory y sobre las instrucciones acerca de cómo cambiar entre ellos, consulte las siguientes secciones de la documentación de Windows Server 2003 en las siguientes URL:

  - Esta sección describe los distintos niveles de bosque y de dominio:

    http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_levels.mspx

  - Esta sección describe cómo cambiar los niveles de bosque y de dominio:

    http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/sag_changedomlevel.mspx

- Para obtener información detallada sobre la actualización del esquema de Active Directory en Windows 2000 al nivel de Windows Server 2003, consulte la página del documento ADPrep en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/adprep.mspx

- Para obtener más información sobre la descarga y utilización de la consola de administración de directivas de grupo, consulte la siguiente dirección URL:

  http://go.microsoft.com/fwlink/?LinkID=8630

- Para descargar la versión 2.0.0.3 de CAPICOM, consulte la siguiente dirección URL:

  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=860EE43A-A843-462F-ABB5-FF88EA5896F6

  No obstante, para asegurarse de que se trata de la última versión, busque "CAPICOM" en la siguiente dirección URL:

  http://www.microsoft.com/downloads

- Para obtener instrucciones sobre la descarga y utilización de Microsoft Baseline Security Analyzer (MBSA), consulte la siguiente dirección URL:

  http://www.microsoft.com/technet/security/tools/mbsahome.mspx

- Para descargar la base de datos más reciente de Microsoft Patch (mssecure.xml) en forma de archivo CAB firmado, consulte la siguiente dirección URL:

  http://download.microsoft.com/download/xml/security/1.0/nt5/en-us/mssecure.cab

- La Guía de seguridad de Microsoft Windows Server 2003 está disponible en:

  http://go.microsoft.com/fwlink/?LinkId=14845

- Para obtener más información sobre Windows Update, consulte la siguiente dirección URL:

  http://v4.windowsupdate.microsoft.com/en/default.asp

- Para obtener más información sobre la utilización de AutoUpdate, consulte el artículo en la siguiente dirección URL:

  http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/standard/autoupdate_top.mspx

- Consulte la administración de revisiones, actualizaciones de seguridad y páginas de descarga en la siguiente dirección URL:

  http://www.microsoft.com/technet/security/topics/patch/default.mspx

- La URL anterior ofrece vínculos a las siguientes guías y a otras relevantes:
  - Patch Management Using Microsoft Software Update Services
  - Patch Management Using Microsoft Systems Management Server 2003
  - Patch Management Using Microsoft Systems Management Server 2.0

(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