Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 5: Creación de la infraestructura de seguridad de LAN inalámbricas

Actualizado: abril 2, 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

En este capítulo se proporcionan instrucciones para la instalación y configuración del Servicio de autenticación de Internet (IAS) con el fin de proporcionar servicios del Servicio de usuario de acceso telefónico de autenticación remota (RADIUS) para una red de área local inalámbrica (WLAN) y la configuración de puntos de acceso inalámbricos para utilizar los servicios RADIUS de IAS.

Los temas principales del capítulo son los siguientes:

- Preparación e instalación de IAS
- Configuración del servidor IAS principal
- Replicación de la configuración en otros servidores IAS
- Adición de puntos de acceso inalámbrico como clientes RADIUS a IAS
- Configuración de los puntos de acceso inalámbricos

Los procedimientos de este capítulo son menos automatizados que los de capítulos anteriores. Aunque se puede configurar IAS de forma programada, algunos valores de configuración no se pueden configurar utilizando Windows® Scripting Host ni herramientas de línea de comandos disponibles. El código de aplicaciones compilado suele ser menos accesible que las secuencias de comandos para aquellos usuarios que no son programadores. Por ese motivo, cuando un procedimiento no se ha podido convertir en secuencias de comandos, se siguen los pasos del manual para completarlo. Si desea automatizar la configuración de IAS mediante la interfaz Objetos de datos del servidor, consulte MSDN® en http://msdn.microsoft.com. Para conocer la ubicación exacta de la información sobre este tema, consulte las referencias al final de este capítulo.

Los pasos de configuración descritos en este capítulo son mayormente manuales; este hecho tiene algunos aspectos positivos. En primer lugar, la interfaz de administración de IAS es fácil de utilizar y suele estar controlada por asistentes de configuración. En segundo lugar, los pasos de configuración se realizan normalmente en un único servidor y, más adelante, esta configuración se replica en los demás servidores IAS mediante unos sencillos comandos. En tercer lugar, la realización manual de estos pasos le ayudará a saber más sobre la instalación y configuración de IAS. Este último punto es más relevante para este componente de la solución que para los otros. IAS es el concentrador alrededor del cual gira el resto de la solución, por lo que es recomendable tener algo de experiencia en la administración y configuración del mismo.

Principio de la página

Requisitos previos del capítulo

Antes de implementar las instrucciones proporcionadas en este capítulo, debe leer e implementar los procedimientos del capítulo 3, "Preparación del entorno", y 4, "Creación de la entidad emisora de certificados de red". También debe leer el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas", y conocer la arquitectura y el diseño de esta solución.

Además, resultará útil que esté familiarizado con los siguientes temas:

- IAS y RADIUS
- Conceptos de WLAN

Principio de la página

Preparación para la implementación

Permisos necesarios

Para llevar a cabo los procedimientos de este capítulo, debe iniciar sesión con una cuenta que pertenezca al grupo de administradores del dominio en el que se van a instalar los servidores IAS.

Nota: si no va a instalar IAS en controladores de dominio, sólo deberá pertenecer al grupo de administradores locales en cada servidor IAS donde se va a instalar y configurar IAS. También deberá tener permisos para modificar la pertenencia al grupo Servidores RAS e IAS del dominio en el que se van a instalar los servidores IAS.

Herramientas necesarias

Para realizar los procedimientos de este capítulo son necesarias las siguientes herramientas.

Tabla 5.1. Herramientas necesarias

Herramienta	Descripción	Fuente
Secuencias de comandos para la seguridad en WLAN de MSS	Conjunto de secuencias de comandos y herramientas que se incluyen en esta solución.	Se proporciona en el capítulo 3, "Preparación del entorno".
Servicio de autenticación de Internet	Herramienta de Microsoft® Management Console (MMC) utilizada para administrar la configuración y las directivas de IAS.	Se proporciona como parte de Windows Server™ 2003.
Usuarios y equipos de Active Directory	Herramienta de MMC utilizada para administrar los equipos, grupos y usuarios del servicio de directorio de Microsoft Active Directory®, así como otros objetos de Active Directory.	Se proporciona como parte de Windows Server 2003.

Parámetros de IAS

En la siguiente tabla se muestran los parámetros principales utilizados en la instalación y configuración del servidor IAS.

Tabla 5.2. Parámetros de configuración del servidor IAS

Elemento de configuración	Valor de configuración
Registro IAS en el registro de sucesos de Windows	
Solicitudes de autenticación rechazadas	Habilitado
Solicitudes de autenticación correctas	Habilitado
Registro de RADIUS IAS	Deshabilitado
Directiva de acceso remoto	
Nombre de directiva de acceso remoto	Permitir acceso a LAN inalámbrica
Grupo de seguridad al que se concede acceso	Acceso a LAN inalámbrica
Tipo de EAP utilizado	Protocolo de autenticación extensible protegido (PEAP)
Tipo de PEAP utilizado	EAP MS-CHAP v2
Reconexión rápida	Habilitado
Perfil de directiva de acceso remoto	
Minutos que el cliente puede estar conectado (tiempo de espera de sesión)	60 minutos Se puede reducir a 15 minutos para redes WLAN 802.11a/g de 54 Mbps
Atributos de RADIUS	Ignorar propiedades de acceso telefónico del usuario = "True" Acción-Terminación = "RADIUS-Request"
Directiva de solicitud de conexión	
Nombre de directiva	Usar autenticación de Windows para todos los usuarios
Condiciones de la directiva	Restricciones de fecha y hora = Todas las horas

Importante: esta configuración se utilizó en las pruebas internas de esta solución y su funcionamiento está garantizado tal y como se describe. Aunque se pueden modificar algunos valores de esta configuración, sólo debería hacerlo si está seguro de que comprende perfectamente la finalidad de un valor de configuración concreto y lo que implicaría su modificación.

Principio de la página

Comprobación de la preparación para la instalación

IAS depende de la correcta configuración y conectividad de la red y de Active Directory. Para la instalación y el mantenimiento adecuados de IAS son necesarias varias herramientas.

Validación del entorno IAS

Antes de instalar IAS en el servidor, debe realizar una serie de comprobaciones para garantizar que puede ponerse en contacto con el controlador de dominio y que se han instalado todas las herramientas necesarias siguiendo los procedimientos descritos en el capítulo 3, "Preparación del entorno". El siguiente procedimiento utiliza una secuencia de comandos para realizar estas comprobaciones por usted de forma automática.

Para comprobar el entorno IAS

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools** que se encuentra en el servidor en el que desea instalar IAS.
2. Ejecute el comando siguiente:

   MSSSetup CheckIASEnvironment

3. La secuencia de comandos confirma el nombre del dominio al que pertenece el servidor. Haga clic en **Aceptar** para confirmar.
4. Cuando finalice las comprobaciones, aparecerá un cuadro de diálogo indicando si cada una de ellas se ha realizado correctamente o no. Haga clic en **Aceptar** para cerrar el cuadro de diálogo.
5. Si todas las comprobaciones se realizaron correctamente, continúe con el siguiente procedimiento. De lo contrario, compruebe el registro de instalación (**%systemroot%\debug\MSSWLAN-Setup.log**) para determinar la causa del error y corregir el problema antes de volver a ejecutar la secuencia de comandos.

Comprobación de la configuración de DHCP

El protocolo de configuración dinámica de host (DHCP) se utilizará para asignar automáticamente direcciones IP a los clientes WLAN. Asegúrese de que los ámbitos DHCP asignados en cada sitio disponen de suficientes direcciones IP para abarcar el máximo número posible de clientes WLAN que pueden estar activos en el sitio. Si el ámbito se comparte con clientes por cable, debe ser lo suficientemente grande como para dar cabida a ambos conjuntos de clientes.

Las organizaciones con un número elevado de clientes WLAN o que tengan clientes de WLAN que se desplacen regularmente de un sitio a otro, deben configurar ámbitos distintos para ellos. Al disponer de distintos ámbitos, se pueden especificar tiempos de concesión muy breves para dichos clientes (por ejemplo, ocho horas o menos) y, de esta forma, se evita que los clientes WLAN transitorios agoten las direcciones IP disponibles. Para ello, coloque a los clientes WLAN en una subred distinta de la red de sitios y configure un enrutador o un conmutador de nivel 3 para conectar las subredes.

En entornos pequeños o relativamente estáticos, la opción de compartir una subred IP y un ámbito DHCP único entre clientes por cable y de WLAN es bastante aceptable.

Para obtener más información, consulte el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Microsoft Windows Server 2003*. La referencia del mismo se proporciona al final de este capítulo.

Principio de la página

Instalación de IAS

En esta sección se describe cómo instalar IAS en el servidor.

Instalación de componentes de software de IAS

Puede instalar los componentes de software de IAS utilizando la secuencia de comandos que se proporciona en esta guía. Esta secuencia de comandos utiliza el administrador de instalación de componentes opcionales de Windows para instalar IAS y crea todos los archivos de configuración necesarios a medida que se ejecuta.

Para instalar IAS

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el siguiente comando para instalar los componentes de software de IAS:

   MSSSetup InstallIAS

3. La secuencia de comandos creará el archivo de parámetros de instalación. Cuando finalice esta operación, se le solicitará que continúe con la instalación. Necesitará el CD de instalación de Windows Server 2003 (o la ruta de red que contiene el origen de instalación de Windows) para finalizar la instalación. Haga clic en **Aceptar** para continuar o en **Cancelar** para detener la instalación antes de que finalice.

   Nota: si decide cancelar la instalación, el archivo de parámetros de componentes opcionales de IAS (OC_IAS.txt) permanecerá en la carpeta de trabajo actual. Puede modificar la ubicación y usarla en la instalación personalizada si no desea aceptar los valores predeterminados de la solución.

4. Cuando finalice la instalación, se mostrará un mensaje de confirmación. Haga clic en **Aceptar**.

Comprobación de la instalación

Para comprobar la instalación, haga clic en **Inicio**, elija **Todos los programas**, seleccione **Herramientas administrativas** y haga clic en **Servicio de autenticación de Internet**. IAS debe aparecer tal y como se instaló y ejecutándose en el servidor.

Principio de la página

Registro de IAS en Active Directory

Todos los servidores IAS se deben registrar en Active Directory. Su registro significa la adición de la cuenta de equipo del servidor IAS para el grupo de seguridad Servidores RAS e IAS, lo que garantiza que los servidores IAS tengan permiso para leer las propiedades de acceso remoto de las cuentas de usuario y equipo en Active Directory.

Puede registrar los servidores de las siguientes maneras:

- Al agregar manualmente los servidores al grupo (utilizando **Usuarios y equipos de Active Directory**).
- Al utilizar el elemento **Registrar con Active Directory** del menú **Acción** de la MMC del **Servicio de autenticación de Internet**.
- Al utilizar el comando **Netsh**.

Este último método (con el comando **Netsh**) se muestra en esta guía porque es fácil de ejecutar como secuencia de comandos y permite registrar el servidor en otros dominios.

Para registrar IAS en el dominio predeterminado

1. Inicie sesión en el servidor IAS y abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el comando siguiente:

   netsh ras add registeredserver

Si tiene varios dominios, realice el siguiente procedimiento para cada dominio con usuarios o equipos que vaya a autenticar este servidor IAS. Por ejemplo, si los servidores IAS se instalan en el dominio A y existen usuarios de WLAN en el dominio B, debe registrar los servidores en ambos dominios. Para ello, necesita tener permiso para modificar la pertenencia al grupo Servidores RAS e IAS en el dominio de destino.

Para registrar IAS en un dominio que no es el predeterminado

1. En el símbolo del sistema, ejecute el siguiente comando y sustituya *NombreDominio* por el nombre del

dominio en el que se debe registrar el servidor IAS:

netsh ras add registeredserver domain = *NombreDominio*

Nota: otra opción consiste en agregar el objeto de equipo del servidor IAS directamente al grupo de seguridad Servidores RAS e IAS en el dominio de destino utilizando **Usuarios y equipos de Active Directory**.

Principio de la página

Configuración del servidor IAS principal

En esta sección se proporcionan instrucciones para la configuración del servidor IAS principal. Los servidores IAS posteriores se configurarán mediante la replicación de la configuración de este servidor y utilizando los procedimientos descritos más adelante en este capítulo.

Inscripción automática de un certificado de servidor IAS

En el capítulo 4, "Creación de la entidad emisora de certificados de red", se proporcionaron los pasos que se deben seguir para instalar un objeto de directiva de grupo (GPO) con el fin de permitir a los miembros del grupo Servidores RAS e IAS inscribir automáticamente certificados de equipo. Al registrar el servidor IAS en Active Directory se agrega la cuenta del servidor a este grupo. Sin embargo, será necesario reiniciar el servidor para que el equipo pueda agregar este grupo al token de inicio de sesión y pueda inscribir un certificado correctamente.

Nota: al igual que ocurre con los usuarios, los equipos no reciben la modificación de la pertenencia de grupo en el token de acceso hasta que vuelven a iniciar sesión en el dominio. En los equipos, esto ocurre durante el inicio.

Antes de continuar con el siguiente procedimiento, reinicie el servidor.

Advertencia: antes de reiniciar el servidor, asegúrese de que no se está realizando ninguna tarea en el mismo. Si el servidor es un controlador de dominio, asegúrese de que dispone de otro controlador para los usuarios antes de reiniciar el primero. También debe evitar su reinicio durante la realización de una tarea importante del sistema, como por ejemplo, la copia de seguridad del servidor.

Comprobación de la implementación de certificados de servidores IAS

Después de reiniciar el servidor, asegúrese de que el certificado de servidor IAS se ha inscrito correctamente.

Para comprobar el certificado de autenticación de servidor IAS

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el siguiente comando para abrir la MMC de **Certificados**:

   ComputerCerts.msc

3. En el árbol de la consola, haga doble clic en **Certificados (equipo local)** y en **Personal**. A continuación, haga clic en **Certificados**.
4. Debe aparecer al menos un certificado con el nombre de este servidor en la columna **Emitido para** y el nombre de la entidad emisora de certificados en la columna **Emitido por**. Desplácese por la lista (situada a la derecha) para ver la columna **Plantilla de certificado**. Debe aparecer el valor **Equipo** para este certificado en esta columna.

   Nota: si éste es el servidor IAS principal y se está instalando en el mismo servidor que la entidad emisora, aparecerá también otro certificado con el nombre de la entidad emisora en ambas columnas; éste es el certificado de entidad emisora con firma personal.

5. Si el certificado necesario no aparece en el complemento MMC de **Certificados**, seleccione **Certificados (equipo local)** en el árbol de la consola (en el panel izquierdo), haga clic en **Todas las tareas** en el menú **Acción** y, a continuación, seleccione **Inscribir certificados automáticamente**. A continuación,

actualice la vista de la MMC de **Certificados**.

Configuración del servidor IAS principal

La configuración de todos los servidores IAS será muy parecida en esta solución (aunque el conjunto de puntos de acceso inalámbrico instalado en cada servidor normalmente será distinto para cada uno de ellos). Para mantener la configuración sincronizada entre los servidores y para reducir el esfuerzo que supone administrar varios servidores, realizará la mayoría de las tareas de configuración en el servidor IAS principal instalado y, a continuación, replicará la configuración de este servidor en los demás servidores IAS de la organización.

Durante los procedimientos de esta sección, configurará los siguientes tipos de valor de configuración en el servidor IAS principal:

- Registro de solicitudes
- Directiva de acceso remoto
- Configuración de solicitudes de conexión

Más adelante, se replicará esta configuración en los demás servidores IAS. También debe agregar una entrada de cliente RADIUS a IAS para cada punto de acceso inalámbrico procesado mediante ese servidor IAS (lo que se explica en la sección "Configuración de puntos de acceso inalámbrico", más adelante en este capítulo).

Configuración del registro en el registro de sucesos de Windows

IAS registra los sucesos importantes del sistema, como por ejemplo, el inicio y cierre del servicio, y problemas tales como los errores de configuración y de servicio en el registro del sistema Windows. También puede registrar, opcionalmente, los intentos de autenticación tanto correctos como erróneos.

Para habilitar el registro de las solicitudes de autenticación en IAS

1. Abra la MMC del **Servicio de autenticación de Internet**, haga clic en **Inicio**, elija **Todos los programas**, seleccione **Herramientas administrativas** y haga clic en **Servicio de autenticación de Internet**.
2. Haga clic con el botón secundario en **Servicio de autenticación de Internet (local)** y, a continuación, seleccione **Propiedades**.
3. Asegúrese de que **Solicitudes de autenticación rechazadas** y **Solicitudes de autenticación correctas** están habilitadas.
4. Haga clic en **Aceptar**.

Configuración del registro de solicitudes de autenticación y de cuentas en registros RADIUS

IAS también puede registrar información de autenticación y de cuentas en registros RADIUS. IAS no crea registros RADIUS de forma predeterminada y no se ha habilitado el registro RADIUS en esta solución con el fin de reducir la carga de administración.

Si necesita el registro RADIUS con fines de administración de cuentas o auditorías de seguridad, es posible habilitar uno o ambos tipos de registros de solicitudes. IAS puede escribir estos registros en archivos de texto o en una base de datos SQL. Puede utilizar estos registros como entrada para los sistemas de supervisión de seguridad con el fin de realizar un seguimiento de posibles infracciones de seguridad. Menos frecuente es el uso por parte de las organizaciones de los registros de cuentas para la facturación, aunque esto suele estar confinado a los proveedores comerciales de servicios de Internet y otros de servicios de red. Si desea implementar el registro RADIUS o simplemente obtener más información sobre él, consulte las referencias al final de este capítulo.

Nota: no debe habilitar el registro de solicitudes de autenticación y de cuentas RADIUS a menos que exista un motivo específico para hacerlo. Puede afectar al rendimiento del servidor y además es necesario el mantenimiento regular de los archivos de registro para garantizar que no llenan los discos del servidor.

Creación de una directiva de acceso remoto IAS para WLAN

Realice el siguiente procedimiento para crear una directiva de acceso remoto en el servidor IAS.

Para crear una directiva de acceso remoto en IAS

1. En la MMC del **Servicio de autenticación de Internet**, haga clic en **Inicio**, elija **Todos los programas**, seleccione **Herramientas administrativas** y haga clic en **Servicio de autenticación de Internet**.

2. Haga clic con el botón secundario en la carpeta **Directivas de acceso remoto** y, a continuación, haga clic en **Nueva directiva de acceso remoto**. Haga clic en **Siguiente** para continuar.

3. Seleccione **Directiva típica para un escenario común** como el modo en que desea configurar la directiva y asígnele el nombre **Permitir acceso a LAN inalámbrica**. Haga clic en **Siguiente**.

4. Seleccione **Inalámbrico** como método de acceso.

5. Seleccione la opción **Grupo** para **Conceder acceso basado en** y escriba (o busque) el grupo de seguridad Acceso a LAN inalámbrica. Haga clic en **Siguiente** para continuar.

6. Seleccione **EAP protegido (PEAP)** en la lista de tipos de EAP.

7. Haga clic en el botón **Configurar**. El certificado de servidor IAS emitido anteriormente debe mostrarse en el campo **Certificado emitido** (si no es así, selecciónelo de la lista de certificados disponibles). **Contraseña segura (EAP MSCHAPv2)** debe aparecer en la lista **Tipos de EAP**. Compruebe la casilla de verificación **Habilitar reconexión rápida**.

   Importante: si utiliza clientes inalámbricos con Pocket PC 2003, no debe activar la casilla de verificación **Habilitar reconexión rápida** a menos que tenga una versión de Pocket PC que sea compatible con esta opción (consulte la referencia del artículo de Knowledge Base al final de este capítulo). Si habilita la reconexión rápida, los clientes con Pocket PC no podrán volver a conectarse a la red una vez transcurrido el tiempo de espera de la autenticación inicial.

8. Haga clic en **Aceptar** y, a continuación, en **Siguiente**. Haga clic en **Finalizar** para completar el procedimiento.

   Importante: la nueva directiva **Permitir acceso a LAN inalámbrica** puede coexistir con otras directivas de acceso remoto que haya creado o con las directivas de acceso remoto predeterminadas. Sin embargo, debe asegurarse de que cualquier otra directiva de acceso remoto predeterminada se elimina o se enumera (en una prioridad inferior) después de la directiva **Permitir acceso a LAN inalámbrica** en la carpeta **Directivas de acceso remoto** de IAS.

Modificación de la configuración del perfil de la directiva de acceso a WLAN

El asistente para **Nueva directiva de acceso remoto** (según se ha utilizado en el procedimiento anterior) crea una directiva de acceso remoto válida, pero los dos siguientes valores se deben configurar de forma manual. La primera agrega el atributo de RADIUS **Ignorar propiedades de acceso telefónico del usuario**. De este modo se indica a IAS que ignore el valor de configuración de permiso de acceso remoto que se especifica en la ficha **Acceso telefónico** del objeto de usuario de Active Directory. También se evita que IAS envíe esta información en las respuestas de RADIUS a los puntos de acceso inalámbrico, ya que en algunas ocasiones puede causar problemas de compatibilidad.

La segunda categoría permite que el servidor IAS termine la conexión del cliente una vez transcurrido el tiempo de vigencia especificado y forzar al cliente a reautenticarse. Esta configuración es particularmente importante cuando se utiliza la protección de datos mediante la privacidad equivalente por cable (WEP) dinámica (la opción predeterminada para esta solución). El tiempo de espera de la sesión controla la frecuencia con la que se generan nuevas claves de red de cifrado de datos.

Nota: el acceso protegido Wi-Fi (WPA) tiene su propio mecanismo para generar nuevas claves para cada paquete transmitido. El siguiente tema no se aplica a WLAN con WPA.

El valor de tiempo de espera de sesión es un equilibrio entre seguridad y confiabilidad. Un tiempo de espera de 60 minutos proporciona una seguridad adecuada para la mayoría de las circunstancias y, con seguridad, para

las redes 802.11b de 11 Mbps. Normalmente, los clientes inalámbricos nunca transmitirán datos suficientes en 60 minutos como para permitir que un atacante recupere una clave WEP dinámica. Las WLAN más rápidas que utilizan estándares 802.11a o 802.11g de 54 Mbps permiten la transmisión de una mayor cantidad de datos en un tiempo determinado; debe considerar el uso de un tiempo de espera de 15 minutos para estas redes. Si utiliza un valor inferior, puede reducir la confiabilidad de la WLAN y aumentar la carga en los servidores IAS.

Debe consultar la sección "Opciones de seguridad para la WEP dinámica" del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas" para obtener información más detallada sobre la configuración del tiempo de espera de sesión del cliente.

Debe configurar el tiempo de espera de sesión del cliente y el atributo **Acción-Terminación** de RADIUS en el valor adecuado de manera que el servidor IAS pueda forzar al cliente a reautenticarse en el intervalo necesario. Para obtener más información sobre la configuración de directivas de acceso remoto, consulte la sección "Directivas de RADIUS" del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas".

Para modificar la configuración del perfil de la directiva de acceso inalámbrico

1. En la MMC del **Servicio de autenticación de Internet**, haga clic con el botón secundario en la directiva **Permitir acceso a LAN inalámbrica** y seleccione **Propiedades**. A continuación, haga clic en **Modificar perfil**.

2. Haga clic en la ficha **Restricciones de marcado** y, a continuación, seleccione la opción **Minutos que el cliente puede estar conectado (tiempo de espera de sesión)** y escriba el valor **60** (minutos) si utiliza una WLAN 802.11b (de 11 Mbps) o **15** (minutos) si utiliza una WLAN 802.11a de velocidad superior o una 802.11g (de 54 Mbps).

   Nota: si utiliza una WLAN con protección WPA en lugar de WEP dinámica, establezca este valor en ocho horas. Un valor de ocho horas garantizará que los clientes tengan unas credenciales actualizadas válidas para un período de tiempo razonable. Al mismo tiempo, garantizará que un cliente no pueda permanecer conectado durante períodos de tiempo excesivos una vez desactivada la cuenta. Sin embargo, en entornos de alta seguridad donde es necesario reducir el tiempo de retraso entre desactivar una cuenta y forzar al cliente a desactivarse de la red, este valor se puede disminuir a una hora.

3. Haga clic en la ficha **Avanzadas**, agregue el atributo **Ignorar propiedades de acceso telefónico del usuario** y establézcalo en **True**. A continuación, agregue el atributo **Acción-Terminación** y establézcalo en **RADIUS Request**.

Comprobación de la directiva de solicitud de conexión para WLAN

La directiva de solicitud de conexión IAS predeterminada está configurada para indicar a IAS que autentique los usuarios y los clientes directamente en Active Directory. Lleve a cabo los pasos siguientes para comprobar la configuración de la directiva de solicitud de conexión predeterminada.

Para comprobar la configuración de la directiva de solicitud de conexión predeterminada

1. Abra la MMC del **Servicio de autenticación de Internet**, vaya hasta la carpeta **Procesamiento solicitud de conexión\Directivas de solicitud de conexión** y haga clic con el botón secundario en la directiva de solicitud de conexión **Usar autenticación de Windows para todos los usuarios**. A continuación, seleccione **Propiedades**.

2. Compruebe que las condiciones de la directiva contienen **Coincidencias de restricciones de fecha y hora"Dom 00:00-24:00; Lun 00:00-24:00; Mar 00:00-24:00; Mié 00:00-24:00; Jue 00:00-24:00; Vie 00:00-24:00; Sáb 00:00-24:00"**.

3. Haga clic en el botón **Modificar perfil** y asegúrese de que ha seleccionado **Autenticar solicitudes en este servidor** en la ficha **Autenticación**.

4. Asegúrese de que no hay reglas especificadas en la ficha **Atributo**.

Principio de la página

Implementación de la configuración en varios servidores IAS

Después de configurar el servidor IAS principal, puede replicar esta configuración en los demás servidores IAS.

Repita los procedimientos anteriores de este capítulo para la "Instalación de IAS" y el "Registro de IAS en Active Directory" en cada uno de los servidores adicionales. También debe realizar el procedimiento de "Comprobación de la implementación de certificados de servidores IAS" para garantizar que se ha inscrito un certificado por cada nuevo servidor. Una vez realizados estos procedimientos, estará listo para exportar la configuración de IAS del servidor principal e importarla a los demás servidores, tal y como se describe en los procedimientos de la siguiente sección.

Importante: sólo puede replicar la configuración a otros servidores IAS de Windows Server 2003. Con estos procedimientos, no puede replicar la configuración de IAS desde versiones de Windows Server 2003 a otras de Windows 2000.

Replicación de la configuración desde el servidor IAS principal

Puede utilizar el comando **Netsh** para exportar parte de la configuración de IAS a archivos de texto. Las secuencias de comandos utilizadas en los siguientes procedimientos utilizan Netsh.exe para exportar la configuración de un servidor IAS e importarla a otro.

Las siguientes categorías de configuración de IAS se pueden exportar por separado de un servidor IAS e importar a otro servidor IAS:

- Configuración de servidor
- Configuración de registro
- Directivas de acceso remoto
- Directivas de solicitud de conexión
- Clientes RADIUS
- Configuración completa (incluye todo lo anterior)

La configuración exportada se almacena en archivos de texto, aunque los datos estén codificados. Estos archivos de texto se pueden utilizar para transferir la configuración habitual a varios servidores IAS con el fin de garantizar una configuración coherente y una implementación rápida.

La mayoría de las categorías de configuración serán comunes a los servidores IAS con una función similar (normalmente con la excepción de la categoría de clientes RADIUS). En esta solución, los servidores IAS autenticarán únicamente clientes WLAN. Si tiene previsto utilizar uno o varios servidores IAS de forma diferente (por ejemplo, para autenticar clientes de acceso remoto), tendrá que configurar y replicar la configuración de estos servidores de manera independiente o realizar la configuración manualmente. De lo contrario, correrá el riesgo de sobrescribirla y perder valores de directivas y otros valores de configuración.

La configuración de los siguientes elementos sólo debe realizarse en el servidor IAS principal (tal y como se describe en la sección anterior "Configuración de IAS").

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

Esta configuración se exportará mediante los procedimientos de esta sección y se replicará en los otros servidores IAS.

Sugerencia: para que sea más fácil realizar un seguimiento de los cambios realizados en la configuración de IAS, incluya un número de versión en el nombre de la directiva de acceso remoto. Cada vez que modifique la

configuración de IAS, actualice el nombre de manera que incluya un nuevo número de versión. De este modo será más sencillo realizar un seguimiento de los cambios realizados en los servidores IAS y comprobar si todos están utilizando la misma configuración.

Designe el servidor IAS principal como servidor IAS "maestro". A continuación, utilice los siguientes procedimientos para replicar la configuración de este servidor en otros servidores IAS de la organización. La replicación de la configuración de clientes RADIUS se detalla en la sección "Replicación de la configuración de clientes RADIUS en otros servidores IAS" más adelante en este capítulo.

Nota: la designación de "maestro" no tiene ningún significado especial para IAS. Sólo se utiliza para indicar el servidor que se usará para realizar los cambios de la configuración inicial antes de replicarla en otros servidores IAS.

Exportación de la configuración del servidor IAS maestro

Este procedimiento guarda la configuración actual del servidor IAS en los archivos de disco.

Para exportar la configuración de IAS a archivos de disco

1. Inicie sesión en el servidor IAS principal y abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Si es necesario, identifique una carpeta para almacenar los archivos de salida o inserte un disco formateado vacío en la unidad del servidor.
3. Ejecute el siguiente comando para exportar la configuración de IAS:

   MSSTools ExportIASSettings [**/path:***CarpetaSalida*]

   CarpetaSalida es un parámetro opcional utilizado para especificar la carpeta en la que se escribirán los archivos exportados. La ruta debe estar escrita entre comillas si incluye espacios. Esta carpeta, si se especifica, debe existir o de lo contrario, los archivos se escribirán en el directorio actual.
4. La secuencia de comandos creará los siguientes archivos:
   - IAS_Server_Settings.txt
   - IAS_Logging.txt
   - IAS_Rem_Access_Policies.txt
   - IAS_Con_Request_Policies.txt
5. Almacene los archivos para importarlos a los demás servidores.

Importación de la configuración a otros servidores IAS

Este procedimiento utiliza los archivos de configuración exportados en el procedimiento anterior para configurar otros servidores IAS con la misma configuración. Este procedimiento no importa los clientes RADIUS, lo cual se explica en una sección posterior.

Advertencia: la importación de la configuración de IAS a otro servidor IAS sobrescribirá la configuración de IAS existente en dicho servidor (excepto la información de clientes RADIUS). Si ha creado diferentes configuraciones en un servidor (por ejemplo, diferentes directivas de acceso remoto para admitir clientes de una red privada virtual, VPN), no utilice este procedimiento para importar la configuración de WLAN de IAS a este servidor. En su lugar, establezca la configuración manualmente mediante los procedimientos descritos en la sección "Configuración del servidor IAS principal" anteriormente en este capítulo.

Para importar la configuración IAS desde archivos de disco

1. Inicie sesión en el servidor IAS de destino y abra un shell de comandos mediante el acceso directo **MSS WLAN Tools**.

   Identifique la carpeta que contiene los archivos de configuración exportados previamente desde el

2. servidor IAS maestro.

3. Ejecute el siguiente comando para importar la configuración de IAS:

   MSSTools ImportIASSettings [**/path:***CarpetaEntrada*]

   CarpetaEntrada es un parámetro opcional que se utiliza para especificar la carpeta en la que la secuencia de comandos buscará los archivos de configuración que va a importar. La ruta debe estar escrita entre comillas si incluye espacios. Si no se especifica ninguna carpeta, los archivos deberán encontrarse en el directorio actual.

Debe comprobar que la configuración se ha importado correctamente abriendo la MMC del **Servicio de autenticación de Internet** y comprobando la configuración de las directivas de solicitud de conexión y acceso remoto.

Principio de la página

Configuración de puntos de acceso inalámbrico

En esta sección se describe cómo agregar puntos de acceso inalámbrico como clientes RADIUS a los servidores IAS.

Adición de puntos de acceso como clientes RADIUS a IAS

Debe agregar puntos de acceso inalámbrico como clientes RADIUS a IAS para que se les permita utilizar los servicios de autenticación y cuentas RADIUS. Para obtener más información sobre cómo asignar puntos de acceso inalámbrico a diferentes servidores IAS, consulte los procedimientos del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas".

Los puntos de acceso inalámbrico de una ubicación concreta se configurarán de la forma habitual para que utilicen un servidor IAS de la misma ubicación para el servidor RADIUS principal y otro servidor IAS de la misma u otra ubicación para el servidor RADIUS secundario. Los términos "principal" y "secundario" no hacen referencia a una relación jerárquica ni a una diferencia de configuración entre los propios servidores IAS. Los términos son relevantes sólo para los puntos de acceso inalámbrico, cada uno de los cuales tiene designados un servidor RADIUS principal y secundario (o de copia de seguridad). Antes de configurar los puntos de acceso inalámbrico, debe decidir qué servidor IAS será el servidor RADIUS principal y cuál será el secundario para cada punto de acceso.

En los procedimientos siguientes se describe cómo agregar clientes RADIUS a dos servidores IAS. Durante el primer procedimiento se crea un secreto de RADIUS para el punto de acceso inalámbrico; IAS y el punto de acceso inalámbrico utilizarán este secreto o clave para autenticarse entre sí. Los detalles de este cliente, junto con su secreto, se registran en un archivo. Este archivo se utiliza en el segundo procedimiento para importar el cliente al IAS secundario.

Importante: no use este primer procedimiento para agregar el mismo cliente a dos servidores IAS. Si lo hace, las entradas del cliente de cada servidor tendrán configurados diferentes secretos de RADIUS y el punto de acceso inalámbrico no podrá autenticarse en ambos servidores.

Adición de puntos de acceso al servidor IAS principal

En esta sección se describe cómo agregar puntos de acceso inalámbrico al servidor IAS principal. Se proporciona una secuencia de comandos para automatizar la creación de un secreto (contraseña) seguro y aleatorio de RADIUS, y agregar el cliente a IAS. La secuencia de comandos también crea un archivo (de forma predeterminada es Clients.txt) que registra los detalles de cada punto de acceso inalámbrico agregado. Este archivo registra el nombre, la dirección IP y el secreto de RADIUS creados para cada punto de acceso inalámbrico. Estos datos serán necesarios para configurar el servidor IAS secundario y los puntos de acceso inalámbrico.

Si prefiere agregar los clientes manualmente, siga el procedimiento "Creación de entradas del cliente para puntos de acceso inalámbrico", descrito más adelante en este capítulo, para crear secretos para los puntos de acceso inalámbrico.

Importante: los clientes RADIUS se agregan a IAS como clientes "RADIUS estándar". Aunque resulta adecuado para la mayoría de los puntos de acceso inalámbrico, puede que algunos puntos de acceso requieran la configuración de atributos específicos del proveedor (VSA) en el servidor IAS. Puede configurar VSA seleccionando un dispositivo de proveedor específico en las propiedades de los clientes RADIUS en la MMC del **Servicio de autenticación de Internet** o (si no aparece el dispositivo) especificando los VSA en la directiva de acceso remoto de IAS. Para obtener más información sobre la configuración de VSA en IAS, consulte las referencias al final de este capítulo.

Asimismo, consulte la documentación sobre puntos de acceso inalámbrico para obtener información relacionada con los requisitos de VSA en servidores RADIUS.

Para agregar un cliente RADIUS al servidor IAS principal

1. Inicie sesión en el servidor IAS al que desea agregar el punto de acceso inalámbrico y abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.

2. Si ya hay un archivo de salida de clientes RADIUS en el directorio actual (o si especifica un archivo existente en el parámetro de ruta), la nueva entrada de cliente se agregará a dicho archivo. Si no desea que esto ocurra, elimine el archivo existente o especifique un nombre de archivo alternativo en el comando.

3. Ejecute el siguiente comando para agregar un punto de acceso inalámbrico a IAS:

   MSSTools AddRADIUSClient [**/path:***ArchivoSalida.txt*]

   Nota: el parámetro de ruta *path* es opcional. Puede especificar el nombre del archivo (más una ruta de carpeta opcional) donde se almacenará el resultado del comando. La ruta debe estar escrita entre comillas si incluye espacios. Si no se especifica ningún parámetro de ruta, el comando guardará el resultado en el archivo Clients.txt en el directorio actual.

4. Cuando se le indique, escriba un nombre para el punto de acceso inalámbrico. Éste debe ser una referencia descriptiva para la MMC del **Servicio de autenticación de Internet** y no tiene por qué ser necesariamente el nombre que se le ha asignado en la configuración del punto de acceso inalámbrico. Utilice el nombre de un sistema de nombre de dominio (DNS) o cualquier otra cadena.

5. Escriba la dirección IP del punto de acceso inalámbrico (en notación decimal con punto; por ejemplo, 10.20.1.153).

6. Se creará una contraseña automáticamente para el cliente (esta contraseña es una cadena cifrada de 23 caracteres imprimibles creada de forma aleatoria, que utilizan IAS y el punto de acceso inalámbrico para autenticarse entre sí). Esta configuración se utiliza para agregar el cliente RADIUS a IAS. El nombre, la dirección IP y el secreto también se agregan al archivo de salida (el predeterminado es Clients.txt) en el directorio actual. El archivo de salida es un archivo de texto delimitado por comas con un cliente RADIUS en cada línea, por lo que se puede utilizar fácilmente en secuencias de comandos o importar y manipular empleando una herramienta como Microsoft Excel.

7. Repita los pasos 3 a 6 para todos los puntos de acceso inalámbrico que desee agregar a este servidor IAS.

Más adelante, utilizará el archivo de salida como referencia al establecer los secretos de RADIUS en los puntos de acceso inalámbrico. Para obtener más información, consulte la sección "Configuración de puntos de acceso inalámbrico" más adelante en este capítulo.

Importante: no deje el archivo de salida de clientes RADIUS en el servidor. Contiene los secretos de los clientes RADIUS sin cifrar. Después de agregar los puntos de acceso inalámbrico, debe mover el archivo a un disco u otro medio extraíble con permiso de escritura y almacenarlo en un lugar seguro.

El procedimiento de "Adición de clientes RADIUS al servidor IAS principal" descrito anteriormente utiliza una herramienta de ejemplo que se incluye en esta solución (AddRADIUSClient.exe*)*. Esta herramienta es una aplicación de Visual Basic.NET sencilla que utiliza la interfaz Objetos de datos de servidor para configurar un

servidor IAS. Puede utilizarla para escribir su propia secuencia de comandos con el fin de agregar clientes al servidor IAS.

Esta herramienta no es compatible con Microsoft y no se ha probado minuciosamente. Sin embargo, el código fuente de esta aplicación se ha incluido en caso de que necesite examinarlo o modificarlo antes de su uso.

Nota: a diferencia de la mayoría de las secuencias de comandos utilizadas en los procedimientos de configuración, esta secuencia no escribe los detalles del progreso en el archivo de registro MSSWLAN-setup.log. El motivo es evitar que se almacenen allí los secretos de los clientes RADIUS, lo que conllevaría un riesgo de seguridad. Sin embargo, los detalles del progreso se registran en la pantalla.

Secuencias de comandos de la adición de puntos de acceso a un servidor IAS (procedimiento alternativo)

Si no desea agregar puntos de acceso inalámbrico al servidor IAS de forma interactiva utilizando el procedimiento anterior, puede simplemente crear los archivos de salida de las entradas de clientes RADIUS para cada punto de acceso inalámbrico sin agregarlos a IAS. Entonces podrá utilizar el procedimiento de "Importación de clientes RADIUS al servidor IAS secundario" descrito más adelante en esta sección para importar las entradas de clientes RADIUS tanto al servidor IAS principal como al secundario. Como esta operación entera se puede convertir en secuencias de comandos, quizás prefiera agregar los clientes RADIUS de este modo, si tiene que agregar un elevado número de puntos de acceso inalámbrico.

Importante: este procedimiento es un método alternativo para agregar clientes RADIUS por secuencias de comandos, en lugar de hacerlo de un modo interactivo. Si ha seguido el procedimiento anterior de "Adición de clientes RADIUS al servidor IAS principal", no tendrá que seguir este otro.

Utilice el siguiente procedimiento para crear secretos de RADIUS seguros. La secuencia de comandos, al igual que el procedimiento anterior, utiliza una función CryptoAPI para crear un valor totalmente aleatorio para cada secreto de RADIUS. De este modo se garantiza que los valores serán lo suficientemente seguros como para evitar ataques de averiguación de la contraseña o de diccionario.

Para crear el archivo de entrada de clientes para puntos de acceso inalámbrico

1. Abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Ejecute el comando siguiente. Sustituya un nombre descriptivo del punto de acceso inalámbrico por el parámetro *NombreCliente* y la dirección IP del mismo por *DirecciónIP*. También puede proporcionar un nombre y una ruta de archivo alternativos para especificar dónde se van a guardar los datos de salida. Si no se especifica ningún parámetro de ruta, los datos de salida se guardarán en el archivo Clients.txt en la carpeta de trabajo actual. Si el archivo de salida ya existe, el nuevo valor se agregará al mismo. Si no existe, se creará.

   MSSTools GenRADIUSPwd /client:*NombreCliente* **/IP:***DirecciónIP* [**/path:***ruta**nombrearchivo*]

   Los parámetros "client" y "path" pueden incluir espacios; si alguno de ellos los tiene, debe ponerlo entre comillas. El comando puede aparecer dividido en varias líneas, pero deberá escribirlo en una sola línea.
3. Repita el paso 2 para todos los puntos de acceso inalámbrico para los que necesita crear secretos de RADIUS. Cada entrada de cliente se agregará al archivo de salida (el predeterminado es Clients.txt). El archivo es un archivo de texto delimitado por comas con un cliente RADIUS en cada línea, por lo que se puede utilizar fácilmente en secuencias de comandos o importar y manipular empleando una herramienta como puede ser Microsoft Excel.

   Precaución: no deje el archivo de salida en el servidor. Contiene los secretos de los clientes RADIUS sin formato. Después de agregar los puntos de acceso inalámbrico, debe mover el archivo a un disco u otro medio extraíble con permiso de escritura y almacenarlo en un lugar seguro.

   Nota: a diferencia de la mayoría de las secuencias de comandos utilizadas en los procedimientos de configuración, esta secuencia no escribe los detalles del progreso en el archivo de registro MSSWLAN-setup.log. El motivo es evitar que se almacenen allí los secretos de los clientes RADIUS, lo que conllevaría un riesgo de seguridad. Sin embargo, los detalles del progreso se registran en la pantalla.

Importación de puntos de acceso en el servidor IAS secundario

Después de agregar los puntos de acceso inalámbrico al servidor IAS principal, tiene que agregarlos a un servidor secundario antes de configurarlos para utilizar RADIUS.

Para importar un cliente RADIUS al servidor IAS secundario

1. Copie el archivo de salida de clientes creado en los procedimientos anteriores (por motivos de seguridad, elimine por completo este archivo del servidor IAS principal; allí ya no es necesario).

2. Compruebe que el archivo contiene las entradas correctas abriéndolo y viéndolo en Bloc de notas o Microsoft Excel. Esta acción es importante, ya que el archivo podría contener entradas antiguas que hayan quedado de una ejecución anterior del procedimiento. Elimine cualquier entrada de cliente que no sea necesaria.

3. Ejecute el siguiente comando para importar estos clientes al servidor IAS secundario:

   MSSTools AddSecRADIUSClients [**/path:***ArchivoEntrada.txt*]

   Nota: el parámetro de ruta *path* es opcional. Puede utilizar otro parámetro de ruta para leer la entrada desde un archivo o una carpeta diferente. La ruta debe estar escrita entre comillas si incluye espacios. Si no se especifica ningún parámetro, el comando buscará y leerá la entrada del archivo Clients.txt en el directorio actual.

4. La secuencia de comandos rechazará cualquier entrada de cliente mal formada y mostrará el número de entradas correctas e incorrectas al final.

5. Compruebe que los clientes se han agregado correctamente. Para ello, abra la MMC del **Servicio de autenticación de Internet** y consulte la carpeta **Clientes RADIUS**.

   Nota: a diferencia de la mayoría de las secuencias de comandos utilizadas en la instalación y configuración de la solución, esta secuencia no escribe los detalles del progreso en el archivo MSSWLAN-setup.log. El motivo es evitar que se almacenen allí los secretos de los clientes RADIUS, lo que conllevaría un riesgo de seguridad. Sin embargo, los detalles del progreso se registran en la pantalla.

Configuración de puntos de acceso inalámbrico

Una vez agregadas las entradas de clientes RADIUS para los puntos de acceso inalámbrico a IAS, es necesario que configure dichos puntos de acceso. Asimismo, debe agregar las direcciones IP de los servidores IAS y los secretos de clientes RADIUS que utilizará cada punto de acceso para comunicarse con estos servidores de forma segura. Cada punto de acceso inalámbrico se configurará con un servidor IAS principal y uno secundario (o de copia de seguridad). Debe realizar los procedimientos de esta sección para los puntos de acceso inalámbrico en cada sitio de la organización. Para obtener más información sobre cómo asignar puntos de acceso inalámbrico a los servidores IAS, consulte el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas".

El procedimiento para configurar puntos de acceso inalámbrico varía según la marca y el modelo del dispositivo. Sin embargo, los proveedores de puntos de acceso inalámbrico ofrecen por lo general instrucciones detalladas para configurar sus dispositivos. Dependiendo del proveedor, estas instrucciones también pueden estar disponibles en línea.

Antes de establecer la configuración de seguridad para los puntos de acceso inalámbrico, debe establecer la configuración de red básica. Entre ellas se incluyen las siguientes:

- Dirección IP y máscara de subred del punto de acceso inalámbrico
- Puerta de enlace predeterminada
- Nombre descriptivo del punto de acceso inalámbrico
- Nombre de red inalámbrica (SSID)

Esta lista incluirá otros parámetros que afectan a la implementación de varios puntos de acceso inalámbrico:

valores de configuración que controlan el alcance de radio correcto en todo el sitio; por ejemplo, canal de radio 802.11, velocidad y potencia de transmisión, etc. La explicación de estos parámetros no entra en el ámbito de esta guía. Utilice la documentación del proveedor como referencia cuando establezca esta configuración o consulte a un proveedor de servicios de red. Para obtener más información sobre la implementación de puntos de acceso inalámbrico, consulte las referencias al final de este capítulo.

Las instrucciones de este capítulo consideran que ha establecido estos elementos correctamente y que puede conectarse al punto de acceso inalámbrico desde un cliente WLAN utilizando una conexión no autenticada. Debe probar estas condiciones antes de configurar los parámetros de autenticación y seguridad que se enumeran en las siguientes secciones.

Habilitación de autenticación de seguridad de WLAN en puntos de acceso

Debe configurar cada punto de acceso inalámbrico con un servidor RADIUS principal y secundario. El punto de acceso utilizará por lo general el servidor principal para todas las solicitudes de autenticación y pasará al secundario si el principal no está disponible. Como se ha explicado en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas", es importante que planee la asignación de los puntos de acceso inalámbrico y que decida con precaución qué servidor debe ser el principal y cuál el secundario. En resumen:

- En un sitio con dos (o más) servidores IAS, equilibre los puntos de acceso inalámbrico en los servidores disponibles de manera que aproximadamente la mitad utilice el servidor 1 como principal y el 2 como secundario, y el resto utilice el servidor 2 como principal y el 1 como secundario.
- En los sitios donde tenga únicamente un servidor IAS, éste debe ser siempre el servidor principal. Debe configurar un servidor remoto (en el sitio con conectividad más confiable a este sitio) como servidor secundario.
- En los sitios donde no haya ningún servidor IAS, equilibre los puntos de acceso inalámbrico entre los servidores remotos utilizando el servidor con la conectividad de mayor rendimiento y menor latencia. Lo ideal es que estos servidores estén en diferentes sitios, a menos que tenga una conectividad de red de área extensa (WAN) de alto rendimiento.

La siguiente tabla muestra la configuración que debe establecer en los puntos de acceso inalámbrico. Aunque el nombre y la descripción de la configuración puede variar de un proveedor a otro, la documentación de estos puntos de acceso le ayudará a determinar los que corresponden a los elementos de la tabla.

Tabla 5.3. Configuración de puntos de acceso inalámbrico

Elemento	Configuración
Parámetros de autenticación	
Modo de autenticación	Autenticación 802.1X
Reautenticación	Habilitar
Volver a crear claves de forma rápida/dinámica	Habilitar
Tiempo de espera de actualización de claves	60 minutos
Parámetros de cifrado (esta configuración suele hacer referencia al cifrado de WEP estática)	(Los parámetros de cifrado se pueden deshabilitar o sobrescribir al habilitar la opción para volver a crear claves.)
Habilitar cifrado	Habilitar
Denegar sin cifrado	Habilitar
Autenticación RADIUS	
Habilitar autenticación RADIUS	Habilitar

Servidor de autenticación RADIUS principal	Dirección IP de IAS principal
Puerto de servidor RADIUS principal	1812 (predeterminado)
Servidor de autenticación RADIUS secundario	Dirección IP de IAS secundario
Puerto de servidor RADIUS secundario	1812 (predeterminado)
Secreto compartido de autenticación RADIUS	**XXXXXX** (sustituir por el secreto creado)
Límite de reintentos	5
Tiempo de espera de reintentos	5 segundos
Administración de cuentas RADIUS	
Habilitar administración de cuentas RADIUS	Habilitar
Servidor de cuentas RADIUS principal	Dirección IP de IAS principal
Puerto de servidor RADIUS principal	1813 (predeterminado)
Servidor de cuentas RADIUS secundario	Dirección IP de IAS secundario
Puerto de servidor RADIUS secundario	1813 (predeterminado)
Secreto compartido de cuentas RADIUS	**XXXXXX** (sustituir por el secreto creado)
Límite de reintentos	5
Tiempo de espera de reintentos	5 segundos

Importante: el valor **Tiempo de espera de actualización de claves** está establecido en 60 minutos para su uso con WEP dinámica. El valor **Tiempo de espera de sesión** establecido en la directiva de acceso remoto es igual o inferior a éste. Para obtener más información, consulte la sección anterior "Modificación de la configuración del perfil de la directiva de acceso a WLAN". El valor que sea inferior tendrá preferencia, por lo que sólo deberá modificarlo en IAS. Si está utilizando WPA, debe aumentar este valor a ocho horas en el punto de acceso. Consulte la documentación del proveedor para obtener más información.

Utilice los mismos secretos de RADIUS creados en el procedimiento de "Adición de un cliente RADIUS al servidor IAS principal" para agregar puntos de acceso inalámbrico a IAS. Aunque puede que aún no haya configurado un servidor IAS secundario como copia de seguridad del principal, todavía podrá agregar la dirección IP del servidor al punto de acceso inalámbrico (para no tener que volver a configurarlo más adelante). La configuración de servidores IAS adicionales se explica en una sección posterior de este capítulo.

Según el modelo de hardware del punto de acceso inalámbrico, quizás no tenga entradas configurables independientes para los servidores de autenticación y cuentas RADIUS. Si, por el contrario, las tiene, establézcalas en el mismo servidor a menos que tenga un motivo para no hacerlo.

Los valores de límite y tiempo de espera de reintentos de RADIUS proporcionados en la tabla son unos valores predeterminados comunes, pero no son obligatorios.

Nota: si actualmente está utilizando puntos de acceso inalámbrico sin ninguna seguridad habilitada o sólo con WEP dinámica, deberá planear la migración a una WLAN basada en 802.1X. Para obtener más información sobre la migración desde una red inalámbrica existente, consulte la sección "Migración desde una WLAN existente" del capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas".

Configuración adicional para proteger los puntos de acceso inalámbrico

Además de habilitar los parámetros 802.1X, debe configurar también los puntos de acceso inalámbrico con el nivel de seguridad más alto. La mayoría del hardware de red se proporciona con unos protocolos de administración habilitados que no son seguros y con unas contraseñas de administrador establecidas en unos

valores predeterminados conocidos, lo que conlleva un riesgo de seguridad. Debe establecer la configuración según la siguiente tabla; sin embargo, esta lista no es exhaustiva. Debe consultar la documentación del proveedor para obtener una información autoritativa sobre este tema. Cuando elija las contraseñas y los nombres de comunidad para el protocolo simple de administración de redes (SNMP), utilice valores complejos que incluyan letras en mayúsculas y minúsculas, números y signos de puntuación. Evite elegir caracteres que se puedan averiguar con facilidad a partir de información como el nombre de dominio, el nombre de la empresa y la dirección del sitio.

Tabla 5.4. Configuración de seguridad de puntos de acceso inalámbrico

Elemento	Valor de configuración recomendado	Notas
General		
Contraseña de administrador	XXXXXX	Establecer una contraseña compleja.
Otras contraseñas de administración	XXXXXX	Algunos dispositivos utilizan varias contraseñas de administración para mejorar la protección del acceso mediante diversos protocolos de administración. Asegúrese de que se modifican todos los valores predeterminados para que sean más seguros.
Protocolos de administración		
Serial Console	Habilitar	Si no hay ningún protocolo cifrado disponible, este método es el más seguro para configurar puntos de acceso inalámbrico, aunque requiere conexiones físicas por cable serie entre los puntos de acceso y el terminal, por lo que no se pueden utilizar de forma remota.
Telnet	Deshabilitar	Todas las transmisiones de Telnet se realizan en texto sin formato, por lo que las contraseñas y los secretos de clientes RADIUS estarán visibles en la red. Si el tráfico de Telnet se puede asegurar mediante la seguridad de protocolos de Internet (IPSec) o SSH, podrá habilitar este servicio y usarlo de forma segura.
HTTP	Deshabilitar	La administración HTTP suele estar en texto sin formato y padece de las mismas debilidades que Telnet sin cifrar. Se recomienda HTTPS, si está disponible.
HTTPS (SSL o TLS)	Habilitar	Siga las instrucciones del proveedor para configurar las claves y los certificados que se necesitan.
Comunidades SNMP		SNMP es el protocolo predeterminado para la administración de redes. Utilice SNMP v3 con protección por contraseña para obtener el nivel más alto de seguridad. Éste suele ser el protocolo utilizado por las herramientas de configuración de GUI y los sistemas de administración de redes. Sin embargo, puede deshabilitarlo si no lo utiliza.
Nombre de comunidad 1	XXXXXX	El valor predeterminado suele ser "pública". Cámbielo a un valor complejo.

Nombre de comunidad 2	Deshabilitado	Todos los nombres de comunidad que no sean necesarios deben estar deshabilitados o establecidos en valores complejos.

No debe deshabilitar la difusión de SSID (nombre de red WLAN), ya que podría interferir en la capacidad de Windows XP para conectar con la red adecuada. Aunque se suele recomendar deshabilitar la difusión de SSID como medida de seguridad, el nivel de seguridad que proporciona no es muy alto si se utiliza un método de autenticación segura 802.1X. Incluso si la difusión de SSID desde el punto de acceso está deshabilitada, es relativamente fácil para un atacante determinar el SSID capturando paquetes de conexiones del cliente. Si le preocupa que se difunda la existencia de la WLAN, puede utilizar un nombre genérico para el SSID, el cual no será atribuible a la organización.

Replicación de la configuración de clientes RADIUS en otros servidores IAS

Por lo general, los puntos de acceso inalámbrico de un determinado sitio son atendidos por un servidor IAS de ese sitio. Por ejemplo, el servidor IAS del sitio A atiende a los puntos de acceso inalámbrico del sitio A, mientras que el servidor del sitio B atiende a los puntos de acceso inalámbrico del sito B, y así sucesivamente. Sin embargo, otra configuración del servidor, como las directivas de acceso remoto, será común a muchos servidores IAS. Por este motivo, la exportación e importación de información de clientes RADIUS se gestiona por separado en los procedimientos descritos en esta sección.

Aunque encontrará relativamente pocos casos donde la replicación de información de clientes RADIUS sea relevante, este proceso resulta útil en determinadas circunstancias (por ejemplo, cuando se tienen dos servidores IAS en el mismo sitio, funcionando como servidores RADIUS principal y secundario para todos los puntos de acceso inalámbrico de dicho sitio).

Para exportar la configuración de clientes RADIUS a un archivo

1. Inicie sesión en el servidor IAS de origen y abra un shell de comandos utilizando el acceso directo **MSS WLAN Tools**.
2. Si es necesario, identifique una carpeta para almacenar el archivo de salida o inserte un disco formateado vacío en la unidad del servidor.
3. Ejecute el siguiente comando para exportar la configuración de clientes RADIUS:

   MSSTools ExportIASClients [**/path:***CarpetaSalida*]

   CarpetaSalida es un parámetro opcional utilizado para especificar la carpeta en la que se escribirá el archivo de salida. Si no se proporciona este parámetro, el archivo de salida se escribirá en el directorio actual. Si, por el contrario, sí se proporciona, la carpeta indicada debe existir.
4. La secuencia de comandos crea el archivo IAS_Clients.txt.

   Precaución: debe eliminar este archivo del servidor y almacenarlo en un lugar seguro, ya que contiene los secretos de RADIUS para todos los puntos de acceso inalámbrico configurados en el servidor. Después de exportar la configuración de clientes RADIUS, puede importarlas en los demás servidores. Lo hará normalmente para crear un servidor secundario para un determinado conjunto de puntos de acceso inalámbrico.

Para importar la configuración de clientes RADIUS desde un archivo:

1. Inicie sesión en el servidor IAS de destino y abra un shell de comandos mediante el acceso directo **MSS WLAN Tools**.
2. Identifique la carpeta (o el disco) donde se ha almacenado el archivo IAS_Clients.txt con los secretos de RADIUS exportados.

3. Ejecute el siguiente comando para importar la configuración de clientes RADIUS:

   MSSTools ImportIASClients [**/path:***CarpetaEntrada*]

   CarpetaEntrada es un parámetro opcional utilizado para especificar la carpeta desde la que se leerá el archivo. Si se especifica, esta carpeta debe existir. Si no se especifica ninguna carpeta, los archivos deberán encontrarse en el directorio actual.

   Advertencia: si ha copiado el archivo IAS_Clients.txt en el servidor de destino, debe eliminarlo del mismo y almacenarlo en un lugar seguro, ya que contiene los secretos de RADIUS para todos los puntos de acceso inalámbrico configurados en este servidor.

   La importación de información de clientes RADIUS no es un proceso adicional. La configuración del cliente RADIUS importada sobrescribirá cualquier entrada de cliente existente que tenga en el servidor.

Puede crear un método más flexible para importar clientes RADIUS utilizando la herramienta AddRADIUSClient.exe que se proporciona con esta solución. De este modo, podrá convertir en secuencias de comandos la adición selectiva de clientes RADIUS a distintos servidores.

Principio de la página

Resumen

En este capítulo se han proporcionado instrucciones sobre los siguientes temas:

- Instalación y configuración del servidor IAS principal.
- Instalación de servidores IAS adicionales y replicación en ellos de la configuración del servidor principal.
- Adición de puntos de acceso inalámbrico a IAS como clientes RADIUS.
- Configuración de puntos de acceso inalámbrico para que utilicen servidores IAS y modificación de la configuración predeterminada para mejorar la seguridad.

Ahora ya está preparado para configurar sus propios clientes WLAN. Puede encontrar la información necesaria para ello en el capítulo 6, "Configuración de clientes de LAN inalámbricas".

Debe leer el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas". Este capítulo contiene información fundamental para mantener el funcionamiento seguro y confiable de la infraestructura de RADIUS.

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.

- La sección sobre el "Servicio de autenticación de Internet" de la documentación del producto Windows Server 2003 se encuentra en la siguiente dirección URL:

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

- Para obtener más información sobre la implementación de IAS, consulte el capítulo sobre implementación de IAS del *Kit de distribución de Microsoft Windows Server 2003* en la siguiente dirección URL:

  http://go.microsoft.com/fwlink/?LinkId=4716

- Para obtener más información sobre la programación de IAS utilizando la interfaz Objetos de datos de servidor, consulte la página sobre Objetos de datos de servidor en MSDN en la siguiente dirección URL:

  http://msdn.microsoft.com/library/en-us/sdo/sdo/server_data_objects_.asp

- Para obtener más información sobre el registro IAS y RADIUS, consulte la sección sobre el registro de acceso remoto de la documentación del producto IAS en la siguiente dirección URL:

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

- Para obtener más información sobre la compatibilidad de Pocket PC para la reconexión rápida de PEAP, consulte el artículo 827824, "FIX: Wireless Clients Cannot Connect When the PEAP Fast Reconnect Authentication Option is Turned On" de Microsoft Knowledge Base en la siguiente dirección URL:

  http://support.microsoft.com/default.aspx?scid=kb;en-us;827824

- Para obtener más información sobre la configuración de la compatibilidad de RADIUS específica para los puntos de acceso, consulte la página sobre los atributos específicos del proveedor de la documentación del producto IAS en la siguiente dirección URL:

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

- Para obtener más información sobre la implementación de una WLAN, consulte el capítulo sobre la implementación de una LAN inalámbrica del *Kit de distribución de Microsoft Windows Server 2003* en la siguiente dirección URL:

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

- Para obtener más información sobre la tecnología inalámbrica de Windows XP, consulte las notas del producto *Windows XP Wireless Deployment Technology and Component Overview* en la siguiente dirección URL:

  http://www.microsoft.com/windowsxp/pro/techinfo/administration/networking/default.asp

(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