Latinoamérica

Microsoft TechNet

Seguridad en LAN inalámbricas con PEAP y contraseñas

Capítulo 7: Prueba de soluciones de seguridad en LAN inalámbricas

Actualizado: abril 2, aaaa

Ver todos los temas de guía de seguridad

En esta página

Introducción

El principal objetivo de este capítulo es proporcionar al lector una guía sobre cómo probar su propia implementación de la solución *Seguridad en LAN inalámbricas con PEAP y contraseñas*. Las recomendaciones que se ofrecen en este capítulo se basan en la experiencia obtenida por Microsoft® durante la prueba de esta solución.

En la primera parte del capítulo se describe el proceso de prueba que ha utilizado Microsoft. En la segunda parte se describen los escenarios de prueba que puede utilizar para comprobar una solución antes de implementarla en el entorno de producción. Los escenarios de prueba incluidos en este capítulo complementan los procedimientos de prueba de comprobación que se incluyen en los capítulos del 3 al 6.

Conocimientos previos necesarios

Para probar esta solución se recomienda tener conocimientos operativos en los siguientes campos:

- Conceptos de la infraestructura de claves públicas y los Servicios de Certificate Server de Microsoft.
- Servidores IAS (Servicio de autenticación de Internet) (servidor RADIUS).
- Instalación de controladores de adaptadores de red inalámbrica y configuración de red inalámbrica en Microsoft Windows® XP.
- Uso y configuración de Pocket PC 2003.
- Servicio de directorio Microsoft Active Directory® (incluidas las herramientas de administración y estructura de Active Directory; el trabajo con usuarios, grupos y otros objetos de Active Directory, y las directivas de grupo).
- Lenguaje Microsoft Windows® Scripting Host y Microsoft Visual Basic® Scripting Edition (VBScript) (serán muy útiles para personalizar o utilizar las secuencias de comandos y las herramientas que se incluyen con esta guía).

Principio de la 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

Cómo se ha probado la solución en Microsoft

El equipo de prueba de Microsoft se ha centrado en comprobar el perfil de la solución descrito en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". A continuación se describen las principales características del perfil:

- Un bosque de Active Directory de un solo dominio que contenía dos controladores de dominio con el nivel funcional de dominio del modo nativo de Windows 2000.
- Se instalaron servidores del controlador de dominio en Windows Server™ 2003, Standard Edition.
- Se utilizaron Windows XP Service Pack 1 (Professional Edition y Tablet Edition) y Pocket PC 2003 (Hewlett Packard IPAQ 5550) como clientes inalámbricos.
- Se instaló IAS en los controladores de dominio.
- Se instaló el servidor de la entidad emisora de certificados en uno de los controladores de dominio.
- La red del sitio de la oficina central se encontraba en una red de área local (LAN); el sitio de la sucursal se encontraba en otra LAN independiente.
- Se utilizó la privacidad equivalente por cable (WEP) dinámica para la protección de datos de WLAN, en lugar de WPA.
- La sucursal remota tenía una infraestructura formada sólo por puntos de acceso inalámbrico y se agregó latencia en la conexión con la oficina central para simular un tipo de conexión de módem por cable o DSL.

Este perfil no cubre todas las configuraciones posibles de la solución (por ejemplo, el escalado a un tamaño de organización mayor), pero se garantiza la prueba de todos los componentes de las configuraciones. Los cambios de arquitectura necesarios para escalar este perfil a una organización con 5000 usuarios son relativamente pequeños.

Nota: las pruebas que aquí se describen sólo incluyen la comprobación de la solución realizada por Microsoft. No se incluyen las pruebas ampliadas del producto realizadas por los grupos de productos de Microsoft; la prueba de la solución es una prueba adicional.

Prueba del diseño de red

El entorno del laboratorio de prueba se basó en el diseño de red descrito en el capítulo 2, "Planeamiento de la implementación de seguridad en LAN inalámbricas". En la siguiente figura se muestra el diseño físico del caso de prueba, que posee la configuración de red más sencilla descrita en el capítulo 2.

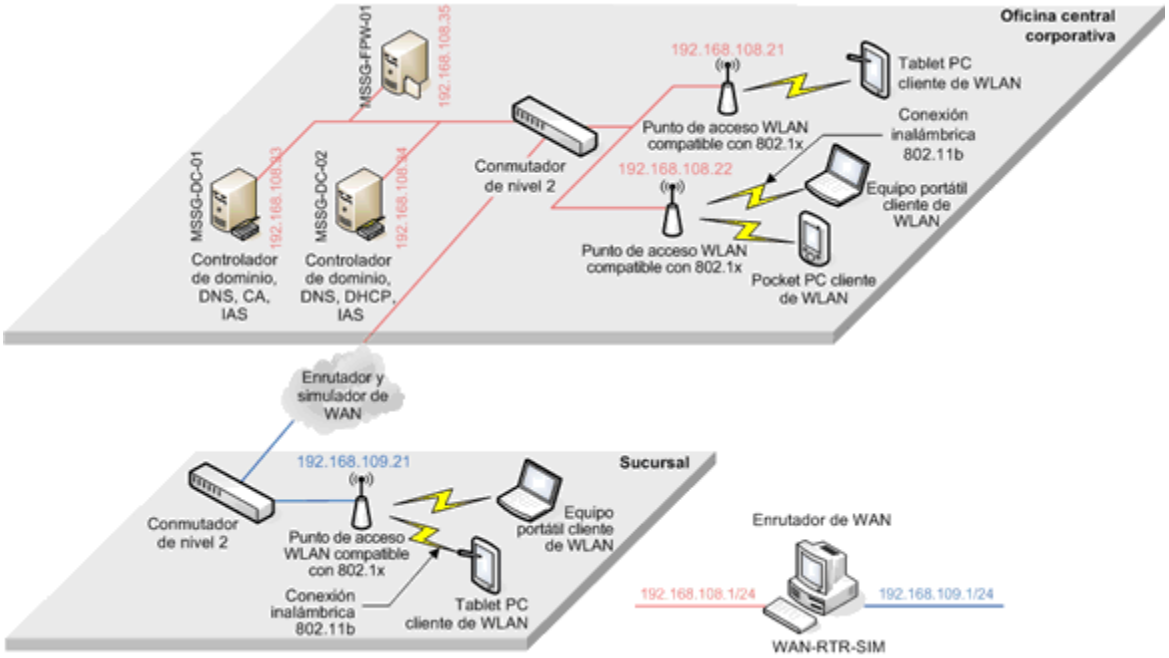

Figura 7.1. Arquitectura de red del laboratorio de pruebas
Vista de imagen a pantalla completa

La red de la oficina central era una única red con los clientes inalámbricos y los servidores de dominio en una subred. El sitio de la sucursal tenía una red independiente y estaba en otra subred. El enrutador que vinculaba la oficina central y la sucursal incluía latencia de WAN simulada y limitaciones de ancho de banda. Los puntos de acceso inalámbrico estaban suficientemente separados para que los usuarios pudieran desplazarse entre ellos.

Aunque se utilizó una única LAN sin segmentar para la prueba, se puede segregar la red interna utilizando distintas subredes, LAN virtuales (VLAN) y conmutadores para administrar mejor el rendimiento y la seguridad de la red.

Una vez desarrollada la red básica formada por controladores de dominio, el Sistema de nombres de dominio (DNS), el Protocolo de configuración dinámica de host (DHCP), los archivos, la impresión y los servicios Web con WEP inalámbrica estática, se utilizó la guía de implementación que se proporciona en los capítulos del 3 al 6 para instalar y configurar cada uno de los componentes. En estos capítulos se incluyen procedimientos de comprobación, que se ejecutan tal y como se describe. Se realizó un conjunto mayor de pruebas antes, durante y después de la creación. Los escenarios de prueba más importantes que se han utilizado se incluyen en la siguiente sección; puede utilizarlos para probar su implementación de la solución.

La solución creada, las secuencias de comandos de creación y de funcionamiento, y la documentación se sometieron a tres rondas de prueba y los problemas se trataron como errores. La prueba se consideró finalizada y satisfactoria cuando se resolvieron todos los errores.

Principio de la página

Comprobación de la implementación

En esta sección se describen los principales escenarios de prueba utilizados por Microsoft para probar la solución.

Estos escenarios de prueba no son exhaustivos; puede desarrollar sus propios ejemplos adaptados a los requisitos de la organización. En este capítulo se han repetido algunos escenarios de comprobación descritos en capítulos anteriores para que la comprobación sea completa. Debe leer los capítulos anteriores antes de utilizar estos escenarios de prueba. Si la prueba falla en alguno de estos escenarios, consulte la sección "Solución de problemas" en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas" para diagnosticar

y resolver los errores de la prueba.

Escenario 1: comprobación de la implementación de certificados de servidor IAS

En este escenario se comprueba que una vez creados y configurados los servidores IAS, éstos reciben el certificado de autenticación de servidor con inscripción automática de la entidad emisora de red.

Detalles de ejecución

1. Abra un shell de comandos con 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, a continuación, haga doble clic en **Personal**. A continuación, haga clic en **Certificados**.
4. Debe aparecer al menos un certificado con el nombre del servidor IAS en la columna **Emitido para** y el nombre de la entidad emisora en la columna **Emitido por**. Desplácese por la lista (a la derecha) y compruebe que el valor de la **Plantilla de certificado** sea **Equipo** para este certificado.
5. Si el certificado necesario no aparece en la MMC de **Certificados**, seleccione **Certificados (equipo local)** en el árbol de la consola del panel de la izquierda, haga clic en **Todas las tareas** en el menú **Acción** y, a continuación, haga clic en **Inscribir certificados automáticamente**. A continuación, actualice la vista de la MMC de **Certificados**.

Escenario 2: comprobación del certificado de entidad emisora raíz en el cliente inalámbrico Windows XP

En este escenario se comprueba que un cliente inalámbrico Windows XP válido recibe el certificado raíz de la entidad emisora de red en el almacén de entidades emisoras raíz de confianza. Este certificado se descarga y se agrega al almacén cuando se actualiza la directiva de grupo.

Detalles de ejecución

1. Inicie la sesión en el equipo cliente como Administrador.
2. Seleccione **Inicio, Ejecutar**, escriba **MMC.exe** y presione **Intro**.
3. Desde el menú **Archivo** de MMC, seleccione **Agregar o quitar complemento**.
4. En la ventana **Agregar o quitar complemento**, haga clic en el botón **Agregar**. Seleccione el elemento **Certificados** en la lista de complementos disponibles.
5. Seleccione **Cuenta de equipo** y, a continuación, haga clic en **Siguiente**.
6. Haga clic en **Finalizar**.
7. Cierre las ventanas **Agregar un complemento independiente** y **Agregar o quitar complemento**.
8. En el panel izquierdo, desplácese hasta Certificados (equipo local)\Entidades emisoras raíz confiables\Certificados.
9. Busque el certificado de la entidad emisora, que aparecerá con el nombre que se le proporcionó durante la instalación de la entidad emisora.
10. Si el certificado no aparece en la lista, ejecute el siguiente comando en un símbolo del sistema:

    Gpupdate /force

11. Vuelva a la MMC de **Certificados**. Haga clic con el botón secundario en el nodo **Certificados (equipo**

local), seleccione **Actualizar** y vuelva a comprobar si aparece el certificado de la entidad emisora.

Escenario 3: comprobación de la autenticación de usuarios en la red inalámbrica

Éste es el escenario de prueba más importante. En él se comprueba que un usuario de la WLAN puede autenticarse y conectarse a la red después de instalar y configurar la solución.

Detalles de ejecución

1. Asegúrese de que un usuario del dominio sea miembro del grupo Usuarios de LAN inalámbrica o del grupo Usuarios del dominio (que es miembro del primer grupo).
2. El usuario deberá iniciar sesión en un equipo cliente que tenga una tarjeta de WLAN instalada y que no esté conectado a la red con cable. El usuario deberá proporcionar las credenciales del dominio durante el inicio de sesión.
3. Abra el panel **Conexiones de red** desde el **Panel de control** y compruebe el estado de las **Conexiones de red inalámbricas**. Debería mostrar el estado **Autenticación satisfactoria** para la conexión inalámbrica.
4. Desde el símbolo del sistema, utilice el comando ping para comprobar la conexión a través de la red con otro equipo de la misma.
5. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de autenticación del usuario.

Escenario 4: comprobación de la autenticación de equipos en la red inalámbrica

En este escenario se comprueba que se ha autenticado un equipo en la red cuando el usuario no ha iniciado una sesión.

Detalles de ejecución

1. Asegúrese de que la cuenta del equipo sea miembro del grupo Equipos de LAN inalámbrica o el grupo Equipos del dominio (que es miembro del primer grupo).
2. Reinicie el equipo después de comprobar que tiene una tarjeta WLAN instalada y que no está conectado a la red con cable.
3. Cuando aparezca el mensaje de inicio de sesión, no inicie la sesión y deje el equipo inactivo unos minutos.
4. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1 para el nombre de host del equipo. Examine la descripción del registro, que debe incluir los detalles de autenticación del equipo.

Escenario 5: comprobación de la autenticación de Pocket PC en la red inalámbrica

En este escenario se comprueba que un usuario puede iniciar una sesión en la red WLAN desde un dispositivo Pocket PC.

Detalles de ejecución

1. Asegúrese de que un usuario del dominio sea miembro del grupo Usuarios de LAN inalámbrica o del grupo Usuarios del dominio (que es miembro del primer grupo).
2. Habilite la conexión inalámbrica en Pocket PC y establezca la configuración de 802.1X en Pocket PC siguiendo las instrucciones que se incluyen en el capítulo 6, "Configuración de clientes de LAN inalámbricas".
3. Mantenga seleccionado el nombre de la red en la lista de redes inalámbricas hasta que aparezca una

opción de conexión. Elija **Conectar** para realizar la conexión.

4. Cuando tenga que especificar las credenciales de domino en la pantalla **Inicio de sesión de red**, escriba el nombre, la contraseña y el dominio del usuario.

5. Si la autenticación es satisfactoria, el icono de estado de la red no tendrá una cruz. Para comprobar el estado, abra **Internet Explorer** en el menú **Inicio** y examine un sitio Web cualquiera de la intranet.

6. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Consulte la descripción del registro, que debe incluir los detalles de autenticación del usuario.

Escenario 6: bloqueo de un cliente WLAN mediante la directiva de acceso remoto IAS

Este escenario se basa en las instrucciones proporcionadas en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas". Un administrador, si es necesario, puede bloquear el acceso inalámbrico de un usuario a la red utilizando la directiva de denegación de acceso remoto (este procedimiento se describe en la sección "Denegación del acceso a WLAN a un usuario o equipo" del capítulo 8). Configure la directiva de denegación de acceso remoto en los servidores IAS antes de ejecutar este escenario de prueba.

Detalles de ejecución

1. Compruebe que la cuenta de un equipo particular sea miembro del grupo Denegar usuarios de LAN inalámbrica.

2. El usuario deberá iniciar sesión en un equipo cliente que tenga una tarjeta de WLAN instalada y que no esté conectado a la red con cable. El usuario deberá introducir las credenciales del dominio al iniciar sesión.

3. El usuario no podrá iniciar una sesión en el dominio; debe aparecer un mensaje de "acceso denegado".

4. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de advertencia del Id. de suceso 2. Examine la descripción del registro, que debe incluir los detalles del error de autenticación del usuario.

Escenario 7: acceso a WLAN denegado si el usuario no es miembro de los grupos de acceso a la WLAN

En este caso se comprueba que se deniega el acceso inalámbrico a la red a un usuario si no es miembro del grupo Usuarios de LAN inalámbrica. Este método es una alternativa al bloqueo del acceso inalámbrico del usuario a la red.

Detalles de ejecución

1. Abra la consola **Usuarios y equipos de Active Directory** en el panel **Herramientas administrativas**.

2. Elimine el grupo Usuarios del dominio del grupo Usuarios de LAN inalámbrica, o elimine un usuario concreto si agrega los usuarios directamente al grupo Usuarios de LAN inalámbrica.

3. El usuario deberá iniciar sesión en un equipo cliente que tenga una tarjeta de WLAN instalada y que no esté conectado a la red con cable. El usuario deberá introducir las credenciales del dominio al iniciar sesión.

4. El usuario no podrá iniciar una sesión en la red; debe aparecer un mensaje de "acceso denegado".

5. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de advertencia del Id. de suceso 2. Examine la descripción del registro, que debe incluir los detalles del error de autenticación del usuario.

Escenario 8: comprobación de la conmutación por error del servicio IAS

En este escenario de prueba se comprueba la disponibilidad del servicio IAS en los clientes inalámbricos cuando

uno de los servidores IAS no está disponible. Este tipo de errores no debería provocar la interrupción de la conexión con la red de los clientes inalámbricos. Éste es un escenario de prueba importante en el que se comprueba que los puntos de acceso cambian a los servidores IAS secundarios cuando el servidor IAS principal no está disponible.

Detalles de ejecución

1. Abra la MMC de **IAS** en el servidor IAS principal de la red y haga clic en el nombre del servidor. A continuación, detenga el servicio IAS haciendo clic en el botón **Detener** de la barra de menús.
2. Utilice una cuenta de usuario de dominio con acceso autorizado a la WLAN e inicie una sesión en la red mediante una conexión inalámbrica.
3. El usuario deberá poder autenticarse en la red y conectarse correctamente a ella. Para comprobarlo, abra el panel **Conexiones de red** desde el **Panel de control** y compruebe el estado de las **Conexiones de red inalámbricas**. El estado debería mostrar **Autenticación satisfactoria** para la conexión inalámbrica.
4. Desde el símbolo del sistema, utilice el comando **ping** para comprobar la conexión a través de la red con otro equipo de la misma.
5. En el servidor IAS secundario, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de autenticación del usuario.

Escenario 9: desplazamiento de clientes inalámbricos entre puntos de acceso y reautenticación en la WLAN

En este escenario se comprueba que los clientes inalámbricos pueden desplazarse entre puntos de acceso, lo que provoca la reautenticación (o la reconexión rápida, si está habilitada). Es importante comprobar este escenario antes de implementar la solución en el entorno de producción. En esta prueba se comprueba que la conexión de la red inalámbrica no se interrumpe para los usuarios.

Detalles de ejecución

1. Utilizando una cuenta de usuario de dominio con acceso autorizado a la WLAN, inicie una sesión en la red mediante una conexión inalámbrica. Compruebe que la conexión de red se ha realizado correctamente.
2. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de autenticación del usuario.
3. En los detalles de autenticación del usuario, busque la dirección IP del punto de acceso con el que esté conectado el usuario. Este valor aparece en el campo **Dirección IP del cliente**.
4. Desplácese con el equipo a otra ubicación para que el cliente esté cerca de un punto de acceso vecino y lejos del punto de acceso con el que estaba conectado.
5. Esto hará que el cliente Windows XP vuelva a autenticarse y se conecte con el nuevo punto de acceso.
6. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de reautenticación del usuario; el campo **Dirección IP del cliente** debe incluir la dirección IP del nuevo punto de acceso.

Escenario 10: reautenticación del cliente inalámbrico porque se ha agotado el tiempo de espera de la sesión IAS

En este escenario se comprueba la rotación de claves WEP dinámicas configuradas en la directiva de solicitud de conexión IAS. En esta prueba se comprueba que los clientes se reautentican periódicamente (después del tiempo configurado) para que las claves WEP continúen cambiando.

Detalles de ejecución

1. Utilizando una cuenta de usuario de dominio con acceso autorizado a la WLAN, inicie una sesión en la red mediante una conexión inalámbrica. Compruebe que la conexión de red se ha realizado correctamente.
2. En el servidor IAS, abra **Visor de sucesos**. El registro de sucesos del **Sistema** debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de autenticación del usuario.
3. Deje el cliente conectado a la red un período de tiempo superior a una hora. Puede iniciar una solicitud ICMP continua en otro equipo de la red para comprobar que la conexión está activada.
4. Cuando transcurra la hora, abra **Visor de sucesos** y consulte el registro de sucesos del **Sistema**. El registro debe contener un registro IAS de tipo de información del Id. de suceso 1. Examine la descripción del registro, que debe incluir los detalles de reautenticación del usuario.

Escenario 11: alerta de correo electrónico de un error de copia de seguridad de IAS

En este caso de prueba se comprueba que las alertas de correo electrónico están correctamente configuradas para los servidores IAS, tal y como se describe en esta solución. Si se han implementado correctamente, estas alertas aumentan significativamente la capacidad de administración del servicio IAS, que es fundamental para la conectividad de la red inalámbrica. La situación ideal sería que esta prueba se realizase después de la implementación para confirmar que los servicios de notificación se ejecutan correctamente.

Para realizar la prueba en este escenario, se simula un error de copia de seguridad de IAS con el fin de crear las alertas de correo electrónico necesarias. Los pasos para configurar la copia de seguridad de IAS que se deben realizar en este escenario se proporcionan en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas". Antes de ejecutar este escenario de prueba, debe leer el capítulo 8 y configurar las secuencias de comandos.

Detalles de ejecución

1. Abra un shell de comandos con el acceso directo MSS WLAN Tools.
2. Edite el archivo **Constants.vbs** y establezca el parámetro **ALERT_EMAIL_ENABLED** en **True**.
3. Configure el parámetro **ALERT_EMAIL_RECIPIENTS** con las direcciones de correo electrónico de las personas a las que se deba alertar.
4. Configure el parámetro **ALERT_EMAIL_SMTP** con el nombre DNS o la dirección IP del servidor SMTP.
5. Ejecute el siguiente comando de copia de seguridad de IAS en una carpeta que no exista:

   MSSTools BackupIAS /path: *C:\RutaIASIncorrecta.*
6. En el servidor IAS, abra **Visor de sucesos**.El registro de sucesos de la **Aplicación** debe contener un registro de operaciones IAS de tipo de error del Id. de suceso 211.
7. Las personas identificadas para las alertas recibirán una alerta de correo electrónico.

Escenario 12: alerta de correo electrónico de un error de servicio de entidad emisora

Este escenario de prueba es parecido al de la alerta de un error de copia de seguridad de IAS. En él se comprueba que las alertas de correo electrónico se envían al personal de administración si falla el servicio de entidad emisora.

Los pasos para configurar la copia de seguridad de entidad emisora que se necesita en este escenario se proporcionan en el capítulo 8, "Mantenimiento de soluciones de seguridad en LAN inalámbricas". Antes de ejecutar este escenario de prueba, debe leer el capítulo 8 y configurar las secuencias de comandos necesarias.

Detalles de ejecución

1. Abra un shell de comandos con el acceso directo MSS WLAN Tools.
2. Edite el archivo **Constants.vbs** y establezca el parámetro **ALERT_EMAIL_ENABLED** en **True**.
3. Configure el parámetro **ALERT_EMAIL_RECIPIENTS** con las direcciones de correo electrónico de las personas a las que se deba alertar.
4. Configure el parámetro **ALERT_EMAIL_SMTP** con el nombre DNS o la dirección IP del servidor SMTP.
5. Abra la **Entidad emisora de certificados** en el panel **Herramientas administrativas**. Haga clic en el nombre de la entidad emisora y seleccione **Acción**, **Todas las tareas** y **Detener servicio**.
6. Abra la MMC de **Servicios** en el panel **Herramientas administrativas**.
7. Haga clic con el botón secundario en **Servicios de Certificate Server** y seleccione **Propiedades**. Cambie el tipo de **Inicio** a **Deshabilitar** y haga clic en **Aceptar** para cerrar.
8. Ejecute el siguiente comando de entidad emisora:

   MSSTools CheckCA
9. En el servidor de entidad emisora, abra **Visor de sucesos**.El registro de sucesos de la **Aplicación** debe contener un registro de operaciones de la entidad emisora de tipo de error del Id. de suceso 1.
10. Las personas identificadas para las alertas recibirán una alerta de correo electrónico cuando falle el servicio de entidad emisora.
11. Invierta el tipo de **Inicio** de **Servicios de Certificate Server** a **Automático** en la MMC de **Servicios**.
12. Inicie el servicio en la MMC de **Entidad emisora de certificados** haciendo clic en el botón **Inicio** de la barra de menús.

Principio de la página

Herramientas de la prueba

Las siguientes herramientas se han utilizado durante la prueba de esta solución. Algunas de estas herramientas también se han utilizado durante las fases de creación y mantenimiento:

1. **Certutil:** ésta es una herramienta multipropósito que se utiliza para configurar la entidad emisora; volcar y visualizar información sobre la configuración de entidad emisora; hacer copias de seguridad y restaurar componentes de entidad emisora; y comprobar certificados, pares de claves y cadenas de certificados.
2. **Dcdiag:** esta herramienta analiza el estado de los controladores de dominio en un bosque o empresa.
3. **Visor de registro de sucesos:** esta herramienta supervisa y captura los registros relacionados con las aplicaciones, la seguridad y el sistema.
4. **Consola de administración de directivas de grupo:** esta herramienta se utiliza para visualizar y editar objetos de directiva de grupo en Active Directory.
5. **NetMon:** esta utilidad captura y filtra las tramas del tráfico de red hacia y desde el equipo en el que está instalada. Esta herramienta no es necesaria directamente, pero es muy útil en la depuración de problemas de autenticación. Esta herramienta se puede instalar desde el **Panel de control** seleccionando **Agregar o quitar componente**, **Componentes de Windows**, **Herramientas de administración y supervisión** y **Herramientas del monitor de red**.
6. **Netsh:** ésta es una utilidad de secuencia de comandos de línea de comandos que permite visualizar o modificar, ya sea de forma local o remota, la configuración de red de un equipo en ejecución. Es una herramienta multipropósito que se utiliza en las operaciones relacionadas con IAS.

7. **Copia de seguridad de Windows:** ésta es la herramienta de copia de seguridad y restauración proporcionada con Windows que realiza operaciones de copia de seguridad y restauración en archivos, carpetas y el estado del sistema. Esta herramienta se puede ejecutar con un asistente o una línea de comandos.
8. **PerfMon:** esta herramienta permite ver los registros de rendimiento del sistema y los contadores. Puede utilizar esta herramienta para supervisar el rendimiento de IAS.
9. **Ping:** esta herramienta comprueba la conectividad de nivel IP con otro equipo TCP/IP mediante el envío de mensajes de solicitud de eco de ICMP. Los mensajes correspondientes de respuesta de eco que se reciben se visualizan con tiempos de retorno.
10. **Schtasks:** esta herramienta programa comandos y programas para que se ejecuten periódicamente o a una hora determinada. Agrega y elimina tareas de la programación, inicia y detiene tareas a petición, y visualiza y cambia tareas programadas.

La mayoría de estas herramientas se instalan automáticamente cuando se instala el sistema operativo Windows. La instalación del resto de herramientas se describe en el capítulo 3, "Preparación del entorno".

Principio de la página

Resumen

Este capítulo trata sobre la prueba de seguridad de la solución WLAN. En la primera parte del capítulo se describen brevemente los parámetros utilizados por Microsoft para probar esta solución en la fase de desarrollo. En la segunda parte se incluyen las instrucciones para realizar algunos de los escenarios de prueba más importantes que se utilizan para probar esta solución. Estos escenarios de prueba permiten comprobar el funcionamiento correcto de la infraestructura de seguridad de WLAN antes de implementarla en un entorno de producción.

Principio de la página