Latinoamérica

Microsoft TechNet

Capítulo 5: Diseño de una infraestructura de RADIUS para la seguridad de LAN inalámbricas

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

En esta página

Introducción

El objetivo de este capítulo es describir la arquitectura y el diseño de la infraestructura del servicio de usuario de acceso telefónico de autenticación remota (RADIUS, Remote Authentication Dial-In User Service) utilizada en esta solución de red de área local inalámbrica (WLAN, Wireless Local Area Network). La infraestructura de RADIUS utiliza la implementación de Microsoft RADIUS: el servicio de autenticación de Internet (IAS, Internet Authentication Service) de Microsoft®.

El primer objetivo del capítulo consiste en mostrar las decisiones sobre diseño implicadas en la infraestructura de IAS para la solución y el razonamiento que acompaña a dichas decisiones.

Las expresiones como “Esta solución utiliza la opción...” o “Este diseño usa...” que aparecen en este capítulo hacen referencia a decisiones tomadas como parte del diseño de la solución implementadas en los capítulos de las guías de generación y operaciones.

El segundo objetivo de este capítulo consiste en determinar si el diseño es adecuado para su organización. Las expresiones como “Debería considerar...” hacen referencia a contextos en los que debe tomar decisiones según sus propios requisitos. En la mayoría de los casos, esto ocurrirá durante la descripción de formas en que podría ampliar la solución para cubrir las necesidades de seguridad más generales de su organización. Por esta razón, algunos temas ofrecen consideraciones más detalladas que le ayudarán a comprender las implicaciones de los pasos específicos y evitarán que tenga que consultar otros documentos.

Requisitos previos

Antes de continuar con este capítulo, le resultará útil familiarizarse con los conceptos de RADIUS y las opciones de implementación de IAS. Encontrará referencias a fuentes de información importantes en la sección “Información adicional” al final de este capítulo. Adicionalmente, se incluye información útil en los capítulos sobre IAS del *kit de recursos* de *Microsoft Windows Server™ 2003* y el *kit de implementación* de *Microsoft Windows Server™ 2003*.

Descripción general del capítulo

El capítulo se presenta dividido en temas que tratan del diseño de una infraestructura de RADIUS. Los objetivos del capítulo son los siguientes:

- ofrecer información general acerca del uso de IAS para proporcionar una solución general de administración de acceso a la red y su aplicación específica a las WLAN.
-

identificar los requisitos del entorno TI para la solución y examinar la infraestructura existente.

- especificar las decisiones de diseño que deben tomarse durante la creación de la arquitectura para una infraestructura de RADIUS basada en IAS, específicamente las decisiones relacionadas con el uso de redes inalámbricas basadas en 802.1X.
- Explorar las estrategias de administración para el mantenimiento de la infraestructura del servidor IAS.
- proporcionar referencias a información adicional sobre conceptos, detalles del producto y planeamiento de la implementación.

El diagrama de flujo siguiente ilustra la estructura del capítulo.

Figura 5.1: Planeamiento de

una infraestructura de IAS

Principio de la página

Utilización de IAS para la administración de acceso a la red

El Servicio de autenticación de Internet en Windows Server™ 2003 de Microsoft constituye la implementación de Microsoft de un servidor y proxy RADIUS. Como servidor RADIUS, IAS realiza la autenticación, autorización y contabilidad (AAA) centralizadas de diversos tipos de conexiones de red. Como proxy RADIUS, IAS puede reenviar las solicitudes RADIUS a otro servidor RADIUS para realizar la AAA. IAS se puede utilizar con servidores red privada virtual (VPN, Virtual Private Network), como el Servicio de enrutamiento y acceso remoto (RRAS, Routing and Remote Access Service) basado en Microsoft Windows®, o bien con otra infraestructura de acceso a la red, como los puntos de acceso inalámbricos y los conmutadores Ethernet de autenticación.

Para maximizar el valor de una infraestructura de RADIUS basada en IAS, debe tomarse una decisión que abarque toda la organización para utilizar los servicios centralizados en la administración de acceso a la red. Esto incluye la utilización de una base de datos de cuentas centralizada, como el servicio de directorio Active Directory® y la centralización de la administración de las directivas de acceso a la red en los servidores IAS. La administración centralizada permite reducir en gran medida los costos asociados al mantenimiento de la información de control de acceso a la red en el equipo de acceso a la red distribuido. Asimismo, el aprovechamiento de directivas de acceso a la red y cuentas centralizadas ayuda a reducir los riesgos de seguridad asociados a la configuración y a la administración de equipos distribuidos.

El planeamiento y la implementación de una infraestructura de IAS que se adapte a las necesidades actuales y futuras de su organización requieren un estudio minucioso. IAS no se ha diseñado para proporcionar acceso a una única red aislada, sino que debe implementarse para proporcionar una administración estratégica de acceso a la red que sirva para diversos escenarios.

Identificación de los requisitos organizativos de administración de acceso a la red

IAS de Windows Server 2003 admite diversos escenarios de acceso a la red, entre los que se incluyen:

- **Acceso inalámbrico**. Es posible configurar puntos de acceso inalámbricos compatibles con 802.1X y aprovechar los servicios AAA de IAS para el control de acceso a WLAN basada en 802.11, así como para proporcionar la administración de claves.
- **Acceso por cable**. Los conmutadores Ethernet compatibles con 802.1X pueden usar los servicios AAA de IAS para el control de acceso de cada puerto a LAN por cable.
- **Acceso a VPN**. Los servidores VPN como RRAS basado en Windows pueden utilizar los servicios AAA de IAS para el control de acceso a la red corporativa, así como para proporcionar la administración de claves.
- **Acceso telefónico**. Los servidores de acceso telefónico como RRAS basado en Windows pueden usar los servicios AAA de IAS para el control de acceso a la red corporativa.
- **Acceso a la extranet**. Los servidores de acceso a la extranet pueden aprovechar los servicios AAA de IAS cuando se proporciona acceso restringido a los recursos compartidos.
- **Acceso a la red corporativa externa**. Los proveedores de soluciones de red pueden aprovechar los servicios AAA de IAS para integrar la infraestructura de red externa en las directivas de control de acceso y bases de datos de cuentas de los clientes. IAS puede proporcionar la información contable requerida para facturar a los clientes por este servicio.
- **Acceso a Internet**. Los proveedores de servicios de Internet (ISP) pueden aprovechar los servicios AAA de IAS para proporcionar acceso a Internet telefónico y de alta velocidad mientras emplean las bases de datos de cuentas y las directivas de control de acceso organizativas individuales. IAS puede proporcionar la información contable requerida para facturar a los clientes por este servicio.

Para maximizar la inversión en IAS y minimizar los cambios futuros de la infraestructura de IAS, debe evaluar cada uno de estos escenarios con respecto a su organización. Aunque IAS sólo se utiliza en esta solución para el

acceso a la red inalámbrica, dicha solución puede ampliarse para admitir cada uno de estos escenarios. El capítulo 3, Arquitectura de la solución para una LAN inalámbrica segura, ofrece información adicional acerca de la ampliación de la infraestructura de RADIUS para admitir escenarios adicionales.

Utilización de IAS para la administración de acceso a la red inalámbrica

El uso de WLAN se está generalizando con la adopción de normas en el sector, como los estándares 802.11 del IEEE (Institute of Electrical and Electronics Engineers). Las WLAN permiten a los usuarios desplazarse por un edificio o recinto y conectarse automáticamente a la red mediante puntos de acceso inalámbrico.

Si bien las WLAN son muy convenientes, presentan los riesgos de seguridad siguientes:

- Una persona que tenga un adaptador de WLAN compatible puede obtener acceso a la red.
- Las señales de red inalámbrica utilizan ondas de radio para enviar y recibir información. Una persona que se encuentre a una distancia apropiada de un punto de acceso inalámbrico puede detectar y recibir todos los datos enviados a y desde el punto de acceso inalámbrico.

Una forma de contrarrestar el primer riesgo de seguridad consiste en configurar los puntos de acceso inalámbricos como clientes RADIUS y, a continuación, configurarlos para que envíen peticiones de acceso y mensajes de cuentas a un servidor RADIUS central que ejecute IAS. Para contrarrestar el segundo riesgo de seguridad, pueden cifrarse los datos enviados entre los dispositivos inalámbricos y los puntos de acceso inalámbricos.

IAS mejora la seguridad de las LAN inalámbricas de dos modos: actúa como servidor RADIUS para los dispositivos cliente y puntos de acceso inalámbricos IEEE 802.1X, y ofrece claves de cifrado dinámicas a través de protocolos de autenticación basados en certificados, como el protocolo de autenticación extensible - protocolo de seguridad de la capa de transporte (EAP-TLS, Extensible Authentication Protocol – Transport Layer Security).

Nota: en este manual los puntos de acceso inalámbricos pueden denominarse también "clientes RADIUS". Aunque los puntos de acceso inalámbricos no son el único tipo de cliente RADIUS posible, éste es el único tipo de cliente RADIUS que se trata en esta guía. Por lo tanto, ambos términos pueden usarse indistintamente.

Principio de la página

Identificación de los requisitos previos de la solución

Antes de empezar a diseñar una solución de administración de acceso inalámbrico mediante IAS, asegúrese de conocer las condiciones existentes necesarias en su entorno.

Consideraciones de Active Directory

Esta solución está diseñada para las organizaciones que han implementado Active Directory y ejecutan Microsoft Windows 2000 Server, o una versión posterior, en los controladores de dominio. Ésta es una condición necesaria, ya que varias de las decisiones sobre el diseño de la infraestructura de RADIUS que se han tomado utilizan características que sólo están disponibles en dominios actualizados al modo nativo de Windows 2000 o posterior. La tabla siguiente muestra algunas características utilizadas en esta solución y su compatibilidad con diversos niveles de funciones de dominio.

Tabla 5.1: Características de dominio de Windows utilizadas en la solución

Característica	Modo nativo de Windows Server 2003	Modo nativo de Windows 2000	Modo mixto- o bien - Microsoft Windows NT® 4.0
Grupos universales y anidados	Sí	Sí	No
Nombres principales de usuario (UPN)	Sí	Sí	No
Control del acceso a través del	Sí	Sí	No

permiso RAP (directiva de acceso remoto) disponible en la cuenta de usuario			
Compatibilidad con EAP-TLS	Sí	Sí	No

Nota: la implementación de los Servicios de Certificate Server en esta solución también tiene requisitos específicos de Active Directory. Para obtener más información, consulte el capítulo 4, Diseño de la infraestructura de claves públicas.

Aunque no es necesario, es posible que tras leer este capítulo decida implementar IAS en los controladores de dominio. Esta solución se basa en IAS de Windows Server 2003 y, por lo tanto, es necesario actualizar los controladores de dominio de destino a esta versión del sistema operativo. Más adelante en este capítulo se ofrece información acerca de la co-ubicación de IAS con controladores de dominio.

Infraestructura de RADIUS preexistente

Esta solución no cubre la integración de servidores RADIUS existentes en su entorno. Sin embargo, los servidores RADIUS basados en IAS y de terceros pueden integrarse en la solución. En la mayoría de los casos utilizará IAS de Windows Server 2003 para beneficiarse de las características relacionadas con el acceso a la WLAN.

Los servidores RADIUS basados en sistemas Windows antiguos se pueden actualizar a Windows Server 2003 para poder utilizarlos como servidores RADIUS principales en esta solución. Como alternativa, es posible cambiar los servidores RADIUS existentes a tráfico de proxy RADIUS para los nuevos servidores RADIUS basados en Windows Server 2003.

Para obtener instrucciones de planeamiento detalladas acerca de la migración de la infraestructura de RADIUS existente a IAS de Windows Server 2003, consulte a su colaborador de Microsoft o póngase en contacto con el ejecutivo de cuentas de Microsoft que pueda remitirle al colaborador adecuado o a los profesionales de los Servicios de consultoría de Microsoft.

Principio de la página

Diseño de la infraestructura de RADIUS

Cuando utilice IAS para el acceso a WLAN basada en 802.1X, deberá tomar varias decisiones sobre el diseño. En esta sección se describen algunas de estas decisiones y se tratan las opciones seleccionadas para esta solución. Debe evaluar la capacidad de aplicación a su entorno de cada una de dichas decisiones.

Determinación de la función de IAS como servidor RADIUS

Los servidores IAS pueden implementarse para utilizarlos en tres funciones RADIUS conceptuales diferentes:

- Servidor RADIUS
- Proxy RADIUS
- Servidor y proxy RADIUS

  Nota: en estas instrucciones, los términos servidor RADIUS y proxy RADIUS se utilizan para describir un servidor IAS configurado para realizar dichas funciones.

En la tabla siguiente se muestran algunas de las capacidades de los servidores configurados para realizar estas funciones, y se identifica su utilidad en escenarios reales.

Tabla 5.2: Funciones RADIUS de IAS

Función RADIUS de	Capacidades	Escenario

IAS		
Servidor RADIUS	– Compara las credenciales directamente con Active Directory u otras fuentes de datos importantes. – Aprovecha RAP para determinar el acceso a la red.	Necesario para todos los escenarios de administración de acceso a la red
Proxy RADIUS	– Enruta la solicitud en función de las propiedades de la misma. – Es posible modificar las propiedades de RADIUS de las solicitudes en tránsito. – Proporciona equilibrio de carga de las solicitudes RADIUS a grupos de servidores RADIUS.	– Útil en escenarios de varios bosques en los que se comparte el equipo de acceso a la red. – Útil para la implementación de arquitecturas AAA de red cliente/servidor a gran escala. – Útil para la federación de autenticación con organizaciones externas.
Servidor y proxy RADIUS	Combinación de las dos capacidades anteriores	Combinación de ambos escenarios

No todas las funciones RADIUS son necesarias para todos los escenarios de administración de acceso a la red. Por ejemplo, en muchas organizaciones, la administración de acceso a LAN inalámbrica sólo requiere la función de servidor RADIUS. No obstante, si su organización tiene previsto utilizar la infraestructura de red inalámbrica para atender a usuarios y dispositivos de bosques múltiples de Active Directory, también será necesaria la función de proxy RADIUS para enrutar las solicitudes a servidores RADIUS independientes de cada bosque.

Para mantener la simplicidad y un costo reducido, la solución incluye servidores IAS configurados como servidores RADIUS. No implementa IAS como proxy RADIUS.

Conmutación por error y equilibrio de carga del servidor

RADIUS es un componente crítico de cualquier solución de administración de acceso a LAN inalámbrica basada en 802.1X. La disponibilidad de servidores IAS para los puntos de acceso inalámbricos que los utilizan determina la disponibilidad de WLAN para los usuarios finales. Por lo tanto, deberá asegurarse de que haya dos o más servidores IAS disponibles en todo momento para los puntos de acceso inalámbricos. La mayoría de los puntos de acceso inalámbricos modernos incluyen la capacidad de configurar dos servidores RADIUS para la autenticación y otros dos para la contabilidad. De esta forma se garantiza que la pérdida de contacto con un único servidor RADIUS no afecte al servicio de los clientes de WLAN.

En lo que respecta a la implementación de varios servidores para lograr resistencia, muchas organizaciones se beneficiarán de la selección de un esquema para equilibrar la carga de las solicitudes desde puntos de acceso inalámbricos configurados como clientes RADIUS en servidores RADIUS, a fin de asegurarse de que ningún servidor tenga limitación de recursos.

Antes de elegir una estrategia de equilibrio de carga, es importante tener presente que 802.1X implementa EAP en RADIUS (EAP-RADIUS) entre los puntos de acceso inalámbricos y los servidores RADIUS. Aunque RADIUS utiliza el protocolo de datagramas de usuario (UDP, User Datagram Protocol) sin conexión, EAP es un protocolo orientado a la sesión con túnel en RADIUS. Esto significa que es necesario garantizar que varios paquetes EAP-RADIUS que incluyen una única operación de autenticación regresen al mismo servidor RADIUS en caso de que se produzcan fallos en las autenticaciones.

La tabla siguiente muestra varias opciones para garantizar que los clientes RADIUS puedan utilizar múltiples servidores RADIUS para las solicitudes RADIUS de equilibrio de carga y lograr un nivel superior de resistencia.

Tabla 5.3: Opciones de conmutación por error y equilibrio de carga de EAP-RADIUS

Método de conmutación por error y equilibrio de carga	**Ventajas**	**Inconvenientes**
Servidores proxy IAS con grupos de servidores RADIUS	– Detección de errores del servicio RADIUS con conmutación por error y conmutación por recuperación. – Distribución de la carga de tráfico en función de las propiedades de tráfico. – Mantiene el estado de la sesión EAP durante el equilibrio de carga. – Distribución configurable de las solicitudes a servidores en función de los parámetros de importancia y prioridad.	– Se requieren servidores IAS adicionales. – Todavía se da el requisito de configuración de los puntos inalámbricos con IP de proxy RADIUS principal y secundario.
Configuración de los servidores RADIUS principal y secundario en puntos de acceso inalámbricos	– Configuración sencilla para entornos pequeños. – El punto de acceso inalámbrico detecta los errores de tráfico y realiza la conmutación por error. – Utiliza las funciones nativas del punto de acceso inalámbrico.	– Es necesario planear y supervisar con detenimiento la selección de los servidores RADIUS principal y secundario. – Muchos puntos de acceso inalámbricos no admiten la función de conmutación por recuperación, lo que provoca el desequilibrio de la carga de los servidores.

Las organizaciones empresariales y los proveedores de servicios de red de gran tamaño deberían plantearse la utilización de los proxy RADIUS para aceptar solicitudes de clientes RADIUS y distribuir la carga a servidores RADIUS, que pueden configurarse en grupos de servidores RADIUS. Puede basar la distribución del tráfico de red a los servidores RADIUS en grupos de servidores RADIUS en diversos elementos configurables. Estos elementos incluyen el tipo de tráfico RADIUS y los atributos RADIUS, además de los valores de prioridad e importancia. A continuación, los servidores RADIUS de cada grupo podrán llevar a cabo la autenticación y autorización principal de los usuarios y dispositivos de un dominio o de todo un bosque. Esto crea una arquitectura cliente/servidor eficaz para atender las solicitudes RADIUS y ofrece flexibilidad óptima en cuanto a las opciones de ajuste de escalabilidad y equilibrio de carga.

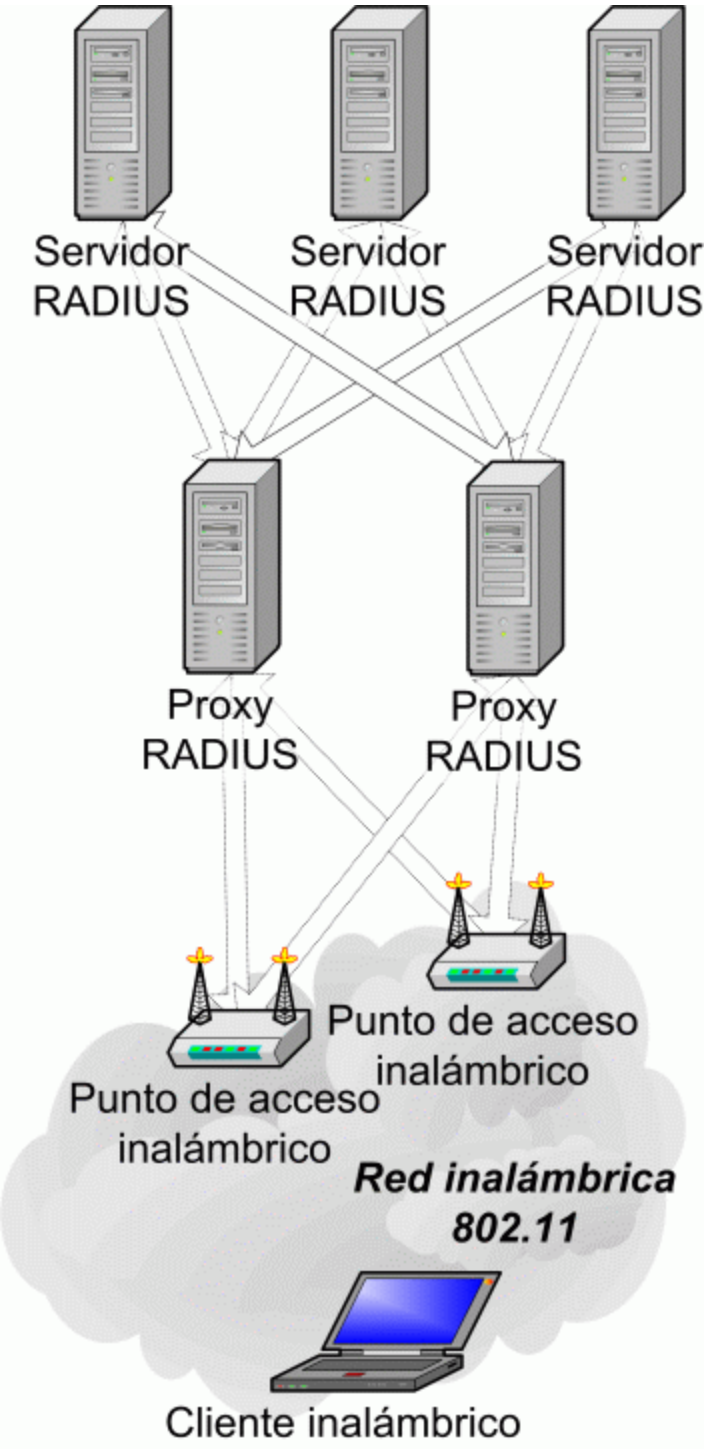

Figura 5.2 Conmutación por error y equilibrio de carga mediante servidores proxy RADIUS

No obstante, las capacidades de conmutación por error de los servidores RADIUS de los puntos de acceso inalámbricos modernos proporcionan un nivel de resistencia adecuado para la mayoría de las organizaciones. En caso de no ser suficiente, la ruta de migración de una estrategia de conmutación por error y equilibrio de carga de proxy RADIUS es relativamente sencilla. Uno de los inconvenientes de la utilización de una estrategia de conmutación por error y equilibrio de carga basada en puntos de acceso inalámbricos es el exceso de carga de administración que comporta emparejar los puntos de acceso inalámbricos con servidores RADIUS, supervisar la carga irregular de los servidores RADIUS y realizar modificaciones en caso necesario. Otro inconveniente de

este tipo de estrategia es que algunos modelos de puntos de acceso inalámbricos no son compatibles con la conmutación por recuperación. La conmutación por recuperación se produce cuando un punto inalámbrico que ha fallado al utilizar un servidor RADIUS secundario regresa automáticamente al uso del servidor RADIUS primario designado tras la recuperación de este servidor. Sin la conmutación por recuperación, es posible que todos los puntos de acceso inalámbrico se conmuten por error al servidor RADIUS secundario y requieran la intervención del administrador para redirigirlos al servidor primario correcto.

Para conseguir el equilibrio de carga mediante una estrategia de conmutación por error basada en puntos de acceso inalámbricos cuando hay varios servidores RADIUS disponibles localmente:

- Configure la mitad de los puntos de acceso inalámbricos de cada ubicación para que utilicen en primer lugar el servidor RADIUS principal y, cuando éste falle, empleen el secundario.
- Configure la otra mitad de los puntos de acceso inalámbricos de cada ubicación para que utilicen en primer lugar el servidor RADIUS secundario y, cuando éste falle, empleen el principal.

  Nota: los términos “principal” y “secundario” no indican diferencias de funcionalidad entre los servidores: son idénticos. Estos términos se utilizan para distinguir entre los servidores en las consideraciones de la conmutación por error.

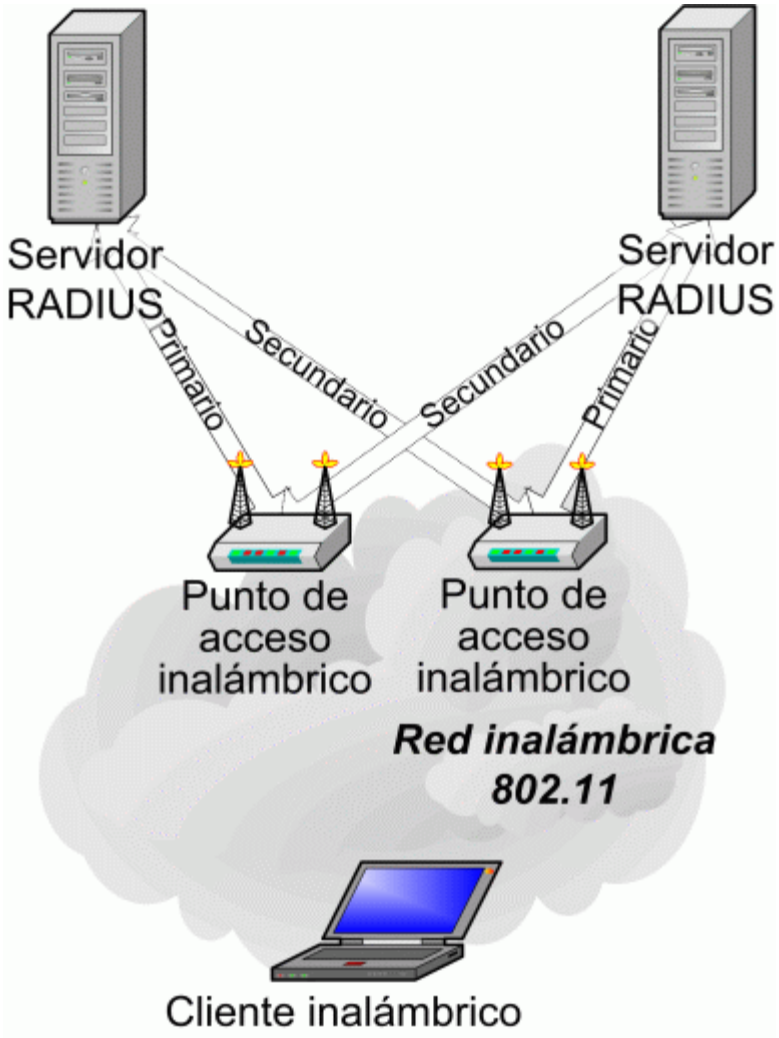

Figura 5.3 Estrategia de conmutación por error y equilibrio de carga basada en puntos de acceso inalámbricos

Para conseguir el equilibrio de carga mediante una estrategia de conmutación por error basada en puntos de acceso inalámbricos en sucursales en las que se dispone de un servidor RADIUS local pero también de uno

remoto, debe configurar todos los puntos de acceso inalámbricos de la sucursal para que utilicen como servidor principal el servidor RADIUS local. A continuación, configure el servidor RADIUS remoto como servidor secundario para utilizarlo en caso de que falle el servidor principal.

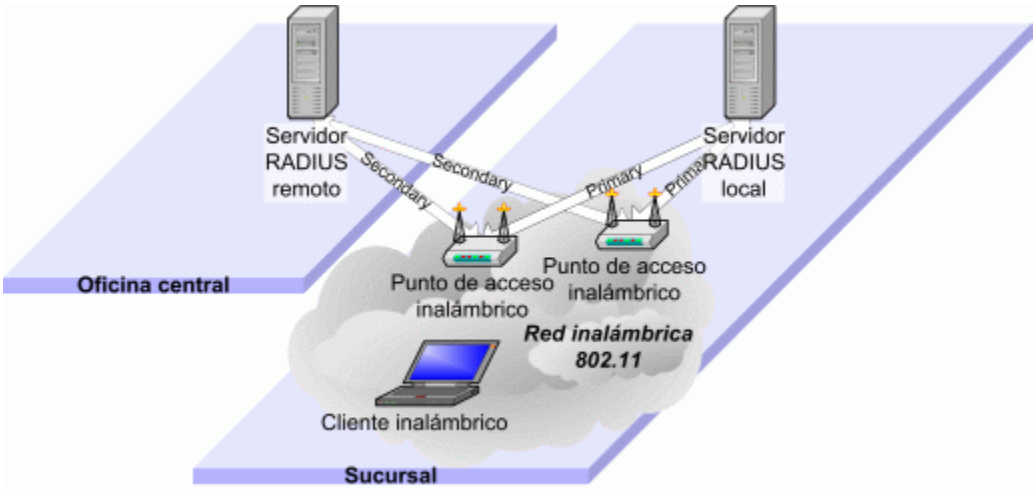

Figura 5.4 Estrategia de conmutación por error y equilibrio de carga basada en puntos de acceso inalámbricos con servidores RADIUS locales y remotos
Ver imagen a tamaño completo

En escenarios de sucursal, asegúrese de que los puntos de acceso inalámbricos admitan la conmutación por recuperación en el servidor RADIUS principal cuando éste regrese al servicio. De lo contrario habrá que reconfigurar manualmente los puntos de acceso inalámbricos para evitar ataques transversales de WAN innecesarios del servicio RADIUS.

Nota: consulte a su proveedor de hardware sobre la compatibilidad de sus productos con la conmutación por recuperación.

Los servidores RADIUS de sucursal son opcionales y, en su lugar, pueden utilizarse servidores RADIUS centralizados en una WAN. Sin embargo, sin un controlador de dominio y un servidor RADIUS local, los usuarios en la oficina remota no podrán acceder a la WLAN local en caso de error de la WAN.

Esta solución está diseñada para aprovechar la conmutación por error de servidor basada en puntos de acceso inalámbricos y la configuración manual para equilibrio de carga. Para obtener más información sobre el planeamiento de una infraestructura de RADIUS que aproveche los proxy RADIUS para la conmutación por error y el equilibrio de carga de servidor, consulte el capítulo “Deploying IAS”, sobre la implementación de IAS, incluido en el *kit de implementación* de *Microsoft Windows Server 2003*. Encontrará una referencia a este recurso al final de este capítulo.

Establecimiento de los requisitos de registro

Puede configurar los servidores IAS para registrar dos tipos de información opcional:

- sucesos de autenticación satisfactorios y rechazados.
- información de autenticación y contabilidad RADIUS.

Los sucesos de autenticación satisfactorios y los rechazados generados a partir de dispositivos y usuarios que intentan obtener acceso a la LAN inalámbrica se registran de forma predeterminada en el registro de sucesos del sistema Windows Server 2003 de IAS. La información del registro de sucesos de autenticación es muy útil para la solución de problemas de autenticación, aunque también puede utilizarse con fines de alerta y auditoría de seguridad.

Inicialmente, debe dejar habilitado el registro de sucesos **satisfactorios** y **rechazados**, pero puede considerar la deshabilitación de los sucesos **satisfactorios** una vez que el sistema se haya estabilizado. Los sucesos de

acceso a LAN inalámbrica satisfactorios llenan rápidamente el registro de sucesos del sistema y pueden ser innecesarios a efectos de seguridad, siempre que el registro de solicitudes de autenticación RADIUS esté habilitado.

Las empresas deben considerar la utilización de herramientas de supervisión empresarial como Microsoft Operations Manager (MOM), que actúen en los sucesos IAS del registro de sucesos del sistema mediante secuencias de comandos personalizadas. Por ejemplo, una secuencia de comandos MOM personalizada puede detectar un aumento de los sucesos IAS relacionados con intentos de autenticación rechazados, y notificarlo a un administrador para que realice la acción pertinente.

IAS también ofrece la posibilidad de guardar información de la sesión de autenticación y del acceso a la red, en forma de registros de peticiones RADIUS. Puede habilitar y deshabilitar determinadas opciones para proporcionar la información siguiente de los registros de solicitudes RADIUS:

- Solicitudes contables: por ejemplo, mensajes contables de inicio y detención que indican el inicio y el final de una sesión de acceso a la red.
- Solicitudes de autenticación: por ejemplo, mensajes de acceso aceptado o acceso rechazado que indican el fracaso o el éxito de los intentos de autenticación.
- Estado periódico: por ejemplo, solicitudes contables provisionales que envían algunos dispositivos de acceso a la red.

Los registros de peticiones RADIUS suelen ser más útiles para aquellas organizaciones tales como proveedores de servicios de red, que cobran a los clientes una tarifa en función de la utilización de la red. Sin embargo, los registros de solicitudes RADIUS también se pueden utilizar a efectos de seguridad. En concreto, los registros de autenticación y contabilidad RADIUS permiten que los auditores de seguridad determinen cuestiones como las siguientes:

- detalles de los intentos de autenticación no autorizados en la WLAN.
- duración de las conexiones aceptadas en la WLAN.

IAS puede registrarse en bases de datos de Microsoft SQL Server™ 2000 o registros de texto. El registro basado en texto de información de autenticación y contabilidad RADIUS está deshabilitado de forma predeterminada en IAS. Antes de habilitarlo, deberá:

- comunicarse con el personal de seguridad de su organización para conocer los requisitos de seguimiento de la información de acceso a WLAN y qué detalles son necesarios.
- realizar pruebas de laboratorio del registro de texto RADIUS para conocer los requisitos de hardware del servidor (disco y CPU) durante el equilibrio de carga de los usuarios de LAN inalámbrica. el acceso a LAN inalámbrica genera mucha más información que otros tipos de acceso a la red.
- diferenciar entre la parte necesaria de la información de solicitudes RADIUS (autenticación, contabilidad y estado periódico) y la parte opcional. El acceso a LAN inalámbrica puede generar gran cantidad de información que consume rápidamente espacio en disco.
- Determinar una estrategia para tener acceso, almacenar y archivar la información del registro de peticiones RADIUS. Dicha información puede guardarse como archivos de texto en el disco duro de cada servidor IAS o bien en una base de datos de Microsoft SQL Server.

Las empresas que necesitan los registros contables de RADIUS deberán considerar el uso de las características de registro de SQL Server de IAS. La información contable de RADIUS se puede registrar en SQL Server Desktop Engine (MSDE 2000) de cada servidor IAS y replicarse en un clúster central de SQL Server. Esta estrategia ofrece el almacenamiento centralizado y estructurado de los datos contables de RADIUS para facilitar las consultas, la creación de informes y el archivo. La realización del registro de SQL Server en bases de datos MSDE locales elimina también la posibilidad de que los problemas de la red impidan que IAS registre la información y, por tanto, se rechacen las solicitudes de acceso a la red.

Las organizaciones que carecen de SQL Server 2000 o de personal para realizar las consultas, la creación de

informes y el archivo regulares de los registros de solicitudes RADIUS deben considerar el registro de esta información para facilitar las investigaciones en caso de producirse incidentes de seguridad. La tabla siguiente muestra las decisiones de diseño que se han tomado en esta solución en lo que respecta al registro de RADIUS. Revise estos datos para establecer cuáles de ellas cumplen los requisitos de su entorno.

Tabla 5.4: Decisiones sobre el diseño del registro IAS

Decisiones sobre el diseño del registro IAS	Comentarios
El tamaño del registro de sucesos del sistema de la plantilla de directiva de grupo IAS, que se encuentra en la *guía de seguridad* de *Windows Server 2003*, ha aumentado respecto a los valores predeterminados para dar cabida a los sucesos de IAS.	Si decide no habilitar el registro de solicitudes de autenticación RADIUS, el registro de sucesos del sistema será el registro principal de los sucesos de seguridad de acceso a WLAN. Analice detenidamente los parámetros, como la configuración predeterminada **Sobrescribir sucesos cuando sea necesario**, ya que esto permite que los datos de auditoría puedan sobrescribirse cuando el registro haya alcanzado el máximo de capacidad.
Se ha habilitado el registro de solicitudes de autenticación y contabilidad RADIUS en archivos de texto.	Esta decisión introduce los requisitos de carga de la CPU y de espacio en disco en los servidores IAS. Si no es posible realizar el registro, IAS dejará de aceptar las solicitudes de autenticación y contabilidad. Por lo tanto, debe prestarse especial atención a los posibles ataques de denegación de servicio (DoS) basados en el llenado del disco del archivo de registro.
Las especificaciones de hardware del servidor IAS que contiene esta guía incluyen un volumen de disco del archivo de registro independiente en discos físicos diferentes.	Con esta decisión se garantiza que el rendimiento de escritura de los archivos de registro de solicitudes RADIUS tenga el mínimo impacto de rendimiento en la administración de acceso a la red RADIUS. También se garantiza que los sucesos causantes de que el registro llene un volumen de disco no afecten a la capacidad de recuperación del servidor.
Se han seleccionado los elementos de autenticación y contabilidad RADIUS, pero no se ha seleccionado el estado periódico.	Esta decisión se ha tomado para garantizar que sólo se registre la información esencial necesaria para determinar el estado de autenticación y la duración de la sesión. Los estados periódicos se han ignorado para reducir los requisitos del archivo de registro. Considere la habilitación del registro de estado periódico si el registro de la duración de sesiones de usuario es importante en su entorno.
Se ha elegido el formato de base de datos compatible con conectividad abierta de bases de datos (ODBC, Open Database Connectivity) para los archivos de registro de autenticación y conectividad RADIUS.	Esta decisión facilita a los administradores la importación de archivos de registro a bases de datos compatibles con ODBC que facilitan el análisis; se suele considerar una práctica recomendable. Asimismo, es posible utilizar IASPARSE.EXE en las herramientas de asistencia de Windows Server 2003 para explorar los archivos.
El intervalo para la creación de nuevos archivos de registro se ha establecido en **mensualmente**.	La selección de un intervalo que genere menos archivos de registro facilita la importación de dichos archivos a las bases de datos o su exploración con IASPARSE.EXE cuando no se utiliza el registro de SQL Server. Esta opción debe sopesarse frente al riesgo de llenar un disco duro con un único archivo de registro.
El registro de solicitudes RADIUS se ha configurado para eliminar el archivo de registro más antiguo cuando el disco esté lleno.	El riesgo de esta configuración (predeterminada) consiste en que la información de seguridad puede perderse si un disco se llena de archivos de registro. Se ha elegido esta configuración para evitar que los servidores IAS se detengan en caso de llenarse el

	archivo de registro. Si la conservación de los archivos de seguridad es más importante que la disponibilidad del servicio, es recomendable deshabilitar esta función.

Selección de servidores centralizados o distribuidos

La decisión de utilizar servidores IAS centralizados o distribuidos se basa, en parte, en la distribución geográfica de su organización y en la estrategia de implementación de la infraestructura de TI correspondiente. Debe analizar cuál de los tres tipos de estrategia de infraestructura de TI se aproxima más al de su organización:

- infraestructura de TI centralizada.
- infraestructura de TI distribuida.
- infraestructura de TI mixta.

Las organizaciones de TI modernas procuran ofrecer una cantidad menor de componentes de infraestructura de TI, que sean más resistentes a los errores y estén más centralizados. Para conseguir este objetivo se requiere una gran inversión en infraestructura WAN de alta velocidad y resistente a errores, que garantice que los usuarios de las sucursales reciban el mismo nivel de servicio de TI que los usuarios de las oficinas centrales. Una ventaja de esta estrategia es que el costo de la infraestructura de servidores distribuidos puede redirigirse a la infraestructura y al ancho de banda de la red. Además, la infraestructura de servidores se encuentra más próxima al personal capacitado de los departamentos de ingeniería y operaciones del centro de datos, de forma que puede lograrse una mayor disponibilidad.

La centralización de los servidores IAS en organizaciones que disponen de WAN resistentes y de alta velocidad puede contribuir considerablemente a reducir el costo de la solución WLAN 802.1X. Este tipo de estrategia de infraestructura de TI debería considerarse como el punto de partida de un diseño de servidor RADIUS para organizaciones empresariales. El protocolo RADIUS no utiliza demasiado ancho de banda y funciona correctamente en vínculos WAN. También debería considerar la posibilidad de utilizar protocolos como el protocolo de configuración dinámica de host (DHCP, Dynamic Host Configuration Protocol), que pueden exceder el tiempo de espera de la autenticación de 802.1X. Adicionalmente, es fundamental disponer de una conexión de alto rendimiento entre los servidores IAS y los controladores de dominio que contengan los usuarios y grupos utilizados para determinar el acceso a la red. Muchos de los problemas potenciales de las redes 802.1X se pueden evitar garantizando comunicaciones de alta velocidad entre los servidores IAS y Active Directory.

Para muchas organizaciones de TI, el costo del ancho de banda, del sofisticado equipo de red y de las conexiones WAN redundantes resulta prohibitivo en lo que respecta a la utilización de un modelo de infraestructura de TI centralizada. Dichas organizaciones eligen un modelo de infraestructura de TI descentralizada con una infraestructura de servidores distribuida a las sucursales. Este modelo garantiza la continuidad del servicio TI en caso de error de la WAN.

Existe un tercer tipo de estrategia de infraestructura de TI en el que las organizaciones eligen una infraestructura de TI centralizada cuando es posible, y una infraestructura de TI distribuida cuando es necesario. Dicha estrategia permite la agrupación de la mayor parte de la infraestructura de TI en ubicaciones de concentradores, para atender tanto a los usuarios que se encuentran en la ubicación del concentrador como a los usuarios de pequeñas oficinas conectadas al mismo. Al mismo tiempo, este modelo permite la distribución de la infraestructura de servidores a sucursales con un mayor número de usuarios finales. El diagrama siguiente muestra un ejemplo de este tipo de organización.

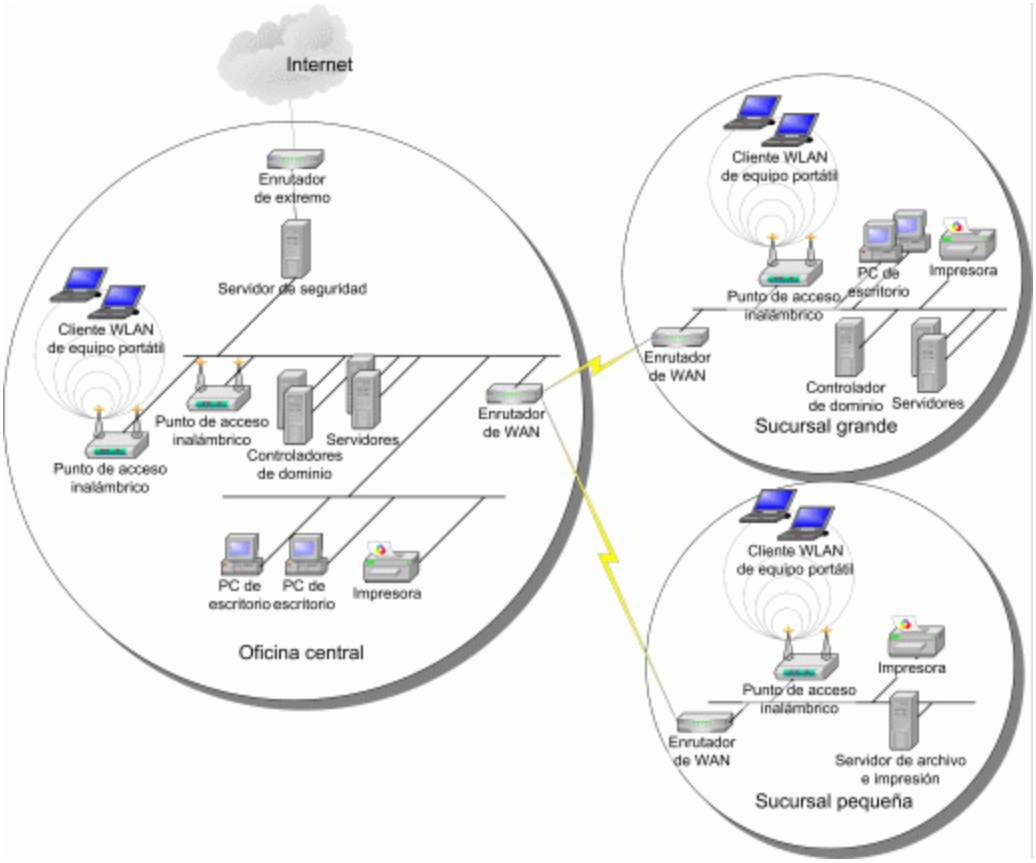

Figura 5.5 Organización con infraestructura de TI mixta, centralizada y distribuida
Ver imagen a tamaño completo

Esta solución se ha diseñado para dar cabida a modelos de implementación de infraestructura de servidores centralizada, descentralizada y mixta mediante la provisión de lo siguiente:

- instrucciones para configurar grandes oficinas con concentradores con dos servidores RADIUS que pueden atender tanto a las solicitudes locales como a las solicitudes de oficinas que carecen de infraestructura de servidores.
- Instrucciones para configurar grandes sucursales con un servidor RADIUS de sucursal opcional.

  Nota: en sucursales que no cuentan con infraestructura de servidor, el acceso a WLAN depende de la disponibilidad de la WAN.

Determinación del número y la ubicación de los servidores

Cada bosque de Active Directory independiente debe tener como mínimo dos servidores IAS que actúen como servidores RADIUS para los usuarios y dispositivos del bosque. De esta forma se garantiza que las solicitudes de acceso a la red sigan atendiéndose en caso de que uno de los servidores RADIUS no esté disponible.

Las ubicaciones de las oficinas centrales con muchos usuarios son buenas candidatas para dos o más servidores RADIUS. Si se dispone de ancho de banda de alta velocidad entre múltiples ubicaciones de concentrador con servidores RADIUS, es posible configurar puntos de acceso inalámbricos para la conmutación por error a los servidores RADIUS que se encuentran en una WAN. Sin embargo, si tiene intenciones de utilizar servidores RADIUS en una WAN, compruebe si dispone de un vínculo de red adecuado entre los servidores RADIUS y los controladores de dominio de que dependen en su entorno. Asimismo, debe probar los valores de tiempo de espera en los puntos de acceso inalámbricos y en los equipos cliente, y realizar modificaciones según sea necesario. Finalmente, localice los servidores RADIUS en el dominio raíz del bosque para optimizar el funcionamiento del protocolo Kerberos.

Las sucursales que sean lo suficientemente grandes para garantizar controladores de dominio y que no tengan conexiones WAN resistentes en las ubicaciones de concentradores, son candidatas probables para un servidor RADIUS local. Si su organización no tiene resistencia WAN, debe comparar el costo inicial y continuo de un servidor IAS de sucursal con el costo que implica que los usuarios inalámbricos no tengan acceso a la red inalámbrica en caso de producirse un problema de WAN.

Determinación de la co-ubicación de IAS con otros servicios

La intensidad de las comunicaciones entre IAS y los controladores de dominio de Active Directory significa que puede conseguirse un incremento del nivel de rendimiento mediante la ejecución de IAS en el mismo servidor que sus controladores de dominio (esto evita problemas de latencia relacionados con la comunicación en la red). Sin embargo, debe analizar detenidamente las implicaciones que comporta la co-ubicación de IAS en controladores de dominio. En la tabla siguiente se detallan algunas de dichas consideraciones.

Tabla 5.5: Consideraciones sobre la co-ubicación de IAS y controladores de dominio

Ubicación de IAS	Ventajas	Inconvenientes
Co-ubicados en controladores de dominio	– Aumento del rendimiento de la autenticación y autorización de usuarios y equipos. – Requiere menos hardware de servidor.	– No hay separación entre los administradores de IAS y los administradores de dominio. – No existe una separación intrínseca entre errores y cuestiones de rendimiento de servicios co-ubicados.
Separación de los controladores de dominio	– No hay separación entre los administradores de IAS y los administradores de dominio. – La carga y el comportamiento de IAS no afecta al servicio de Active Directory.	Requiere hardware de servidor adicional

Los controladores de dominio de Active Directory constituyen una parte crítica de la infraestructura de TI que debe tratarse con sumo cuidado. Muchas organizaciones empresariales tienen una directiva de software o de servicios adicionales mínimos en los controladores de dominio que garantiza la máxima fiabilidad de la continuidad del servicio.

En muchas organizaciones empresariales, los administradores de RADIUS tienen funciones independientes de los administradores de Active Directory. IAS es un componente opcional de Windows, y no existe una separación intrínseca entre la administración de IAS y las tareas que llevan a cabo los administradores locales de Windows. Por este motivo, cuando IAS se instala en los controladores de dominio, los administradores de IAS son miembros del grupo de seguridad de administradores de dominio.

Esta solución requiere la versión Windows Server 2003 de IAS, de modo que necesita actualizar sus controladores de dominio a Windows Server 2003 (si aún no lo ha hecho). Debe tener en cuenta los siguientes requisitos previos antes de actualizar los controladores de dominio de Windows 2000 Server a Windows Server 2003.

Tabla 5.6: Requisitos previos de los controladores de dominio de Windows Server 2003

Asunto	Requisito previo	Comentarios
De forma predeterminada, los controladores de dominio de Windows Server 2003 requieren	Actualice todos los equipos cliente como mínimo al sistema operativo Microsoft Windows® 95	Acuda al *Centro de ayuda y soporte técnico* de *Windows Server* 2003 para más detalles a los que se hace

la firma y cifrado de bloque de mensajes del servidor (SMB, Server Message Block) o la firma de comunicaciones de canal seguro. Este requisito puede causar algunos problemas con versiones anteriores de clientes Windows.	con el cliente Active Directory o a Windows NT 4.0 con Service Pack 4 (SP4) o posterior.	referencia en la sección Información adicional incluida al final del capítulo.
Los controladores de dominio de Windows Server 2003 requieren la firma y el cifrado predeterminados de canal seguro. Este requisito puede afectar a la confianza de los dominios en servidores incluidos en dominios que ejecutan Windows NT 4.0 sin SP4.	Actualice todos los controladores de dominio del dominio heredado a Windows NT Server 4.0 con SP4 o posterior.	Acuda al *Centro de ayuda y soporte técnico* de *Windows Server* 2003 para más detalles a los que se hace referencia en la sección Información adicional incluida al final del capítulo.
Los controladores de dominio Windows Server 2003 requieren una preparación de los dominios y bosques de Active Directory previa a la instalación.	Prepare el nuevo bosque mediante la utilidad ADPrep antes de actualizar los controladores de dominio en su entorno a Windows Server 2003.	Esto no afecta al conjunto de atributos parciales (PAS, Partial Attribute Set) y, por lo tanto, no provoca una regeneración del servidor de catálogo global.

Esta solución se ha creado para permitir la co-ubicación de IAS y Active Directory en controladores de dominio si se desea. La solución se ha probado con IAS separado de los controladores de dominio Windows Server 2003 en las ubicaciones de concentradores, y se ha co-ubicado con controladores de dominio Windows Server 2003 en las sucursales.

Cálculo de la carga del servidor RADIUS

IAS funciona correctamente en hardware modesto del servidor y puede aumentar la escalabilidad mediante hardware adicional o bien disminuir la escalabilidad mediante grupos de servidores RADIUS. Sin embargo, es recomendable calcular por adelantado la carga que provocarán los clientes de LAN inalámbrica en el hardware del servidor IAS para evitar las restricciones de recursos del servidor que pueden afectar a la disponibilidad del servicio.

Un diseño óptimo debería incluir el número mínimo de servidores necesarios para la resistencia, dejando cabida para el futuro crecimiento. La posibilidad de ampliación es especialmente importante a la hora de seleccionar hardware de servidor para utilizarlo en un modelo de equilibrio de carga basado en puntos de acceso inalámbricos. Cuando se cambia del equilibrio de carga basado en puntos de acceso inalámbricos al equilibrio de carga basado en proxy RADIUS, el número de servidores necesarios puede pasar de dos a cinco (suponiendo que los servidores RADIUS existentes han alcanzado su máxima capacidad).

Las consideraciones sobre la carga de servidores IAS son:

- Número de usuarios y dispositivos que requieren autenticación y contabilidad.
- opciones de autenticación, como el tipo de protocolo de autenticación extensible (EAP, Extensible Authentication Protocol) y la frecuencia de reautenticación.
- Opciones de RADIUS como el registro y el seguimiento del software IAS.

Para calcular la carga del servidor IAS, es necesario calcular el número de usuarios y dispositivos que requieren acceso a WLAN. Algunas organizaciones limitan la utilización de LAN inalámbricas a una parte de sus usuarios (por ejemplo, ejecutivos), mientras que otras deciden ofrecer acceso a LAN inalámbrica a todos los usuarios. Independientemente de la estrategia que elija su organización, debe estimar el “peor” escenario posible en el

que el número total de usuarios y dispositivos habilitados para WLAN requieran la autenticación y autorización en un breve período de tiempo. De esta forma, se garantiza que el tamaño de los servidores IAS se adecuará para afrontar períodos de gran actividad, por ejemplo las horas punta de la oficina, y también para afrontar en un breve margen de tiempo una interrupción de la red.

Asimismo, las opciones de autenticación de WLAN tienen un gran efecto en la carga del servidor IAS. Los protocolos basados en certificados (como EAP-TPS) realizan una operación de clave pública intensiva de la CPU después del primer inicio de sesión pero, a partir de ahí, emplean una estrategia de credenciales en caché, una reconexión rápida, para cada inicio de sesión posterior hasta que finaliza la caché (ocho horas de forma predeterminada). Se puede producir una reautenticación completa cuando los clientes inalámbricos pasan de la autenticación de un punto inalámbrico con un servidor IAS a la autenticación de un punto inalámbrico con un servidor IAS diferente (por ejemplo, cuando el cliente cambia de ubicación en un edificio). Esta reautenticación itinerante sólo se produce una vez entre cada cliente y servidor IAS y es transparente para el usuario final cuando se utiliza EAP-TLS.

Asimismo, los clientes inalámbricos pueden verse forzados a reautenticarse en los servidores RADIUS, como una forma de renovar las claves de cifrado de sesión WEP 802.11. Algunos modelos de puntos de acceso inalámbricos incluyen características que realizan la renovación de las claves de sesión WEP programadas, sin necesidad de forzar a los clientes a realizar una reautenticación frecuente con el servidor RADIUS a intervalos programados. Este tipo de característica es específica de los fabricantes. Asimismo, el estándar de acceso protegido Wi-Fi (WPA, WiFi Protected Access) incluye características de cifrado y administración de claves mejoradas que pueden mitigar la necesidad de reautenticación frecuente de las claves de sesión.

Por lo tanto, al crear un modelo para el número de autenticaciones que atenderá cada servidor IAS, debe considerar los diferentes tipos de autenticación que muestra la tabla siguiente.

Tabla 5.7: Tipos de autenticación de EAP-TLS

Tipo de autenticación	Comentarios
Autenticación inicial del equipo	El cliente realiza una autenticación completa con IAS.
Autenticación inicial del usuario	El cliente realiza una autenticación completa con IAS.
Reautenticación del usuario al desplazarse entre puntos de acceso inalámbricos	El cliente realiza una autenticación completa una vez con cada servidor IAS y, más adelante, utiliza la reconexión rápida para las autenticaciones adicionales.
Reautenticación del dispositivo al desplazarse entre puntos de acceso inalámbricos	El cliente realiza una autenticación completa una vez con cada servidor IAS y, más adelante, utiliza la reconexión rápida para las autenticaciones adicionales.
Reautenticación programada del equipo	El cliente utiliza una autenticación almacenada en caché con IAS.
Reautenticación programada del usuario	El cliente utiliza una autenticación almacenada en caché con IAS.

Los cálculos del número de autenticaciones que IAS puede atender se representan mejor como autenticaciones por segundo. IAS puede conseguir las cifras siguientes en un equipo que ejecute Windows Server 2003 con Active Directory que utilice una CPU Intel Pentium de 4,2 GHz.

Importante: la información de la tabla siguiente se proporciona sin garantías de ningún tipo y sólo debe utilizarse a modo de orientación con fines de planeamiento de la capacidad y no para realizar comparaciones de rendimiento.

Tabla 5.8: Autenticaciones por segundo

Tipo de autenticación	Autenticaciones por segundo
Nuevas autenticaciones de EAP-TLS	36
Nuevas autenticaciones de EAP-TLS con compatibilidad para tarjetas de descarga	50
Autenticaciones con reconexión rápida	166

IAS puede configurarse para generar registros de texto basados en disco que contengan diversos volúmenes de información de solicitud RADIUS. Debido a la carga que los registros de RADIUS imponen en los servidores, necesitará utilizar un disco de alto rendimiento para almacenarlos. Los subsistemas de disco lentos pueden retrasar las respuestas de RADIUS IAS a los puntos de acceso inalámbricos, provocando tiempos de espera de protocolos y la conmutación por error innecesaria de los puntos de acceso inalámbricos a servidores RADIUS secundarios.

Adicionalmente, la habilitación de las características de seguimiento de software de Windows Server 2003 aplicará una carga adicional en los servidores IAS. No obstante, esto puede ser necesario de forma ocasional para solucionar problemas de acceso a la red. Por lo tanto, los servidores IAS deben tener la capacidad de ejecutarse con el seguimiento habilitado durante períodos de tiempo limitados y seguir atendiendo a la vez la carga de producción.

Estimación de los requisitos de hardware del servidor

Debe seleccionar el hardware del servidor para IAS en la lista de compatibilidad de hardware (HCL, Hardware Compatibility List) de Windows Server 2003. La selección de hardware del servidor en la HCL de Windows Server 2003 ayuda a evitar problemas de fiabilidad y compatibilidad que pueden surgir con el hardware y los controladores de dispositivos no probados.

Asegúrese de que sus servidores IAS cumplen los requisitos de hardware recomendados para Windows Server 2003. Deben tenerse en cuenta otros servicios que puedan estar ejecutándose también en el sistema, como Active Directory. Considere la posibilidad de utilizar hardware de servidor IAS que pueda modificar para doblar la carga de autenticación prevista por servidor. De este modo podrá asegurarse de que se encuentran disponibles los recursos del servidor apropiados para manejar los escenarios de conmutación por error del servidor y las condiciones de red inusuales.

El diagrama siguiente se basa en la estructura de servidores de Woodgrove Bank, una organización ficticia, y muestra un ejemplo de diseño de servidor RADIUS basado en IAS. La figura muestra la ubicación y el número de servidores IAS en función de la distribución de la carga y los usuarios previstos. Sin embargo, solamente se probó un subconjunto de la infraestructura para la guía (utilizando el concentrador de Londres y las oficinas regionales de Johannesburgo).

Nota: Woodgrove Bank es una compañía ficticia representativa de organizaciones medianas y grandes. La arquitectura y las características de su red se han utilizado como base para diversas decisiones sobre el diseño en la implementación de esta solución.

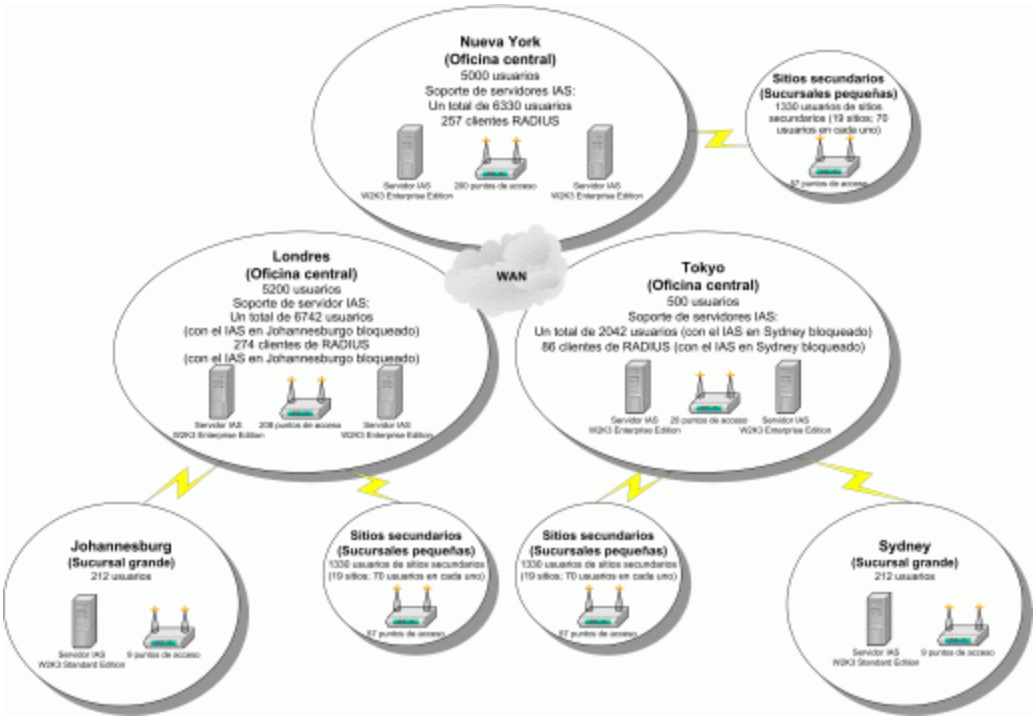

Figura 5.6 Usuario, punto de acceso inalámbrico y distribución de servidores IAS en Woodgrove Bank
Ver imagen a tamaño completo

Esta solución se ha diseñado con dos servidores RADIUS situados en una oficina central que atendía a 6742 usuarios. Sólo la mitad de los usuarios admitían el sistema inalámbrico; por lo tanto, 3371 usuarios y los 3371 dispositivos asignados correspondientes se autentican mediante EAP-TLS en los dos servidores RADIUS durante la carga pico. El tamaño de cada servidor puede ajustarse para atender a 3371 difusiones de autenticación en un período de inicio de sesión pico de 30 minutos. Este período de inicio de sesión pico equivale aproximadamente a dos nuevas autenticaciones EAP-TLS por segundo, con capacidad para cuatro nuevas autenticaciones por segundo durante la conmutación por error del servidor.

El servidor se configuró para registrar solicitudes de autenticación y contabilidad RADIUS en archivos de texto. Este servidor era un servidor RADIUS dedicado; los servicios de controlador de dominio estaban ubicados en otros servidores. De forma intencionada, se integró un exceso de capacidad en la especificación del hardware de servidor RADIUS para acomodar posibles requisitos futuros de control de acceso red para aplicaciones como VPN, redes por cable y acceso telefónico.

La tabla siguiente muestra el hardware de servidores IAS utilizado durante la prueba de esta solución.

Tabla 5.9: Hardware del servidor probado

Recurso	Configuración
CPU	Pentium III con CPU dual a 850 MHz
RAM	512 MB (megabytes)
Tarjeta de interfaz de red (NIC)	Dos NIC equipadas para resistencia
Disco duro	– Dos unidades de disco duro de 9 GB en una configuración RAID 1 (volumen C) para el sistema operativo. – Dos unidades de disco duro de 18 GB en una configuración RAID 1 (volumen D) para archivos de registro y datos de configuración.

Es probable que los requisitos de hardware de sus servidores IAS sean ligeramente distintos. Analice sus requisitos según las variables específicas de su organización.

Determinación de los requisitos de software del servidor

Debe determinar si los servidores IAS de su entorno requieren la versión Standard Edition o Enterprise Edition de Windows Server 2003. La versión Standard Edition de Windows Server 2003 está limitada para admitir 50 clientes RADIUS (puntos de acceso inalámbricos, por ejemplo) y dos grupos de enrutamiento de servidores.

Esta solución se ha probado con Windows Server 2003 Enterprise Edition para los servidores RADIUS situados en la oficina central y Windows Server 2003 Standard Edition para los servidores RADIUS ubicados en la sucursal. No obstante, la solución funcionará igualmente con cualquier versión, sujeta a las limitaciones mencionadas de cada una de ellas.

Su entorno requerirá otros componentes de software en función de los estándares de su organización, por ejemplo:

- Agentes de copia de seguridad.
- Agentes de administración tales como los componentes de cliente MOM o Microsoft Systems Management Server (SMS).
- Software antivirus.
- Agentes de detección de intrusos.

Principio de la página

Creación de un plan de administración

Los servidores RADIUS basados en IAS requieren poco mantenimiento continuo para garantizar la disponibilidad continua del servicio y la seguridad de la red. No obstante, debe determinar su estrategia de administración de IAS al principio de su proyecto de WLAN, de modo que pueda formar y equipar al personal adecuado para administrar la infraestructura de RADIUS.

Administración de los cambios y la configuración

El mantenimiento de un estado conocido en los servidores IAS es fundamental a la hora de garantizar la disponibilidad del servicio y la seguridad de la red. IAS facilita de forma nativa los cambios transaccionales en diversos elementos de configuración del servidor mediante el comando **netsh** y, por lo tanto, facilita la restauración en caso de que un cambio origine un comportamiento imprevisto.

Puede utilizar el comando **netsh** para exportar e importar parte de la configuración de IAS a archivos de texto. Puede usar estos archivos para replicar la configuración entre los servidores IAS, lo que permite acelerar la implementación de cambios de configuración en entornos amplios.

Las tareas necesarias para administrar correctamente los cambios y la configuración se enumeran en el capítulo 12, Administración de la infraestructura de seguridad de RADIUS y LAN inalámbrica.

Planeamiento de la recuperación de servicios

La garantía de una rápida recuperación del servicio RADIUS en caso de desastre conlleva un proceso de planeamiento meticuloso antes de producirse el evento. Puede simplificar la instalación y la configuración de IAS mediante el uso de secuencias de comandos de instalación proporcionadas con esta guía y es muy fácil automatizar los pasos requeridos para restaurar rápidamente el estado de configuración de IAS por medio de secuencias de comandos **netsh**. Para obtener más detalles sobre tareas de recuperación, consulte el capítulo 12, Administración de la infraestructura de seguridad de RADIUS y LAN inalámbrica.

Planeamiento de permisos administrativos

IAS es un componente opcional del sistema operativo Windows Server 2003 y, por lo tanto, no requiere un modelo de seguridad administrativo independiente del modelo del servidor local. La separación total entre la

administración de IAS y los administradores del servidor local no es posible. Puede conseguirse cierta separación sin una programación personalizada, como la creación de una aplicación Web segura que permita realizar cambios de configuración de IAS mediante una cuenta con permisos administrativos de servidor local.

Sin embargo, sigue siendo importante planear los tipos de administración necesarios y los requisitos de acceso a diversos recursos IAS para lograr un modelo de privilegios mínimos. La tabla siguiente muestra ejemplos de las funciones y tareas relacionadas con los servidores IAS.

Tabla 5.10: Descripciones y tareas de las funciones de IAS

Función del personal	Descripción de la función	Tareas
Administradores de IAS	Función necesaria para realizar las tareas de administración diarias de IAS, como el control del servicio y la configuración de IAS.	Iniciar, detener, consultar, configurar el servicio IAS y realizar modificaciones en la base de datos de configuración de IAS.
Auditores de seguridad IAS	Función necesaria para permitir el acceso a la información de seguridad a los auditores de seguridad que no disponen de permisos administrativos.	Revisar los archivos de registro de contabilidad y autenticación RADIUS de los sucesos de seguridad. Cuando los registros de solicitudes de autenticación RADIUS están deshabilitados, los auditores de seguridad IAS quizás necesiten revisar y guardar las entradas del registro de sucesos del sistema correspondientes a los sucesos de seguridad relacionados con IAS. Esto puede requerir permisos adicionales.
Operadores de copia de seguridad de IAS	Esta función permite a los operadores responsables realizar copias de seguridad periódicas de los servidores IAS. Las copias de seguridad incluyen el estado de configuración y los datos históricos de IAS.	Administrar las copias de seguridad diarias/semanales/mensuales de los servidores IAS.
Personal del servicio de asistencia de WLAN	Personal responsable de ayudar a los usuarios a resolver problemas relacionados con el acceso a la LAN inalámbrica.	Revisar los sucesos IAS del registro de sucesos del sistema relacionados con la autenticación de usuarios y dispositivos o ver los sucesos según se replican en otro sistema.

La tabla siguiente muestra los permisos de recursos necesarios para realizar las diferentes tareas del servidor IAS.

Tabla 5.11: Permisos necesarios para las tareas del servidor IAS

Tarea	Pertenencia al grupo	Permiso o derechos necesarios
Detener/iniciar/consultar/configurar el servicio IAS	El grupo global de administradores de IAS de Active Directory, que se encuentra dentro del	Puede modificar los permisos de servicio de Windows Server 2003 mediante el comando SC. Consulte al personal de asistencia técnica de Microsoft antes de modificar los permisos predeterminados de los componentes del

	grupo de administradores local en los servidores IAS.	sistema operativo.
Modificar la configuración de IAS	El grupo global de administradores de IAS, que se encuentra dentro del grupo de administradores local en los servidores IAS.	Se requieren permisos en los archivos de la base de datos de IAS incluidos en el directorio C:\WINDOWS\system32\ias, así como en diversas claves de registro en **HKLM\System\CurrentControlSet\Services**. Estos permisos se conceden de forma predeterminada a los miembros del grupo de seguridad de administradores integrado/local.
Acceso a los registros de peticiones RADIUS que se encuentran en los servidores IAS	Grupo global de dominio de auditores de seguridad IAS.	Los auditores de IAS deben ser capaces de leer y eliminar los archivos del registro de peticiones RADIUS que se encuentran en el directorio D:\IASLogs. Al aplicar las instrucciones de generación de esta solución se concede el permiso de cambiar NSFS al grupo de seguridad de auditores de seguridad IAS de este directorio y se crea un recurso compartido denominado IASLogs con el permiso compartido de cambiar concedido al grupo de seguridad de auditores de seguridad IAS.
Leer y guardar sucesos de seguridad de IAS en el registro de sucesos del sistema	Administradores locales – O bien – Operadores de copia de seguridad en servidores IAS.	Esta solución ofrece instrucciones para habilitar el registro de autenticación RADIUS en los archivos de texto del disco. Por lo tanto, los auditores de IAS generalmente no necesitan tener acceso a los Registros de sucesos del sistema IAS correspondientes a los sucesos de seguridad de autenticación RADIUS. Sin embargo, si decide deshabilitar el registro de autenticación RADIUS, los Auditores de seguridad IAS deberán ser capaces de leer y guardar los eventos IAS del registro de sucesos del sistema. El archivo de los registros de sucesos del sistema requiere la pertenencia al grupo Administrador u Operadores de copia seguridad.
Realizar las copias de seguridad diarias/semanales/mensuales de los servidores IAS.	Operadores de copia de seguridad en servidores IAS.	La copia de seguridad de IAS incluye el estado de configuración y los datos históricos de IAS, como los registros de solicitudes RADIUS. La pertenencia al grupo de operadores de copia de seguridad permite el acceso a los archivos de la base de datos de IAS que se encuentran en el directorio %systemroot%\system32\ias, a las diversas claves de registro de **HKLM\System\CurrentControlSet\Services**, a los archivos de registro de solicitudes RADIUS de D:\IASLogs y a los archivos de texto de configuración de IAS **NETSH** que se encuentran en D:\IASConfig.
Revisar los sucesos de	Pertenencia al grupo	Se debe conceder permiso de lectura al personal

autenticación IAS en el registro de sucesos del sistema para la solución de problemas	con permisos de lectura en el registro de sucesos del sistema.	senior encargado de la solución de problemas en el registro de sucesos de Windows Server 2003 para ver e interpretar los sucesos de rechazo de autenticación IAS.

Supervisión y auditoría de seguridad

IAS es un componente de la infraestructura de seguridad y debe supervisarse de forma preventiva. La investigación del sector de seguridad ha demostrado que los ataques que logran su objetivo suelen ir precedidos de diversos ataques fallidos. Para saber cuándo está siendo atacada la red, es necesaria una supervisión de la seguridad de forma preventiva de los servidores IAS y de los correspondientes registros relacionados, para detectar un posible comportamiento sospechoso.

La tabla siguiente enumera las posibles amenazas a las que está expuesta una infraestructura de servidor IAS y que deben supervisarse de forma preventiva.

Tabla 5.12: Amenazas de la infraestructura de servidor IAS

Amenaza/Vulnerabilidad	Síntoma	Herramienta de supervisión
Intento de autorización con credenciales robadas (como las que se encuentran en un equipo portátil perdido o robado).	Los sucesos de éxito/rechazo de autenticación (origen: IAS, ID 1 y 2) del registro de sucesos del sistema o de los registros de solicitudes de autenticación RADIUS indican el uso de certificados revocados.	– MOM con una secuencia de comandos personalizada escrita para analizar las entradas del registro de sucesos para el uso de certificados revocados. – Secuencias de comandos de análisis de archivos o herramientas de SQL Server que buscan la utilización de certificados revocados.
Intento de realizar un ataque de tipo "man in the middle" mediante un punto de acceso inalámbrico falso	Contadores del monitor del sistema en un servidor IAS que muestre una cantidad excesiva de las siguientes situaciones: autenticadores incorrectos (atributo autenticador de mensajes incorrecto) o solicitudes no válidas (recibidas de clientes o servidores RADIUS desconocidos).	MOM con una secuencia de comandos personalizada para detectar los contadores del monitor del sistema y mostrar una alerta.
Intento de DoS o de desbordamiento de búfer en el servicio del servidor IAS	Contadores del monitor del sistema en un servidor IAS que muestre una cantidad excesiva de las siguientes situaciones: paquetes formados incorrectamente (paquetes que contienen datos incorrectos), tipo desconocido (se han recibido paquetes que no son RADIUS) o paquetes perdidos (paquetes perdidos que no son MAC erróneos/incorrectos/desconocidos)	MOM con una secuencia de comandos personalizada para detectar los contadores del monitor del sistema y mostrar una alerta.
Intento de autenticación no autorizada	Sucesos repetidos de error de autenticación (origen: IAS, ID 2) en el registro de sucesos del sistema.	– Secuencia de comandos de MOM personalizada para analizar las entradas del registro de sucesos para patrones de rechazos de autenticación excesivos. – Secuencias de comandos de análisis de archivos o SQL Server que identifiquen

		los patrones de rechazos de autenticación excesivos.
Autenticación no autorizada satisfactoria mediante credenciales robadas	Los registros de cuentas RADIUS indican una actividad de red sospechosa.	– Microsoft Access para importar registros y realizar consultas personalizadas. – Informes que identifican la información de acceso a la red inesperado en una base de datos de SQL Server.

Además de la supervisión básica de la seguridad, Microsoft recomienda la auditoría de seguridad periódica de los servidores IAS y el uso de sistemas de supervisión para definir claramente y mitigar las vulnerabilidades que puedan descubrirse en la infraestructura de red.

La tabla siguiente enumera las posibles amenazas a las que se expone la infraestructura del servidor IAS y las tecnologías relacionadas que se pueden utilizar para realizar una auditoría de seguridad preventiva.

Tabla 5.13: Amenazas de la infraestructura del servidor IAS que se auditarán de forma preventiva

Amenaza/Vulnerabilidad	Síntoma	Herramienta de auditoría
Permiso débil en los datos históricos y en la configuración de IAS	Miembro no autorizado de: los grupos de administradores de IAS, auditores de seguridad IAS o administradores locales.	Active Directory y herramientas de auditoría del grupo de seguridad local, como DumpSec de SomarSoft.
Intento de ocultar la autenticación no autorizada.	El registro de sucesos del sistema se ha limpiado de forma imprevista.	– Auditoría del registro de sucesos de Windows mediante herramientas como EventcombMT, del *kit de recursos* de *Windows Server 2003*. – Herramienta de supervisión y alerta del registro de sucesos como MOM.
Modificación no autorizada de los registros de autenticación y contabilidad RADIUS.	Un Id. de usuario imprevisto ha conseguido escribir en los registros de auditoría de carpetas.	Auditoría de archivos de Windows y una herramienta de supervisión como MOM. Para detectar la modificación de archivos no autorizada, debe habilitar la auditoría de archivos.

Principio de la página

Resumen

Este capítulo ha descrito el proceso de diseño de una infraestructura de RADIUS que admita redes inalámbricas seguras basadas en 802.1X. El diseño presentado en este capítulo es lo suficientemente flexible como para adaptarse a una amplia gama de requisitos futuros. Adicionalmente, puede utilizar el diseño de la infraestructura para otros tipos de administración del acceso a la red.

El diseño descrito en este capítulo se utilizará en capítulos posteriores para implementar la infraestructura de RADIUS. El capítulo siguiente se ocupa del diseño genérico de RADIUS para describir la configuración de 802.1X y la infraestructura de WLAN requeridas a la hora de implementar el resto de los componentes de la infraestructura de seguridad de WLAN.

Información adicional

Si desea obtener más información acerca de IAS, consulte los recursos siguientes:

- El sitio Web del Centro de soporte técnico de Windows Server 2003 en http://www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/default.mspx.
- La documentación del producto ofrece una descripción general de las características de IAS, instrucciones básicas de configuración y las mejores prácticas de implementación.
- La *guía de referencia técnica de Microsoft Windows Server 2003* y el *kit de implementación de Microsoft Windows Server 2003* en http://www.microsoft.com/windows/reskits/default.asp.
- El capítulo "IAS Technical Reference" de la *guía de referencia técnica* de *Microsoft Windows Server* 2003 en http://www.microsoft.com/resources/documentation/windowsServ/2003/all/techref/en-us/W2K3TR_ias_intro.asp.
- Este capítulo de referencia técnica proporciona información sobre IAS más detallada que la documentación del producto y puede utilizarse como referencia en caso de necesitar información adicional.
- El capítulo "Deploying IAS" de la guía *Deploying Network Services*, sobre implementación de servicios de red, del *kit de implementación de Microsoft Windows Server 2003* en http://www.microsoft.com/windowsserver2003/techinfo/reskit/deploykit.mspx.
- Este capítulo del kit de implementación contiene instrucciones para el uso de IAS en distintos escenarios que quedan fuera del alcance de esta guía sobre seguridad de redes inalámbricas pero que afectan a las decisiones sobre diseño.

Para obtener más información sobre las tecnologías WLAN 802.1X, consulte:

- Las notas del producto "Windows XP Wireless Deployment Technology and Component Overview", que ofrecen una descripción general de los componentes y la tecnología de implementación inalámbrica en Windows XP, incluidas en Microsoft TechNet en http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx.

Principio de la página

Administre su perfil