Latinoamérica

Microsoft TechNet

Capítulo 11: Administración de la infraestructura de claves públicas

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

En esta página

Introducción

En este módulo se describen los procedimientos operativos requeridos para administrar la infraestructura de claves públicas (PKI, Public Key Infrastructure) implementada como parte de esta solución *Seguridad en LAN inalámbricas*. La estructura está basada en las categorías y conceptos de Microsoft Operations Framework (MOF) tratados en el primer módulo de la Guía de operaciones (capítulo 10).

La finalidad de este capítulo es permitirle implementar un sistema de administración completo para su PKI. Esto incluye todas las tareas de instalación necesarias para empezar a supervisar y mantener el sistema y las tareas operativas normales necesarias para su funcionamiento correcto. También se tratan los procedimientos de ayuda para solucionar los incidentes de compatibilidad, administrar los cambios del entorno y optimizar el rendimiento del sistema.

Este capítulo se divide en dos partes principales. La primera parte consta de dos secciones, "Tareas de mantenimiento esenciales" y "Asignación de funciones administrativas", que son breves y se deben leer en su totalidad. En estas secciones se proporciona información esencial acerca de la configuración de un entorno administrado correctamente para el sistema. El resto del capítulo es fundamentalmente una referencia. A continuación se ofrecen algunas tareas de la secciones de referencia que tendrá que implementar cuando implemente el sistema, pero se indican de forma clara en la sección "Tareas de mantenimiento esenciales".

Aunque no es necesario que se detenga en todos los detalles de la sección de referencia, revísela para familiarizarse con el contenido de modo que pueda encontrar rápidamente los elementos que necesite en el futuro.

Requisitos previos

Debe estar familiarizado con los conceptos empleados en MOF según lo descrito en el capítulo 10, "Introducción a la guía de operaciones". No es preciso un conocimiento detallado de MOF.

También debe estar familiarizado con los conceptos de PKI y Servicios de Certificate Server de Microsoft® en concreto. También se precisan conocimientos de Microsoft Windows® 2000 Server (o posterior) en las siguientes áreas:

- Operaciones básicas y mantenimiento de Microsoft Windows Server™ 2003, incluido el uso de herramientas como Visor de sucesos, Administración de equipos y NTBackup.
- El servicio de directorio de Active Directory®, incluidas la estructura y las herramientas de Active Directory, la

manipulación de usuarios, grupos y otros objetos de Active Directory, así como el uso de Directiva de grupo.

- Seguridad del sistema de Windows: conceptos de seguridad como usuarios, grupos, auditoría, listas de control de acceso, uso de plantillas de seguridad y aplicación de plantillas de seguridad mediante Directiva de grupo o herramientas de la línea de comandos.
- Administración de Servicios de Internet Information Server (IIS).
- Los conocimientos de Windows Scripting Host y del lenguaje Microsoft Visual Basic® Scripting Editing (VBScript) le resultarán útiles para obtener el máximo provecho de las secuencias de comandos suministradas, pero no es esencial.

Antes de continuar con este capítulo, debe leer los capítulos relacionados de la guía de planeamiento y de la guía de generación (capítulos 4 y 6), así como disponer de un conocimiento exhaustivo de la arquitectura y el diseño de la solución.

Descripción general del capítulo

En la siguiente lista se describen las principales secciones de este capítulo.

- **Tareas de mantenimiento esenciales.** Contiene dos tablas que enumeran las tareas necesarias para configurar el sistema de administración y la lista normal de tareas que se tienen que realizar para mantener el sistema.
- **Funciones administrativas**. Describe las funciones administrativas utilizadas en la solución, las capacidades de cada función y cómo estas funciones se asignan a clústeres de funciones de MOF y los grupos de seguridad administrativos definidos para la solución.
- **Tareas de cuadrante operativo**. Incluye todas las tareas relacionadas con el mantenimiento normal de la PKI. Estas tareas incluyen supervisión, copias de seguridad y operaciones de directorio y seguridad.
- **Tareas del cuadrante de compatibilidad**. Incluye todos los procedimientos relacionados con la recuperación de problemas del sistema. Estos procedimientos incluyen la revocación de certificados y entidades emisoras de certificados, restauración de copias de seguridad y operaciones para tratar con una entidad emisora con error.
- **Tareas del cuadrante de optimización**. Incluye algunos procedimientos de planeamiento de administración de capacidad.
- **Tareas del cuadrante de cambio**. Incluye tareas comunes relacionadas con la realización de cambios en la configuración de la entidad emisora y su puesta en producción de un modo controlado. También se incluyen los procedimientos que le servirán para recopilar y mantener información de configuración fundamental acerca de la PKI.
- **Solución de problemas**. Contiene procedimientos para ayudarle a solucionar problemas comunes que se pueden producir en la PKI. También incluye descripciones de herramientas útiles para solucionar problemas y procedimientos para habilitar el registro de distintos componentes.
- **Tablas de configuración.** Contiene un subconjunto de los parámetros de configuración empleados en la guía de generación. Estos valores se utilizan como ejemplo en el texto de los procedimientos.
- **Información adicional**. Enumera una serie de fuentes de información adicionales a las que se hace referencia en el texto.

Principio de la página

Tareas de mantenimiento esenciales

En esta sección se enumeran las tareas importantes que debe realizar para utilizar la PKI con éxito. Las tareas de configuración que se efectúan una vez y las tareas operativas continuadas se enumeran en dos tablas. Las tareas que aparecen en las tablas se describen con detalle más adelante en este documento. Las tareas se agrupan por cuadrante MOF y, junto a cada una de ellas, se indica la función de administración de servicio (SMF) de MOF a la que pertenece, lo que sirve de ayuda para encontrar la tarea necesaria con facilidad.

También se incluye en esta sección una lista de las herramientas y las tecnologías utilizadas en los procedimientos de este capítulo.

Tareas iniciales de configuración

En esta tabla se muestran las tareas que deben realizarse para colocar las operaciones de PKI en producción. Según los estándares y prácticas operativos de que disponga, es posible que no tenga que realizar todas estas tareas, pero debe revisarlas en detalle y decidir si son necesarias. Algunas de las tareas podrían tener que llevarse a cabo otra vez; por ejemplo, si se instala otra entidad emisora, tendrá que configurar sus trabajos de copia de seguridad y supervisión.

Tabla 11.1: Tareas iniciales de configuración

Nombre de tarea	Clúster de funciones	SMF
Cuadrante operativo		
Preparación de una estructura de unidad organizativa (UO) de dominio para la administración de Servicios de Certificate Server	Infraestructura	Administración de servicios de directorio
Publicación de las listas CRL de entidad emisora de certificados en el servidor Web	Seguridad	Administración de seguridad
Configuración de una copia de seguridad de la base de datos de entidad emisora	Infraestructura	Administración de almacenamiento
Configuración de la copia de seguridad de la base de datos de entidad emisora raíz	Infraestructura	Administración de almacenamiento
Prueba de copias de seguridad de la base de datos de entidad emisora de certificados	Operaciones	Administración de almacenamiento
Prueba de copias de seguridad de claves de entidad emisora de certificados	Operaciones	Administración de almacenamiento
División en categorías de las alertas de supervisión	Infraestructura	Supervisión y control de servicios
Supervisión de restricciones de capacidad de Servicios de Certificate Server	Infraestructura	Supervisión y control de servicios
Supervisión del estado y la disponibilidad de Servicios de Certificate Server	Infraestructura	Supervisión y control de servicios
Configuración de alertas de SMTP para solicitudes de certificados pendientes	Infraestructura	Supervisión y control de servicios
Programación de trabajos en una entidad emisora	Infraestructura	Programación de trabajos
Cuadrante de optimización		
Determinación de la carga máxima de la entidad emisora	Infraestructura	Administración de capacidad
Determinación de los requisitos de almacenamiento y copia de seguridad para una entidad emisora	Infraestructura	Administración de capacidad
Cuadrante de cambio		
Administración de actualizaciones del sistema operativo	Infraestructura	Administración de cambios Administración de versión

Si bien no hay una tarea documentada para configurar un sistema de administración de configuración para la PKI, revise los procedimientos de la sección "Administración de configuración". Estos procedimientos describen los tipos de información que deben recopilarse y mantenerse en un sistema de administración de configuración.

Tareas de mantenimiento

En esta tabla se muestran las tareas que deben realizarse regularmente para mantener el correcto funcionamiento de la PKI. Puede utilizar esta tabla para planear los recursos que necesitará y el programa operativo para la administración del sistema.

Es posible que algunas tareas no sean necesarias; sin embargo, debe revisar el detalle de las mismas para decidirlo. Algunas de estas tareas, además, posiblemente necesiten realizarse tanto puntualmente como de forma programada. Por ejemplo, si se renueva un certificado de una entidad emisora raíz, será necesario realizar una copia de seguridad de la entidad emisora raíz aunque la misma no se encuentre programada. Si fuera así, ésta se incluye en la columna Frecuencia. Las dependencias como éstas también se anotan automáticamente en los detalles de la tarea.

Tabla 11.2: Tareas de mantenimiento

Nombre de tarea	Frecuencia	SMF
Cuadrante operativo		
Comprobación de solicitudes pendientes	Diariamente	Administración de seguridad
Renovación del certificado de entidad emisora raíz	Cada ocho años	Administración de seguridad
Renovación del certificado de entidad emisora de certificados	Cada cuatro años	Administración de seguridad
Publicación de una lista CRL y un certificado de entidad emisora fuera de línea	Cada seis meses	Administración de seguridad
Copia de seguridad de claves y certificados de entidad emisora	Anualmente o cada vez que se renueve un certificado de entidad emisora (lo primero que se produzca)	Administración de almacenamiento
Prueba de copias de seguridad de la base de datos de entidad emisora de certificados	Mensualmente	Administración de almacenamiento
Prueba de copias de seguridad de claves de entidad emisora de certificados	Cada seis meses	Administración de almacenamiento
Archivado de los datos de auditoría de seguridad desde una entidad emisora de certificados	Mensualmente (CA emisora)	Administración de almacenamiento
Archivado de los datos de auditoría de seguridad desde una entidad emisora de certificados	Cada seis meses (entidad emisora raíz)	Administración de almacenamiento

Tecnología requerida en la Guía de operaciones

En la tabla siguiente se enumeran las herramientas o tecnologías utilizadas en los procedimientos descritos en este capítulo.

Tabla 11.3: Tecnología requerida

Nombre de elemento	Fuente
Usuarios y equipos de Active Directory de Management	Microsoft Windows Server 2003

Console (complemento MMC)	
Complemento Entidad emisora de certificados de MMC	Windows Server 2003
Complemento Plantilla de certificados de MMC	Windows Server 2003
Certutil.exe	Windows Server 2003
Certreq.exe	Windows Server 2003
Secuencias de comandos MSS	Esta solución
Editor de texto	Bloc de notas: Windows Server 2003
Servicio del programador de tareas de Windows	Windows Server 2003
SchTasks.exe	Windows Server 2003
Copia de seguridad de Windows	Windows Server 2003
Cipher.exe	Windows Server 2003
Visor de eventos	Windows Server 2003
Monitor del sistema	Windows Server 2003
Net.exe	Windows Server 2003
DSquery.exe	Windows Server 2003
Ldifde.exe	Windows Server 2003
DCDiag.exe	Windows Server 2003
Consola de alertas operativas	Microsoft Operations Manager (MOM)
Medios extraíbles para la creación de copias de seguridad de entidad emisora raíz	CD–RW o cinta
Copia de seguridad del servidor de entidad emisora	Servicio de copia de seguridad corporativa o dispositivo de copia de seguridad local
Complemento Directiva de grupo de MMC	Descarga Web desde Microsoft.com
Estado de PKI	Kit de recursos de Windows Server 2003

Tabla 11.4: Tecnología recomendada

Nombre de elemento	**Fuente**
Consola de alertas operativas	Microsoft Operations Manager u otro sistema de supervisión de servicios
Infraestructura de correo electrónico para alertas operativas (una alternativa para MOM)	Servidor y cliente de SMTP/POP3/IMAP, como Microsoft Exchange Server y Microsoft Outlook®
Eventquery.vbs	Windows Server 2003
Herramientas de planeamiento de capacidad	Microsoft Operations Manager u otras herramientas de planeamiento de capacidad
Sistema de distribución de actualizaciones de seguridad	Microsoft Systems Management Server o Servicios de actualización de software de Microsoft

Principio de la página

Funciones administrativas de Servicios de Certificate Server

En la administración de una PKI intervienen numerosas funciones distintas. Las dos secciones siguientes las dividen en funciones importantes y funciones auxiliares.

Funciones importantes de Servicios de Certificate Server

Las funciones importantes de Servicios de Certificate Server son fundamentales para la administración de una infraestructura de claves públicas. Muchas de estas funciones corresponden a las funciones de seguridad de criterios comunes (CC) definidas para Servicios de Certificate Server. Si éste es el caso, dicha condición se indica entre paréntesis a continuación del nombre de la función.

Tabla 11.5: Funciones de servicios de certificados principales

Nombre de la función	Ámbito	Descripción
Administrador de la PKI de la empresa	Empresa	Responsable general de la PKI: define los tipos de certificados, las directivas de aplicación, las rutas de confianza, etc. correspondientes a la empresa.
Publicador de la PKI de la empresa	Empresa	Responsable de publicar certificados raíz de confianza, certificados de subentidades emisoras de certificados y listas CRL en el directorio.
Administrador de entidad emisora (Función "Administrador" de CC)	Entidad emisora	Administrador de entidad emisora: responsable de la configuración de la entidad emisora y de la asignación de funciones de la misma. Generalmente se trata de las mismas personas que actúan como administradores de PKI de empresa. Es posible que existan diferentes administradores de entidad emisora a cargo de diferentes entidades emisoras si el uso del certificado así lo indica.
Administrador (Función "Administrador" de CC)	Entidad emisora	Administrador del sistema operativo del servidor de entidad emisora: responsable de la configuración en el nivel de servidor (como la instalación de la entidad emisora). Generalmente se trata de las mismas personas que actúan como administradores de entidad emisora. Es posible que existan diferentes administradores a cargo de diferentes entidades emisoras si el uso del certificado así lo indica.
Auditor de entidad emisora (Función "Auditor" de CC)	Entidad emisora	Administra los sucesos de auditoría, la directiva y tipos similares de sucesos que se pueden auditar de las entidades emisoras de certificados.
Administrador de certificados (Función "Oficial" de CC)	Entidad emisora	Aprueba solicitudes de certificado que requieren la aprobación manual y revoca certificados. Puede haber varios administradores de certificados a cargo de aprobaciones de diferentes entidades emisoras de certificados si el uso del certificado lo requiere.
Autoridad de registro	Perfil de certificado	Extensión de la función del administrador de certificados. Es responsable de aprobar y firmar las solicitudes de certificado siguiendo la comprobación de Id. del sujeto del certificado. Puede ser una persona, un proceso de TI o un dispositivo (por ejemplo, un escáner de huellas dactilares y base de datos)

		Se pueden especificar diferentes autoridades de registro para distintos perfiles de certificados (plantillas) y pueden abarcar múltiples entidades emisoras de certificados.
Agente de recuperación de claves	Entidad emisora	Contiene la clave para descifrar claves privadas archivadas en la base de datos de la entidad emisora de certificados.
Operador de copia de seguridad de la entidad emisora (Función "Operador" de CC)	Entidad emisora	Responsable de la copia de seguridad y recuperación de los servidores de entidad emisora y el almacenamiento seguro de los medios de copia de seguridad.

Funciones auxiliares de Servicios de Certificate Server

Las funciones operativas de la siguiente tabla no son esenciales para la administración de la infraestructura de claves públicas, pero sirven de apoyo a las funciones esenciales.

Tabla 11.6: Funciones auxiliares de Servicios de Certificate Server

Nombre de la función	Ámbito	Descripción
Operador de supervisión	Empresa	Responsable de la supervisión de sucesos.
Planeador de capacidad	Empresa	Responsable del análisis del rendimiento y la carga para predecir futuros requisitos de capacidad.
Administrador de Active Directory	Empresa	Responsable de la configuración y compatibilidad de la infraestructura de Active Directory.
Operaciones de Active Directory	Empresa	Responsable del mantenimiento diario del directorio, como el mantenimiento del grupo de seguridad, la creación de cuentas, etc.
Cambio de tarjeta de aprobaciones	Empresa	Se requieren representantes comerciales y técnicos para aprobar cambios en la infraestructura.

Asignación de funciones de Servicios de Certificate Server a grupos de seguridad

En la siguiente tabla se enumeran los grupos de seguridad definidos para esta solución y se describen brevemente las capacidades o permisos de cada uno.

Para entidades emisoras de certificados sin conexión, sólo hay grupos de seguridad locales. En este caso, debe crear cuentas locales individuales en la propia entidad emisora que se utilizan para asignar los grupos locales. Puede hacer que las cuentas individuales sean miembros de varios grupos de funciones locales (incluso de de todos) si esta configuración es compatible con las directivas de TI y la seguridad de la organización.

En las entidades emisoras de certificados en línea, los grupos de seguridad de dominio se utilizan para aplicar los permisos correspondientes a cada función. Las cuentas de dominio se utilizan para rellenar los grupos de funciones. Nuevamente, puede hacer que las cuentas individuales sean miembros de múltiples grupos de funciones locales si dicha configuración es compatible con las directivas de TI y seguridad de la organización.

Tabla 11.7: Asignación de funciones de Servicios de Certificate Server a grupos de seguridad

Nombre de la función	Grupo de seguridad del dominio (entidades emisoras en línea)	Grupo de seguridad local (entidades emisoras en línea)	Capacidades
Administrador de la PKI de la empresa	Administradores de PKI de empresa	–	Control sobre el contenedor de servicios de claves públicas de Active

			Directory. Por lo tanto, controla las plantillas, la publicación confiable y otros elementos de configuración de la empresa (bosque).
Publicador de la PKI de la empresa	Editores de PKI de empresa	–	Puede publicar certificados raíz de confianza de empresa, certificados de subentidades emisoras de certificados y listas CRL en el directorio.
Administrador de entidad emisora	Administradores de entidad emisora	Administradores de entidad emisora (sólo entidad emisora raíz)	Tiene permisos de "administración de la entidad emisora de certificados (CA)" en la entidad emisora. Controla la asignación de funciones en la entidad emisora. También tiene permisos para cambiar las propiedades de la entidad emisora. Se suele combinar con un administrador local en el servidor de entidad emisora, a menos que se imponga una separación de funciones.
Administrador		Administradores	Administrador local del servidor de entidad emisora.
Auditor de entidad emisora	Auditores de entidad emisora	Administradores de auditores de entidad emisora (sólo entidad emisora raíz)	Tiene derechos de usuario para la "administración de los registros de auditoría y seguridad" en una entidad emisora. Además es miembro del grupo Administradores local en la entidad emisora (condición obligatoria para obtener acceso a los registros de auditoría).
Administrador de certificados	Administradores de certificados	Administradores de certificados (sólo entidad emisora raíz)	Tiene permiso de "emisión y administración de certificados" en la entidad emisora. Es posible configurar varios administradores de certificados en cada entidad emisora y cada uno de ellos administra certificados de un subconjunto de usuarios u otras entidades finales.
Autoridad de registro	–	–	Contiene la clave y el certificado requeridos para firmar la solicitud de certificado antes de la aprobación.
Agente de recuperación de claves	–	–	Contiene la clave y el certificado requeridos para descifrar las claves privadas archivadas y guardadas en la base de datos de certificados.
Operador de copia de seguridad de la entidad emisora	Operadores de copia de seguridad de CA	Operadores de copia de seguridad de entidad emisora (sólo entidad emisora raíz)	Tiene derechos de "restauración y creación de copias de seguridad" en un servidor de entidad emisora.

Principio de la página

Tareas de cuadrante operativo

Esta sección contiene información más detallada acerca de las tareas de mantenimiento pertenecientes al cuadrante operativo MOF.

El cuadrante operativo de MOF incluye estándares, procesos y procedimientos operativos de TI que se aplican periódicamente a soluciones de servicio para alcanzar y mantener niveles de servicio predeterminados. El objetivo de este cuadrante consiste en la ejecución altamente previsible de tareas diarias manuales y automatizadas.

El cuadrante operativo contiene las siguientes SMF:

- Administración de servicios de directorio
- Administración de seguridad
- Administración de almacenamiento
- Supervisión y control de servicios
- Programación de trabajos

No hay tareas que correspondan al resto de las SMF:

- Administración del sistema
- Administración de la red
- Administración de impresión y resultados

Nota: cada descripción de tarea incluye la siguiente información de resumen: requisitos de seguridad, frecuencia y requisitos de tecnología.

Administración de servicios de directorio

Los servicios de directorio permiten a los usuarios y las aplicaciones localizar recursos de red como usuarios, servidores, aplicaciones, herramientas, servicios y otro tipo de información en la red. La administración de servicios de directorio se ocupa de las operaciones, las tareas de mantenimiento y la asistencia técnica diarias del directorio de la empresa. El objetivo de la administración de servicios de directorio consiste en garantizar que cualquier solicitante autorizado pueda obtener acceso a la información mediante un proceso simple y organizado.

Preparación de una estructura de unidad organizativa (UO) de dominio para la administración de Servicios de Certificate Server

La finalidad de esta tarea consiste en crear una estructura de unidad organizativa adecuada para administrar los grupos de seguridad y las cuentas de usuario de los Servicios de Certificate Server.

Información de resumen

- **Requisitos de seguridad:** cuenta con derechos para crear unidades organizativas en la parte designada de Active Directory
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**: complemento Usuarios y equipos de Active Directory de MMC

Detalles de la tarea

Esta tarea no es de carácter normativo puesto que depende principalmente de su estructura de unidad organizativa existente y de sus directivas y procedimientos de administración actuales. En la siguiente tabla se proporciona un ejemplo de subárbol de una unidad organizativa simple que podría utilizarse para organizar los grupos de seguridad creados y mencionados en esta guía.

Tabla 11.8: Ubicación de grupos de seguridad dentro de la estructura de la unidad organizativa

UO	Grupos	Finalidad
Servicios de Certificate Server		
Administración de Servicios de Certificate Server	Administradores de PKI de empresa Editores de PKI de empresa Administradores de entidad emisora Auditores de entidad emisora Administradores de certificados Operadores de copia de seguridad de CA	Contiene grupos administrativos para la administración de la configuración de la entidad emisora y la PKI de empresa.
Administración de plantillas de certificados	Ejemplos: Administración de plantilla de usuarios Administración de plantilla de inicio de sesión con tarjeta inteligente	Contiene grupos que poseen Control total de la plantilla del mismo nombre. Permite la delegación de control por tipo de plantilla.
Inscripción de plantillas de certificados	Ejemplos: Inscripción de certificado de usuario Inscripción automática de certificado de usuario Inscripción de certificado con firma electrónica	Contiene grupos que poseen permisos de inscripción o inscripción automática en plantillas del mismo nombre. El control de los grupos puede delegarse a continuación en el personal apropiado para favorecer un régimen de inscripción flexible sin tocar las plantillas reales.

Creación de grupos de administración de plantillas de certificados

Los grupos de administración de plantillas son útiles para delegar a diferentes administradores el control de las plantillas y la configuración de las mismas. De otro modo, sólo los administradores de empresa y los administradores de PKI de empresa tienen permiso para modificar las plantillas. Es posible que esta clase de delegación detallada no sea necesaria si su organización de TI no tiene un tamaño considerable. En este caso, sólo los miembros de los grupos Administradores de la empresa (el grupo integrado) y Administradores de PKI de empresa (creado como parte de esta solución) podrán administrar las plantillas de certificados.

Información de resumen

- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Usuarios y equipos de Active Directory de MMC
  - Complemento Plantilla de certificados de MMC

    Precaución: sea muy cuidadoso al utilizar esta característica. La delegación de control sobre un tipo de plantilla implica que debe tener completa confianza en la persona en la que delega. Los usuarios con permisos de escritura pueden cambiar todos los parámetros de una plantilla para crear el tipo de certificado que deseen. Puede que prefiera crear la plantilla en nombre de dichos usuarios, manteniendo el control de los tipos de certificados únicamente dentro del grupo Administradores de PKI de empresa.

Detalles de la tarea

Para cada plantilla de certificados que cree o desee activar en su entorno, lleve a cabo los siguientes procedimientos.

Para crear grupos de administración de plantillas de certificados

1. Inicie una sesión como miembro del grupo Administradores de PKI de empresa.

2. En la unidad organizativa Administración de plantillas de certificados, cree un grupo de seguridad global de dominio denominado **Administración de la plantilla *NombrePlantillaCertificado*** (donde *NombrePlantillaCertificado* es el nombre de la plantilla de certificados que se va a administrar).

3. Cargue el complemento **Plantillas de certificados** en una MMC.

4. Abra las propiedades de la plantilla requerida y haga clic en la ficha **Seguridad**.

5. Agregue el grupo Administración de la plantilla *NombrePlantillaCertificado* con permiso de **Escritura**.

Creación de grupos de inscripción de plantillas de certificados

Los grupos de inscripción de plantillas facilitan la administración de quién puede inscribirse o quién se inscribe automáticamente en un determinado tipo de certificado; los equipos o usuarios se pueden agregar o eliminar de un grupo de seguridad. También puede otorgar el control sobre la pertenencia de estos grupos al personal administrativo, sin que éste tenga permiso para editar las propiedades de las plantillas de certificados.

Información de resumen

- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Usuarios y equipos de Active Directory de MMC
  - Complemento Plantilla de certificados de MMC

Detalles de la tarea

Cree un grupo de inscripción para cada tipo de plantilla de certificado o, como mínimo, para todos cuya aprobación de certificado sea automática. (Si utiliza un proceso de registro más complejo o manual para un determinado tipo de certificado, el uso de grupos de inscripción de plantillas puede no resultar útil.) Si la inscripción automática es adecuada para el tipo de certificado, puede crear un grupo independiente que controle qué usuarios y dispositivos inscriben automáticamente el certificado.

Para crear un grupo de inscripción de plantillas de certificados

1. Inicie una sesión como miembro del grupo Administradores de PKI de empresa y abra el complemento Usuarios y equipos de Active Directory de MMC.

2. En la unidad organizativa de inscripción de plantilla de certificado, cree grupos de seguridad globales de dominio denominados del siguiente modo:
   - **Inscripción del certificado *NombrePlantillaCertificado***
   - **Inscripción automática del certificado *NombrePlantillaCertificado*** (si fuera necesario)

3. Cargue el complemento Plantillas de certificados en una MMC.

4. Abra las propiedades de la plantilla para editar la seguridad.

5. Agregue el grupo Inscripción del certificado *NombrePlantillaCertificado* y otórguele permisos de **Lectura** e **Inscripción**.

6. Agregue el grupo Inscripción automática del certificado *NombrePlantillaCertificado* y otórguele permisos de **Lectura**, **Inscripción** e **Inscripción automática**.

   Nota: de manera opcional, puede delegar el control de estos grupos de seguridad para permitir al propietario de la aplicación de certificados especificar quién puede inscribir este tipo de certificado y quién no.

Activación de la inscripción (o inscripción automática) de un tipo de certificado para un usuario o equipo

Esta tarea utiliza grupos de inscripción automática para permitir la inscripción manual o para iniciar la inscripción automática de un tipo de certificado para un usuario, equipo o grupo de seguridad que contiene usuarios y/o

equipos.

Información de resumen

- **Requisitos de seguridad**: modifique los permisos de pertenencia para el grupo de inscripción de certificados
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: complemento Usuarios y equipos de Active Directory de MMC

Nota: la inscripción automática también se debe habilitar en la directiva de dominio de los usuarios o equipos de destino. Para obtener más información, consulte la sección acerca de la configuración de la inscripción automática en Directiva de grupo en el capítulo 6, "Implementación de la infraestructura de claves públicas".

Detalles de la tarea
Para permitir la inscripción o la inscripción automática de un usuario o un equipo

1. En Usuarios y grupos de Active Directory, busque el grupo de seguridad Inscripción de plantillas de certificados (o el grupo Inscripción automática para inscribir automáticamente el certificado) correspondiente al tipo de certificado que se va a inscribir. Debe haber iniciado la sesión como usuario con permisos para **Modificar pertenencia a grupo** de este grupo.
2. Agregue el usuario, el equipo o el grupo de seguridad al grupo de seguridad de la plantilla seleccionada.

Desactivación de la inscripción (o inscripción automática) de un tipo de certificado para un usuario o equipo

La emisión de un certificado a un usuario o equipo habitualmente activa algunas funciones para el titular del certificado; es posible que tenga que revocar esta funcionalidad posteriormente.

Información de resumen

- **Requisitos de seguridad**: modifique los permisos de pertenencia para el grupo de inscripción de certificados
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Usuarios y equipos de Active Directory de MMC
  - Complemento Entidad emisora de certificados de MMC

Detalles de la tarea
Para deshabilitar la inscripción o la inscripción automática de un usuario o un equipo

1. En Usuarios y grupos de Active Directory, busque el grupo de seguridad Inscripción de plantillas de certificados (o Inscripción automática) correspondiente al tipo de certificado que se va a deshabilitar. Debe iniciar la sesión como usuario con permisos para **Modificar pertenencia a grupo** de este grupo.
2. Elimine el usuario, el equipo o el grupo de seguridad del grupo de seguridad de la plantilla.

   Nota: para cada usuario de certificado que desee deshabilitar, también deberá revocar el certificado de dicho usuario.
3. Inicie una sesión como miembro de Administradores de certificados y busque el certificado o los certificados existentes del usuario en la base de datos de la entidad emisora de certificados (en la MMC Entidad emisora de certificados). Para buscar los certificados, en la carpeta Certificados emitidos de la entidad emisora de certificados (CA), haga clic en el menú **Ver** y, a continuación, en la opción **Filtro**.
4. Haga clic en el certificado y, a continuación, en el menú **Tareas**, haga clic en **Revocar**.
5. Seleccione un código de motivo adecuado para la revocación. Si ninguno de los códigos de motivo predefinidos se adecua al motivo real de la revocación, seleccione **No especificado**.

   Importante: el único motivo que permite la posterior reinstalación del certificado es la **Posesión de certificado**. Todos los demás motivos darán como resultado la deshabilitación permanente del certificado. No obstante, no utilice **Posesión de certificado** si existe la posibilidad de que el certificado se pueda

rehabilitar. Utilice este código sólo cuando realmente deba suspender de forma temporal el certificado.

Administración de seguridad

La administración de seguridad es responsable de mantener un entorno de equipo seguro. La seguridad es una parte importante de la infraestructura de una organización; un sistema de información con una base de seguridad débil acabará sufriendo una infracción de seguridad.

Comprobación de solicitudes pendientes

Las solicitudes de certificados pueden publicarse en las entidades emisoras de certificados (CA) en cualquier momento. La mayoría de los certificados se emitirán automáticamente mediante Active Directory como autoridad de registro (RA) o un conjunto predefinido de firmas de autoridades de registro designadas. Si ha configurado la aprobación manual en determinados tipos de certificados mediante un Administrador de certificados, estas solicitudes se colocarán en una cola hasta que se aprueben o se rechacen.

Información de resumen

- **Requisitos de seguridad**: administradores de certificados
- **Frecuencia**: diaria
- **Requisitos de tecnología:** complemento Entidad emisora de certificados de MMC

Detalles de la tarea

Compruebe la carpeta de solicitudes diariamente para ver las solicitudes en cola. Antes de enviar un certificado, revise la solicitud cuidadosamente para comprobar el solicitante y el contenido de la solicitud. Compruebe que dicha solicitud contenga el nombre de asunto, el nombre de asunto alternante, los usos de claves, las directivas y las extensiones previstas. Si tiene dudas sobre alguno de estos elementos, no apruebe la solicitud.

También puede configurar la entidad emisora de certificados para enviar alertas por correo electrónico para diferentes sucesos, incluida la llegada de una solicitud pendiente. Consulte el procedimiento "Configuración de alertas de SMTP para solicitudes de certificados pendientes".

Para comprobar las solicitudes pendientes

1. Inicie una sesión en la entidad emisora como miembro de Administradores de certificados (puede realizar esta tarea de forma remota volviendo a establecer el foco en la MMC Entidad emisora de certificados en la CA).
2. Abra la MMC Entidad emisora de certificados y, a continuación, abra la carpeta **Solicitudes**.
3. Para ver los detalles de una solicitud de la carpeta, haga clic con el botón secundario del mouse en la solicitud y seleccione **Ver atributos/extensiones** en el submenú **Ver**.

   Nota: la ficha **Atributos** muestra los atributos de la solicitud recibidos como parte de la misma y la ficha **Extensiones** muestra las extensiones del certificado que se utilizarán en el mismo. Cada entrada de extensión indica si ésta se encuentra allí porque se ha incluido en la solicitud, porque es un valor suministrado por el servidor o porque se ha definido mediante el módulo Directiva de entidad emisora de certificados. (Este último origen generalmente indica que se trata de una extensión definida en la plantilla de certificados.)

   Según las directivas de su organización, es posible que reciba otra información relacionada con solicitud. Esta información se puede proporcionar en persona, por teléfono, correo electrónico u otro medio.
4. Después de haber comprobado que la solicitud es válida, puede aprobarla haciendo clic con el botón secundario del mouse y seleccionando **Emitir** en el submenú **Tareas**. Si no está convencido de su validez, puede denegar la solicitud haciendo clic en **Denegar** en el mismo menú.

Renovación del certificado de entidad emisora raíz

Debe renovar el certificado de entidad emisora regularmente para permitir que las entidades emisoras y las entidades finales subordinadas inscriban certificados con esta entidad emisora de certificados. Los certificados emitidos por esta entidad emisora y sus entidades subordinadas no pueden tener una fecha de caducidad posterior a la de este certificado de entidad emisora. Otras razones para renovar el certificado de entidad emisora se

producen cuando es necesario:

- Cambiar la clave utilizada por la entidad emisora (en caso de peligro real o potencial).
- Agregar directivas de certificado a la entidad emisora (subordinación calificada).
- Cambiar las rutas de acceso de CDP o de Acceso a la información de autoridad (AIA).
- Dividir la lista de revocación de certificados (CRL).

Normalmente, *siempre* debe cambiar la clave de la entidad emisora en cada renovación. Si desea renovar con la misma clave, consulte el procedimiento "Renovación del certificado de entidad emisora raíz con la misma clave".

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: cada 8 años
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS
  - Complemento Entidad emisora de certificados de MMC
  - Editor de texto

  Precaución: la renovación del certificado de entidad emisora raíz es un suceso muy importante. Asegúrese de informar a los propietarios de la aplicación afectados del nuevo certificado raíz en caso de que deban configurar esta nueva raíz en su aplicación.

Detalles de la tarea

Para renovar un certificado de entidad emisora raíz

1. Inicie una sesión en la entidad emisora raíz como miembro del grupo Administradores locales.
2. Si necesita cambiar el tamaño de la clave, debe editar el archivo CAPolicy.inf almacenado en el directorio %systemroot%. Cambie el valor de RenewalKeyLength por el nuevo tamaño de bit deseado. El proveedor de servicios criptográficos (CSP) que utiliza la entidad emisora debe admitir el tamaño de clave. En el ejemplo siguiente, este valor es 2.048.

   ```
   [Certsrv_Server]
   RenewalKeyLength=2048
   ```

   Nota: si necesita realizar algún cambio en el período de validez o en las directivas del certificado de entidad emisora, también deberá especificar dicho cambio en el archivo CAPolicy.inf (en %systemroot%) antes de iniciar este procedimiento.
3. Abra el complemento Entidad emisora de certificados de MMC. En el menú **Tareas** del objeto Entidad emisora, haga clic en **Renovar certificado de entidad emisora**. Aparecerá una advertencia de Servicios de Certificate Server avisándole de que tiene que detener la entidad emisora para renovar el certificado.
4. Seleccione la opción **Clave nueva**. Servicios de Certificate Server se reiniciará.
5. Lea el certificado desde las propiedades de la entidad emisora y compruebe que la fecha **Válido desde** del certificado de entidad emisora más reciente coincida con la fecha actual.
6. Emita una lista CRL y cópiela en el disco, junto con el certificado de entidad emisora nuevo, con los comandos siguientes:

   Cscript //job:getcacerts c:\MSSScripts\ca_operations.wsf

Cscript //job:getcrls c:\MSSScripts\ca_operations.wsf

7. Lleve el disco a la CA emisora. (Puede utilizar cualquier miembro de dominio que tenga instalado certutil.exe y las secuencias de comandos que se incluyen con esta solución, no tiene que ser la CA emisora).

8. Inicie una sesión como miembro del grupo Administradores de PKI de empresa y, a continuación, ejecute las siguientes secuencias de comandos:

   Cscript //job: PublishCertstoAD c:\MSSScripts\ca_operations.wsf

   Cscript //job: PublishCRLstoAD c:\MSSScripts\ca_operations.wsf

   Cscript //job: PublishRootCertstoIIS c:\MSSScripts\ca_operations.wsf

   Cscript //job: PublishRootCRLstoIIS c:\MSSScripts\ca_operations.wsf

   Nota: es recomendable renovar todas las entidades emisoras subordinadas a la vez. No obstante, no es obligatorio hacerlo. (Consulte "Renovación del certificado de entidad emisora de certificados").

9. Realice una copia de seguridad del certificado y de la clave de la entidad emisora raíz. (Consulte "Creación de copias de seguridad de claves y certificados de entidad emisora").

10. Realice una copia de seguridad del estado del sistema y de la base de datos del certificado de entidad emisora raíz. (Consulte "Copia de seguridad de la base de datos de la entidad emisora raíz").

Renovación del certificado de entidad emisora de certificados

Debe renovar el certificado de entidad emisora periódicamente para permitir que las entidades finales (y las entidades emisoras subordinadas si hubiera alguna) sigan inscribiendo certificados con esta entidad emisora de certificados. Los certificados emitidos por esta entidad emisora no pueden tener una fecha de caducidad posterior a la de este certificado de entidad emisora. Otras razones para renovar el certificado de entidad emisora se producen cuando es necesario:

- Cambiar la clave que utiliza la entidad emisora (en caso de peligro real o potencial).
- Agregar directivas de certificado a la entidad emisora (subordinación calificada).
- Cambiar las rutas de acceso CDP o AIA.
- Dividir la lista CRL.

Normalmente, *siempre* debe cambiar la clave de la entidad emisora en cada renovación. Si desea renovar con la misma clave, consulte el procedimiento "Renovación del certificado de entidad emisora de certificados con la misma clave".

Información de resumen

- **Requisitos de seguridad**:
  - Administradores locales en la entidad emisora
  - Administradores de certificados en entidad emisora raíz
  - Administradores de PKI de empresa
- **Frecuencia**: cada 4 años
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS
  - Complemento Entidad emisora de certificados de MMC
  -

Editor de texto

Importante: para renovar el certificado de entidad emisora correctamente y publicarlo en el almacén NTAuth de Active Directory (el cual identifica la entidad emisora como una entidad emisora de certificados de empresa), es necesario realizar la instalación del certificado de entidad emisora utilizando una cuenta que *sea* miembro de los grupos Administradores de PKI de empresa y Administradores locales. El primer grupo tiene derechos para publicar el certificado en el directorio y el último tiene derechos para instalar el certificado de entidad emisora en la entidad emisora de certificados.

Detalles de la tarea
Para renovar el certificado de entidad emisora

1. Inicie la sesión en la CA emisora como miembro del grupo de administradores locales.
2. Si necesita cambiar el tamaño de la clave, debe editar el archivo CAPolicy.inf almacenado en el directorio %systemroot%. Cambie el valor de RenewalKeyLength por el tamaño de bit deseado (el CSP que utiliza la CA debe admitir el tamaño de clave).

```
[Certsrv_Server]
RenewalKeyLength=2048
```

   Importante: si necesita realizar algún cambio en el período de validez o en las directivas del certificado de entidad emisora, también deberá especificar dicho cambio en el archivo CAPolicy.inf (en % systemroot%) antes de iniciar este procedimiento.

3. Abra el complemento Entidad emisora de certificados de MMC y, en el menú **Tareas** del objeto Entidad emisora de certificados, haga clic en **Renovar certificado de entidad emisora**.
4. Seleccione la opción **Clave nueva**.
5. Cuando se le solicite una entidad emisora a la que enviar la renovación, haga clic en **Cancelar** para guardar el archivo de la solicitud en el disco. A continuación, Servicios de Certificate Server se reiniciará.
6. Copie el archivo de solicitudes de certificados en disco. La solicitud de certificado se generará y se guardará en la ruta de acceso de la carpeta compartida (C:\CAConfig). Copie este archivo *HQ-CA-02.woodgrovebank.com_Woodgrove Bank Issuing CA 1*.req en disco. (reemplace el texto en cursiva por los detalles de su entidad emisora de certificados).
7. Lleve el disco a la entidad emisora raíz e inicie una sesión como miembro del grupo Administradores de certificados local.
8. En complemento Entidad emisora de certificados de MMC, desde el menú **Tareas** de la entidad emisora, haga clic en **Enviar solicitud nueva** y, a continuación, envíe la solicitud transferida desde la CA emisora (en el disco de solicitud de la entidad emisora subordinada).
9. La entidad emisora raíz requiere que se aprueben manualmente todas las solicitudes. Busque la solicitud en el contenedor **Peticiones pendientes**, compruebe que el campo **Nombre común** contenga el nombre de la CA emisora y, a continuación, apruebe (emita) la solicitud.
10. Busque el certificado recién emitido en el contenedor **Certificados emitidos** y ábralo.
11. Compruebe que los detalles del certificado sean correctos y, a continuación, haga clic en **Copiar en archivo** para exportar el certificado a un archivo. Guárdelo como un archivo PKCS#7 en el disco (para transferirlo de nuevo a la CA emisora).
12. Vuelva a iniciar sesión en la CA emisora con una cuenta que sea miembro *tanto* del grupo de administradores de PKI de empresa *como* del grupo de administradores locales. A continuación, introduzca el disco.
13. En el complemento Entidad emisora de certificados de MMC, en el menú **Tareas** de la entidad emisora de

certificados, haga clic en **Instalar certificado**. Instale el certificado de CA emisora desde el disco. La entidad emisora se reiniciará.

14. Lea el certificado desde las propiedades de la entidad emisora y compruebe que la fecha **Válido desde** del certificado de entidad emisora más reciente coincida con la fecha actual.

15. Publique el nuevo certificado de entidad emisora en la ubicación de publicación Web de CDP. (Consulte el procedimiento "Publicación del certificado de entidad emisora en el servidor Web").

16. Realice una copia de seguridad del certificado y de la clave de CA emisora. (Consulte el procedimiento "Creación de copias de seguridad de claves y certificados de entidad emisora".)

17. Realice una copia de seguridad del estado del sistema y de la base de datos del certificado de entidad emisora raíz. (Consulte el procedimiento "Copia de seguridad de la base de datos de la entidad emisora raíz".)

18. Realice una copia de seguridad del estado del sistema y de la base de datos del certificado de CA emisora. (Consulte el procedimiento "Configuración de la copia de seguridad de la base de datos de la entidad emisora de certificados".) De todos modos esta copia de seguridad se realiza con la copia de seguridad diaria normal.

Renovación del certificado de entidad emisora raíz con la misma clave

Normalmente, se debe cambiar *siempre* la clave de la entidad emisora raíz en cada renovación de certificado de entidad emisora programada (consulte el procedimiento "Renovación del certificado de entidad emisora raíz"). Es posible que necesite renovar el certificado de entidad emisora sin renovar la clave de entidad emisora si tiene que cambiar las directivas de la entidad emisora o ampliar la duración del certificado, etc. y mantener el mismo par de claves.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS
  - Editor de texto

Detalles de la tarea

Para renovar el certificado de entidad emisora raíz sin cambiar la clave de entidad emisora de certificados

- Siga el procedimiento "Renovación del certificado de entidad emisora raíz", pero cuando se le pregunte si desea renovar con una clave nueva, haga clic en **No**. Los cambios en el valor de RenewalKeyLength en el archivo CAPolicy.inf no se aplicarán.

El procedimiento es idéntico a "Renovación del certificado de entidad emisora raíz" con la única diferencia de que en éste se hace clic en **No** en la pregunta para generar una clave nueva.

Precaución: la renovación del certificado de entidad emisora raíz es un suceso muy importante. Asegúrese de informar a los propietarios de la aplicación afectados del nuevo certificado raíz en caso de que deban configurar esta nueva raíz en sus aplicaciones.

Renovación del certificado de entidad emisora de certificados con la misma clave

Normalmente, *siempre* debe cambiar la clave de una entidad emisora en cada renovación de certificado de entidad emisora programada. (Consulte "Renovación del certificado de entidad emisora de certificados".) Sin embargo, es posible que necesite renovar el certificado de entidad emisora sin renovar la clave de entidad emisora; por ejemplo, si tiene que cambiar las directivas de la entidad emisora o ampliar la duración del certificado, etc. y mantener el mismo par de claves.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS
  - Complemento Entidad emisora de certificados de MMC
  - Editor de texto

Detalles de la tarea
Para renovar el certificado de entidad emisora sin cambiar la clave de entidad emisora de certificados

- Siga el procedimiento para la renovación del certificado de entidad emisora raíz, pero cuando se le pregunte si desea renovar con una clave nueva, haga clic en **No**. Los cambios en el valor de RenewalKeyLength en el archivo CAPolicy.inf no se aplicarán.

El procedimiento es idéntico a "Renovación del certificado de entidad emisora de certificados" con la única diferencia de que en éste se hace clic en **No** en la pregunta para generar una clave nueva.

Publicación de una lista CRL y un certificado de entidad emisora fuera de línea

Debe publicar la lista de revocación de certificados (CRL) de una entidad emisora de certificados fuera de línea en una ubicación en línea para que los usuarios del certificado puedan comprobar el estado de revocación de toda la cadena de entidad emisora de certificados.

Información de resumen
- **Requisitos de seguridad**:
  - Administradores locales en la entidad emisora
  - Editores de PKI de empresa
- **Frecuencia**: cada seis meses o cuando sea necesario
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS

Detalles de la tarea
Para publicar la lista CRL raíz en Active Directory y la dirección URL Web sin conexión

1. Inicie una sesión en la entidad emisora raíz como miembro del grupo Administradores de entidad emisora de certificados.
2. Emita una lista CRL y cópiela en el disco, junto con el certificado de entidad emisora nuevo, con los comandos siguientes:

   Cscript //job:getcacerts c:\MSSScripts\ca_operations.wsf

   Cscript //job:getcrls c:\MSSScripts\ca_operations.wsf
3. Lleve el disco a la CA emisora. (El servidor no necesita ser la CA emisora; puede ser un miembro del dominio con certutil.exe y las secuencias de comandos de MSS instaladas.)
4. Inicie una sesión como miembro del grupo Editores de PKI de empresa y ejecute las siguientes secuencias de comandos:

   Cscript //job: PublishCertstoAD c:\MSSScripts\ca_operations.wsf

Cscript //job: PublishCRLstoAD c:\MSSScripts\ca_operations.wsf

Cscript //job: PublishRootCertstoIIS c:\MSSScripts\ca_operations.wsf

Cscript //job: PublishRootCRLstoIIS c:\MSSScripts\ca_operations.wsf

Cómo forzar la emisión de una lista CRL en línea

Las listas CRL de una entidad emisora de certificados de empresa en línea se emiten y publican de forma automática por lo que, normalmente, no se requiere forzar la emisión de una lista CRL en línea. No obstante, puede ser necesario forzar la emisión de una lista CRL en línea cuando se ha producido una revocación crítica (por ejemplo, si la entidad emisora ha revocado todos los certificados) y es necesario publicar una listas CRL nuevas lo más rápidamente posible.

Nota: no es posible pasar una lista CRL a los clientes, ya que éstos conservarán sus copias en caché existentes hasta que éstas caduquen. No obstante, aparte de los retrasos en la propagación, desde el momento que se publica la lista CRL nueva, cualquier cliente que solicite una lista CRL recibirá la nueva.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología:** complemento Entidad emisora de certificados de MMC

Detalles de la tarea

Para emitir y publicar la lista CRL de entidad emisora de certificados sin conexión en Active Directory

1. Inicie una sesión en la entidad emisora de certificados como miembro de Administradores de entidad emisora de certificados y cargue el complemento Entidad emisora de certificados de MMC.
2. Haga clic en **Publicar** para emitir una nueva lista CRL desde el menú **Tareas** de la carpeta Certificados revocados.
3. Seleccione **Lista de revocación de certificados (CRL) nueva** para emitir una CRL básica, o bien **Sólo diferencias entre listas CRL** para una diferencia entre listas CRL nueva.

Publicación del certificado de entidad emisora en el servidor Web

El certificado o los certificados de la entidad emisora de certificados deben publicarse en la ubicación AIA de HTTP (Protocolo de transferencia de hipertexto).

Información de resumen

- **Requisitos de seguridad**: Editores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Secuencias de comandos MSS
  - Certutil.exe

Detalles de la tarea

Técnicamente, es posible configurar la entidad emisora para publicar directamente en la carpeta del servidor Web. Sin embargo, este método no siempre resulta práctico por motivos de seguridad y conectividad de red. El método siguiente utiliza una técnica de copia de archivos simple, pero puede ampliarse para adaptarse a la mayor parte de configuraciones.

Nota: es posible que este método no resulte adecuado para publicar directamente en un servidor Web conectado a Internet ya que requiere conectividad de red directa y utilizar el uso compartido de archivos de bloques de mensajes de servidor (SMB), que normalmente se bloquea en los servidores de seguridad. Para publicar en un servidor de Internet, utilice el método siguiente para publicar en una ubicación intermedia y, a continuación, utilice el método estándar que desee para publicar contenido en el servidor Web de forma segura. Debe tener en cuenta la latencia agregada de este método.

El certificado de entidad emisora se actualiza con poca frecuencia, por lo que puede publicar en AIA manualmente cuando se renueve el certificado de entidad emisora.

Para publicar el certificado de CA emisora

1. Inicie la sesión en la CA emisora con una cuenta que disponga de permisos de escritura en la carpeta del servidor Web publicada.
2. Si el servidor Web se encuentra en un servidor remoto, asegúrese de que la carpeta del servidor Web esté compartida. Anote la ruta de acceso UNC (Convención de nomenclatura universal) de la carpeta compartida.
3. Si el servidor Web está en el mismo servidor que la entidad emisora, anote la ruta de acceso local de la carpeta.
4. Actualice el parámetro WWW_REMOTE_PUB_PATH en C:\MSSScripts\PKIParams.vbs para que coincida con la ruta de acceso de destino de la carpeta del servidor Web (el valor predeterminado es la ruta local C:\CAWWWPub).
5. Ejecute el siguiente comando para publicar el certificado de entidad emisora en el servidor Web:

   Cscript //job:PublishIssCertsToIIS C:\MSSScripts\CA_Operations.wsf

Publicación de las listas CRL de entidad emisora de certificados en el servidor Web

Debe publicar las CRL de entidad emisora de certificados en la ubicación del Punto de distribución de CRL (CDP) de HTTP.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Secuencias de comandos MSS
  - Certutil.exe
  - Servicio del programador de tareas de Windows
  - SchTasks.exe

Detalles de la tarea

Técnicamente, es posible configurar la entidad emisora para publicar directamente en la carpeta del servidor Web. Sin embargo, este método no siempre resulta práctico por motivos de seguridad y conectividad de red. El método siguiente utiliza una técnica de copia de archivos simple, pero puede ampliarse para adaptarse a la mayor parte de configuraciones.

Nota: es posible que este método no resulte adecuado para publicar directamente en un servidor Web conectado a Internet ya que utiliza el uso compartido de archivos de bloques de mensajes de servidor (SMB) y requiere conectividad de red directa que normalmente se bloquea en los servidores de seguridad. Para publicar en un servidor de Internet, utilice el método siguiente para publicar en una ubicación intermedia y, a continuación, utilice el método estándar que desee para publicar contenido en el servidor Web de forma segura. Debe tener en cuenta la latencia agregada de este método y el efecto que puede tener en la actualización de las listas CRL.

La entidad emisora de certificados emite listas CRL frecuentemente (diariamente o cada hora, en el caso de diferencias entre listas CRL). Por lo tanto, se requiere un método automático de replicación de las CRL en el servidor Web.

Para automatizar la publicación de las listas CRL

1. Inicie sesión en la CA emisora con una cuenta miembro del grupo de administradores locales.
2. Asegúrese de que se pueda obtener acceso a la carpeta del servidor Web (como carpeta compartida o

como ruta de acceso local) desde este servidor.

3. Si el servidor Web es remoto, conceda a la cuenta del equipo de CA emisora acceso para escribir en la carpeta del sistema de archivos (acceso para **Modificar**) y al recurso compartido (acceso para **Cambiar**) correspondiente a la carpeta del servidor Web publicado. Si el servidor Web es un miembro del bosque, puede utilizar el grupo Publicadores de certificados para conceder acceso con el fin de garantizar que todas las entidades emisoras de certificados de empresa tengan los permisos necesarios para publicar certificados y listas CRL en esta carpeta. No es necesario cambiar los permisos del servidor Web. (Consulte la sección "Configuración de IIS para la publicación de AIA y CDP" del capítulo 6.)

4. Cree un trabajo programado que utilice el siguiente comando para copiar las listas CRL:

   schtasks /create /tn "Publicar listas CRL" /tr "cscript.exe
   //job:PublishIssCRLsToIIS \"C:\MSSScripts\CA_Operations.wsf\""
   /sc Hourly /ru "Sistema"

   Este comando se muestra en varias líneas; escríbalo en una sola.)

   Nota: con este procedimiento se creará un trabajo programado por horas para publicar las listas CRL en el servidor Web. Este intervalo es suficiente para hacer frente a un programa de publicación de diferencia entre listas CRL cada día o incluso cada medio día. Si el programa de CRL es más frecuente, haga que el trabajo de copia se ejecute con mayor frecuencia. Una buena norma general es que el programa de trabajo de copia debe ser aproximadamente del cinco al diez por ciento del programa de diferencia entre listas CRL.

Administración de almacenamiento

La administración de almacenamiento pertenece al almacenamiento en el sitio y fuera del sitio en lo que se refiere a la restauración de datos y el archivado histórico. El equipo de administración de almacenamiento debe garantizar la seguridad física de las copias de seguridad y archivos. El objetivo de la administración de almacenamiento consiste en definir, realizar un seguimiento y mantener los datos y los recursos de datos en el entorno de TI de producción.

Configuración de la copia de seguridad de la base de datos de la entidad emisora de certificados

El objetivo de esta tarea consiste en realizar una copia de seguridad de los certificados y claves privadas CA, la base de datos de certificados y la información de configuración de Servicios de Certificate Server. La información de configuración de Servicios de Certificate Server incluye la configuración del sistema operativo y cualquier información sobre el estado de la que dependa la entidad emisora.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Copia de seguridad de Windows
  - Sistema de copia de seguridad organizativo
  - Servicio del programador de tareas de Windows
  - SchTasks.exe

Detalles de la tarea

Esta tarea configura un trabajo programado para la creación de una copia de seguridad nocturna del estado del sistema del servidor de entidad emisora de certificados. El procedimiento supone que su organización dispone de un sistema de copia de seguridad de servidor. Este proceso de copia de seguridad dará como resultado un archivo de copia de seguridad que puede copiar el sistema de copia de seguridad de su organización. La copia de seguridad organizativa puede ser una copia de seguridad de red o de un dispositivo local. La solución también supone que el sistema de copia de seguridad de servidor de la organización se ejecuta durante la noche para realizar las copias de seguridad del servidor de la CA.

Nota: si utiliza un módulo de seguridad de hardware (HSM), este procedimiento podría realizar una copia de seguridad del material de claves cifradas (según cómo funcione el HSM), pero esta copia de seguridad normalmente no podrá utilizarse en un equipo restaurado sin un HSM idéntico y las claves de acceso a HSM. Siga las instrucciones del proveedor del HSM para realizar la copia de seguridad y proteger el material importante y las claves de acceso.

Para configurar una copia de seguridad de la CA

1. Cree un directorio en el que pueda guardar los archivos temporales de copia de seguridad (por ejemplo, C:\CABackup) y proteja el directorio ejecutando el siguiente comando:

   cacls c:\CABackup /G system:F administrators:F "Backup Operators":C "CA Backup Operators":C

   (Este comando se muestra en varias líneas; escríbalo en una sola.)

2. Si elige una carpeta diferente para almacenar la copia de seguridad, debe actualizar la configuración relacionada en pkiparams.vbs. Cambie la ruta de la línea siguiente según sea necesario.

   ```
   CONST SYSSTATE_BACKUP_PATH = "C:\CABackup"   'path used by NTBackup
   ```

   Nota: puesto que se utiliza la misma función de secuencia de comandos para crear copias de seguridad de la entidad emisora de certificados en línea y fuera de línea, debe realizar copias individuales de las secuencias de comandos si va a utilizar rutas de acceso diferentes para las distintas entidades emisoras de certificados.

3. Programe el trabajo de copia de seguridad para que se ejecute durante la noche con el comando siguiente. Este comando establece que el trabajo se ejecutará a las 2:00 a.m. cada noche.

   SCHTASKS /Create /RU system /SC Daily /TN "CA Backup" /TR "cscript.exe //job:BackupCADatabase \"C:\MSSScripts\ca_operations.wsf\"" /ST 02:00

   Este comando se muestra en varias líneas; escríbalo en una sola.)

   Nota: la barra diagonal inversa seguida de comillas (\") que se muestra a ambos lados del nombre de secuencia de comandos, "C:\MSSScripts\ca_operations.wsf", sólo se necesita si hay espacios incluidos en el nombre de archivo o de ruta de acceso de esta secuencia de comandos. La barra diagonal inversa se utiliza para crea una secuencia de "escape" de las comillas que encierran el nombre de secuencia de comandos para que dicho nombre y la ruta de acceso se almacenen como un solo parámetro de la línea de comandos del trabajo schtasks en vez de dividirse en varias partes. Estos caracteres pueden omitirse si no hay espacios en el nombre de la ruta de acceso.

4. Configure el sistema de copia de seguridad del servidor de la organización para que realice una copia de seguridad de la carpeta de copia de seguridad temporal (C:\CABackup) cada noche en un medio extraíble. Si es posible, establezca una secuencia de comandos como condición previa para el archivo de bloqueos (BackupRunning.lck, almacenado en la carpeta de copia de seguridad temporal) que el archivo de secuencia de comandos de copia de seguridad crea mientras se ejecuta. Si este archivo existe, esto significa que se produjo un error en la copia de seguridad anterior o que continúa ejecutándose. Si lo desea, puede hacer que el sistema de copia de seguridad de la organización ejecute la secuencia de comandos de copia de seguridad de la CA como un trabajo previo a la ejecución.

   Nota: cada vez que se ejecuta la secuencia de comandos de copia de seguridad BackupCADatabase, busca el archivo de bloqueos. Si el archivo existe, la secuencia de comandos escribe el siguiente suceso de error en el registro de aplicación:

   Origen: Operaciones de entidad emisora de certificados

   Id. de suceso: 30

   Tipo de suceso: Error

La copia de seguridad de entidad emisora de certificados no se ha podido iniciar porque el archivo de bloqueo C:\CABackup\BackupRunning.lck de un trabajo anterior sigue en el sistema. Esto puede significar que la copia de seguridad anterior todavía se está ejecutando.

Si el sistema de copia de seguridad del servidor de la organización no tiene la capacidad de realizar comprobaciones previas a la condición o ejecutar secuencias de comandos, programe el inicio de la copia de seguridad del servidor a una hora conveniente, posterior a la del inicio de la copia de seguridad del estado del sistema. Para estimar el tiempo adecuado, ejecute una copia de seguridad del estado del sistema (con la opción **Comprobar** activada) en el servidor con Servicios de Certificate Server desactivado. (Al cerrar la CA, se evita que se puedan truncar los registros de la CA para esta copia de seguridad de prueba.) Esto realizará una copia de seguridad de aproximadamente 500 megabytes (MB) de datos de estado del sistema. Cronometre el proceso y utilice la siguiente ecuación para calcular el tiempo aproximado para una copia de seguridad de la base de datos CA más el estado del sistema:

Ttotal = TEstadoSistema x (500 + (Nusuarios x NCertificados x 20KB x 2)) ÷ 500

En esta ecuación se suponen cinco certificados por usuario y por equipo, por año, almacenados durante cinco años en la base de datos antes del archivado. Si permite 20 kilobytes (KB) por certificado, el resultado del cálculo es de 1 MB de almacenamiento por usuario. Si el tiempo para realizar la copia de seguridad de sólo el estado del sistema ha sido de 10 minutos, deje 70 minutos para una entidad emisora de certificados con 3.000 usuarios. Este cálculo es aproximado; para calcularlo de otra forma, deje 1 gigabyte (GB) por cada 50.000 certificados.

Nota: si utiliza el archivado de claves, los requisitos de almacenamiento de certificados será mayor para certificados con claves archivadas. Para estos certificados, deja unos 10 KB adicionales por certificado (aunque se puede necesitar almacenamiento adicional si tiene configurados numerosos agentes de recuperación en la CA).

5. Almacene adecuadamente el medio de copia de seguridad.

   Precaución: estos datos de copia de seguridad son muy importantes, ya que contienen el material de claves privadas de la entidad emisora. Debe transportar y almacenar los datos con el mismo cuidado y seguridad que concede a la entidad emisora. Almacene los datos de copia de seguridad en un sitio físico distinto de la entidad emisora para poder recuperarla si se destruye todo el equipo informático del sitio o no se puede acceder a él.

Configuración de la copia de seguridad de la base de datos de entidad emisora raíz

El objetivo de esta tarea consiste en preparar los certificados y claves privadas de la entidad emisora, la base de datos de certificados y la información de configuración de Servicios de Certificate Server para la copia de seguridad. La información de configuración de Servicios de Certificate Server incluye la configuración del sistema operativo y cualquier información sobre el estado de la que dependa la entidad emisora.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Copia de seguridad de Windows
  - Medios extraíbles (como un CD-RW o una cinta)

Detalles de la tarea

Normalmente, la entidad emisora raíz sólo emite algunos certificados, de modo que el tamaño de los datos nunca será demasiado grande. Los datos cambian con muy poca frecuencia, posiblemente una vez cada varios años. El procedimiento también sería el mismo para cualquier otra entidad emisora, como un intermediario sin conexión, si ha elegido utilizar entidades emisoras intermedias.

La entidad emisora raíz no tiene conexión, por lo que necesitará cierto tipo de dispositivo de copia de seguridad local (como una entidad emisora de certificados con unidad de cinta o permiso de escritura) en el que se pueda

guardar el archivo de copia de seguridad.

Precaución: si utiliza un HSM, este procedimiento puede realizar la copia de seguridad del material de claves cifradas (según el funcionamiento de HSM), pero las claves que se copien no podrán utilizarse en un equipo restaurado sin un HSM y claves de acceso a HSM idénticas. Siga las instrucciones del proveedor del HSM para realizar la copia de seguridad y proteger el material importante y las claves de acceso.

Para configurar una copia de seguridad de la CA

1. Cree un directorio en el que pueda guardar los archivos de copia de seguridad (por ejemplo, C:\CABackup) y proteja el directorio ejecutando el siguiente comando:

   cacls c:\CABackup /G system:F administrators:F "Backup Operators":C "CA Backup Operators":C

   Este comando se muestra en varias líneas; escríbalo en una sola.)

2. Si elige una carpeta diferente para almacenar la copia de seguridad, debe actualizar la configuración relacionada en pkiparams.vbs. Cambie la ruta de la línea siguiente según sea necesario.

```
CONST SYSSTATE_BACKUP_PATH = "C:\CABackup"   'path used by NTBackup
```

Copia de seguridad de la base de datos de la entidad emisora raíz

La finalidad de esta tarea consiste en crear copias de seguridad de los certificados y claves privadas de entidad emisora de certificados, la base de datos de certificados y la información sobre la configuración de Servicios de Certificate Server. La información de configuración de Servicios de Certificate Server incluye la configuración del sistema operativo y cualquier información sobre el estado de la que dependa la entidad emisora.

Información de resumen

- **Requisitos de seguridad**: operadores de copia de seguridad de CA
- **Frecuencia**: cada vez que se emite o se revoca un certificado nuevo
- **Requisitos de tecnología**:
  - Copia de seguridad de Windows
  - Medios extraíbles (como un CD-RW o una cinta)

Detalles de la tarea

Normalmente, la entidad emisora raíz sólo emite algunos certificados, de modo que el tamaño de los datos nunca será demasiado grande. Los datos cambian con muy poca frecuencia, posiblemente una vez cada varios años. El procedimiento también sería el mismo para cualquier otra entidad emisora, como un intermediario sin conexión, si ha elegido utilizar entidades emisoras intermedias.

La entidad emisora raíz no tiene conexión, por lo que necesita cierto tipo de dispositivo de copia de seguridad local (como una entidad emisora de certificados con unidad de cinta o permiso de escritura).

Precaución: si utiliza un HSM, este procedimiento puede realizar la copia de seguridad del material de claves cifradas (según el funcionamiento de HSM), pero las claves que se copien no podrán utilizarse en un equipo restaurado sin un HSM y claves de acceso a HSM idénticas. Siga las instrucciones del proveedor del HSM para realizar la copia de seguridad y proteger el material importante y las claves de acceso.

Para realizar una copia de seguridad de la entidad emisora raíz

1. Ejecute el comando siguiente para realizar la copia de seguridad de los datos de la entidad emisora en un archivo temporal:

   cscript //job:BackupCADatabase C:\MSSScripts\ca_operations.wsf

2. Este comando produce un archivo de copia de seguridad CABackup.bkf en la ruta de acceso elegida anteriormente (la ruta predeterminada es C:\CABackup). Copie este archivo en un medio extraíble y guárdelo en un lugar seguro.

Precaución: estos datos de copia de seguridad son muy importantes, ya que contienen el material de claves privadas de la entidad emisora. Debe transportar y almacenar los datos con el mismo cuidado y seguridad que concede a la entidad emisora. Almacene los datos de copia de seguridad en un sitio físico distinto de la propia entidad emisora para poder recuperarla si se destruye todo el equipo informático del sitio o no se puede acceder a él.

Creación de copias de seguridad de claves y certificados de entidad emisora

Deben realizarse copias de seguridad de certificados y claves independientemente de la base de datos de certificados. Es posible que las claves privadas y los certificados de entidad emisora deban firmar una lista CRL o un certificado en caso de que el servidor de entidad emisora de certificados falle y no pueda recuperarse en el tiempo previsto.

Información de resumen

- **Requisitos de seguridad**: operadores de copia de seguridad de CA
- **Frecuencia:** anualmente o cada vez que se renueve un certificado de entidad emisora (lo primero que se produzca)
- **Requisitos de tecnología**:
  - Certutil.exe
  - Secuencias de comandos MSS

Detalles de la tarea

Las claves y los certificados de entidad emisora de certificados sólo ocupan algunos kilobytes de almacenamiento y, por lo tanto, pueden guardarse en un disco sin problemas. Esta tarea se aplica a la entidad emisora raíz y a las entidades emisoras de certificados intermedias y emisoras de la organización. Si va a realizar la copia de seguridad de las claves en un almacenamiento de larga duración, como CD o DVD, no tiene que hacer la copia de seguridad anualmente. Si va a utilizar medios magnéticos, como disquetes o cintas, debe realizar una copia de seguridad de las claves y de los certificados anualmente, así como después de una renovación de certificado de CA. La señal grabada en un medio magnético se deteriora con el tiempo, en concreto si se expone a campos eléctricos. Aunque los medios magnéticos pueden tardar muchos años en deteriorarse y quedar ilegibles, es mejor ser precavidos.

Precaución: si utiliza un HSM, este procedimiento no funcionará como se indica. Siga las instrucciones del proveedor del HSM para realizar la copia de seguridad y proteger el material importante y las claves de acceso.

Para exportar los certificados y claves a un disco

1. Ejecute el siguiente comando:

   cscript //job:BackupCAKeys c:\MMSScripts\ca_operations.wsf

   Realice dos copias de seguridad distintas como mínimo en discos diferentes (los discos no siempre son completamente confiables). Rotule y feche los discos claramente según corresponda, teniendo en cuenta que podría transcurrir mucho tiempo antes de que vuelvan a necesitarse.

   Esta secuencia de comandos utiliza certutil.exe para exportar las claves y los certificados de la entidad emisora a un archivo PKCS#12 (P12) de la siguiente ubicación:

   A:\CAKeyBackup*NombreEquipoCA**aammdd_hhmm*\Nombre común CA.p12

   NombreEquipoCA es el nombre de host de la entidad emisora y *aammdd_hhmm* es la fecha y hora de la copia de seguridad.

2. Escriba una contraseña cuando se le solicite.

   Importante: grabe y almacene esta contraseña en una ubicación distinta, pero igualmente segura, de la de las propias copias de seguridad de las claves. El registro de la contraseña debe indicar claramente con qué copia de seguridad (etiqueta de disco, fecha y nombre de la CA) está relacionada. Pueden pasar meses o años hasta que vuelvan a necesitarse estas claves y es improbable que alguien pueda recordar la contraseña que se utilizó en el momento. Asegúrese de destruir el resto de registros de esta contraseña.

No utilice una contraseña que conozca el personal administrativo.

3. Guarde el disco adecuadamente. Al igual que las copias de seguridad de la base de datos de la entidad emisora, estas copias de seguridad de claves deben estar muy protegidas. Almacene como mínimo dos copias de seguridad de los certificados y las claves en dos ubicaciones seguras separadas.

Prueba de copias de seguridad de la base de datos de entidad emisora de certificados
Compruebe las copias de seguridad de entidad emisora de certificados para asegurarse de que el proceso y la tecnología del proceso de copia de seguridad se realicen correctamente.

Información de resumen
- **Requisitos de seguridad**: administradores locales u operadores de copia de seguridad en equipo de prueba
- **Frecuencia**:
  - Antes de que la entidad emisora esté operativa
  - Mensualmente
  - Vuelva a hacer pruebas siempre que se haga algún cambio en la tecnología o el proceso de copia de seguridad
- **Requisitos de tecnología**:
  - Copia de seguridad de Windows
  - Sistema de copia de seguridad organizativo
  - Certutil.exe
  - Cipher.exe

Detalles de la tarea
Debe restaurar la copia de seguridad del estado del sistema en un sistema que tenga un diseño de disco idéntico. Por ejemplo, Windows debe instalarse en la misma ruta de acceso del directorio que el sistema a partir del cual se realizó una copia de seguridad. Además, el diseño de la unidad para guardar los archivos de Windows (como los archivos de paginación) así como la base de datos y los registros de la entidad emisora de certificados debe ser igual al diseño de la entidad emisora de certificados original a partir de la cual se creó la copia de seguridad.

Importante: el servidor de prueba restaurado debe guardarse sin conexión desde el momento en que el archivo de copia de seguridad del estado del sistema se recupera de los medios de copia de seguridad y, en cualquier caso, antes del inicio de la restauración del estado del sistema. Esta separación de la red impedirá que las claves de entidad emisora restauradas se expongan innecesariamente y que se produzcan conflictos por nombres y direcciones IP duplicados entre la prueba y los servidores originales.

Advertencia: si utiliza un HSM, este procedimiento no será suficiente para restaurar totalmente la entidad emisora de certificados. Según el funcionamiento del HSM, el equipo restaurado no podrá utilizarse sin un HSM y claves de acceso al HSM idénticas. Esta situación quizás sea suficiente para una prueba normal, pero debe realizar una restauración completa periódicamente con recuperación de HSM para garantizar que sus procedimientos y su tecnología de copia de seguridad funcionen correctamente. Siga las instrucciones del proveedor de HSM para realizar la copia de seguridad, restaurar y proteger el material importante y las claves de acceso.

Para restaurar la entidad emisora de certificados

1. Restaure el archivo de copia de seguridad correspondiente al estado del sistema desde los medios de copia de seguridad a la carpeta C:\CABackup.
2. Ejecute la utilidad de copia de seguridad de Windows y seleccione el archivo de copia de seguridad restaurado en C:\CABackup. Necesitará ser un miembro de un grupo que tenga derechos de creación de copias de seguridad y restauración en el equipo (como son los operadores de copia de seguridad de entidad emisora de certificados, operadores de copia de seguridad o administradores).
3. Haga clic en **Restaurar**.

4. Reinicie el sistema.
5. Compruebe que todo se realice según lo previsto.
6. Elimine de forma segura el contenido del disco del servidor de prueba (o elimine las claves como mínimo) al final de la prueba.

Si decide eliminar únicamente las claves, primero debe eliminar los contenedores de claves de entidad emisora y, a continuación, elimine de forma segura las partes no asignadas del disco. Para realizar esta operación, deberá ser miembro del grupo Administradores locales.

Para eliminar de forma segura las claves de entidad emisora restauradas

1. Muestre los contenedores de claves en el servidor de prueba con el siguiente comando:

   Certutil –key

2. Anote todos los contenedores que coincidan con el nombre de entidad emisora (incluidos los que tiene un sufijo de índice). Por ejemplo, "Entidad emisora de Woodgrove Bank 1(1)".
3. Elimine cada uno de estos contenedores de claves del servidor de prueba con el siguiente comando y reemplace NombreContenedorClaves por los valores obtenidos en el paso anterior:

   Certutil –delkey *NombreContenedorClaves*

4. Elimine de forma segura el espacio no asignado en la unidad para garantizar que los datos de claves se eliminan por completo del disco. En el siguiente comando, la ruta de acceso %allusersprofile% hace que el comando cipher se ejecute en la unidad que contiene el material de claves.

   Cipher /W:%AllUsersProfile%

Prueba de copias de seguridad de claves de entidad emisora de certificados

Compruebe las copias de seguridad de claves de entidad emisora de certificados periódicamente para comprobar su validez, en caso de que alguna vez se necesiten.

Información de resumen

- **Requisitos de seguridad**: administradores locales en el equipo de prueba
- **Frecuencia**:
  - Tarea de configuración (antes de que la entidad emisora esté operativa)
  - Cada 6 meses
- **Requisitos de tecnología**:
  - Certutil.exe
  - Cipher.exe

Detalles de la tarea

Puede instalar las claves y certificados de entidad emisora en cualquier sistema. No obstante, debido a la naturaleza extremadamente confidencial de estas claves, este sistema debe estar en un sistema de confianza y sin conexión, en concreto para las claves de entidad emisora raíz sin conexión. Para garantizar que se han eliminado todos los rastros del material de claves del equipo, cree una cuenta de usuario local temporal e independiente en el equipo dedicado a este fin (puede utilizar cualquier nombre para esta cuenta).

Precaución: si utiliza un HSM, este procedimiento no funcionará como se indica. Siga las instrucciones del proveedor de HSM para realizar la copia de seguridad, restaurar y proteger el material importante y las claves de acceso.

Para restaurar las claves de entidad emisora

1. Asegúrese de que el equipo está desconectado de la red. Inicie la sesión como miembro de los

administradores locales y cree la cuenta de usuario local TestCAKeys.

2. Inicie la sesión con la cuenta TestCAKeys.
3. Inserte el disco que contenga la copia de seguridad de las claves de la entidad emisora que debe probarse.
4. Utilice el Explorador de Windows para buscar el archivo de clave P12 y haga doble clic en el archivo. Se iniciará el Asistente para importación de certificados.
5. Escriba la contraseña cuando se le solicite. No active las casillas de verificación para proporcionar alta protección para las claves o para hacerlas exportables.
6. Haga clic en **Colocar todos los certificados en el siguiente almacén** y, a continuación, en **Examinar** y seleccione **Almacén personal** como la ubicación en la que deben restaurarse las claves de la entidad emisora.
7. Abra el complemento Certificados de MMC y busque el almacén personal. Busque el certificado de entidad emisora para la entidad emisora restaurada y ábralo para comprobar que tiene la clave privada correspondiente. (Debe verlo indicado en la parte inferior de la ficha **General**.)

Para probar las claves restauradas

1. Obtenga una lista CRL o un certificado emitido por la entidad emisora que se está probando.
2. Según haya elegido una lista CRL o un certificado en el paso anterior, elija y ejecute el comando pertinente entre los que se incluyen a continuación y sustituya el nombre del archivo obtenido en el paso 1 por *NombreArchivoCRL* o *NombreArchivoCertificado*:

   Certutil -sign *NombreArchivoCRL.crl CRLNueva.crl*

   Certutil -sign *NombreArchivoCertificado.cer NombreArchivoCertificado.cer*
3. Cuando se le solicite, seleccione el certificado de entidad emisora (importado en el procedimiento anterior) como el certificado de firma.
4. Ejecute el siguiente comando certutil para comprobar que la operación de firma se ha realizado correctamente. La salida del comando debe ser similar a la siguiente:

   C:\CA>Configcertutil -sign "Entidad emisora de Woodgrove Bank 1.crl" "Entidad emisora de Woodgrove Bank 1xxs.crl"

   ThisUpdate: 10/02/03 22:52

   NextUpdate: 2/25/2003 3:11 PM

   Entradas de CRL: 0

   Firma del sujeto del certificado:

   CN=Woodgrove Bank Issuing CA 1

   DC=woodgrovebank,DC=com

   Longitud de salida = 970

   CertUtil: -comando de firma completado correctamente.

Ahora debe limpiar las claves del sistema de pruebas.

Para limpiar las claves del sistema

1. Inicie la sesión como miembro de Administradores locales y elimine el perfil de usuario de la cuenta TestCAKeys (mediante **Propiedades avanzadas** en Mi PC).

2. Elimine la cuenta TestCAKeys.
3. Borre de forma segura las áreas sin asignar del disco para quitar permanentemente todo rastro de las claves. Para ello, ejecute el comando siguiente:

   Cipher /W:%AllUsersProfile%

   Nota: al especificar %allusersprofile% como ruta de acceso, se asegura de que Cipher.exe se ejecutará en la unidad que contiene los perfiles de usuario. Esto limpia toda la unidad, no sólo la ruta indicada.

Archivado de los datos de auditoría de seguridad desde una entidad emisora de certificados
Archive y guarde registros de auditoría a fin de cumplir con los requisitos legales o jurídicos, o bien para cumplir con una directiva de seguridad interna.

Información de resumen
- **Requisitos de seguridad**:
  - Auditores de entidad emisora
  - Administradores locales en la entidad emisora
- **Frecuencia**:
  - Mensualmente (CA emisora)
  - Cada 6 meses (entidad emisora raíz)
- **Requisitos de tecnología**:
  - Visor de eventos
  - Medios extraíbles (como un CD-RW o una cinta)

Detalles de la tarea
Para archivar el registro de sucesos de seguridad

1. Inicie una sesión en el servidor como miembro de Auditores de entidad emisora de certificados y Administradores locales (cree una cuenta que sea miembro de ambos grupos).
2. Abra Visor de sucesos (haga clic en **Inicio**, **Todos los programas** y, a continuación, en **Herramientas administrativas**).
3. Haga clic en la carpeta Registro de seguridad para seleccionarla.
4. Haga clic con el botón secundario del mouse en la carpeta y, en el menú desplegable, haga clic en **Guardar registro como**.
5. Guarde el registro en un archivo temporal.
6. Cópielo en un medio extraíble (CD-RW) y, a continuación, elimine el archivo temporal.

Exportación de una plantilla de certificados desde Active Directory
Puede guardar definiciones de plantillas de certificados desde el directorio para poder restaurarlas en el futuro sin tener que realizar una restauración completa del mismo.

Información de resumen
- **Requisitos de seguridad**: usuarios de dominio
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Idifde.exe
  - Complemento Plantilla de certificados de MMC

Detalles de la tarea
Este procedimiento describe una manera sencilla de exportar un objeto de Active Directory correspondiente a una plantilla de certificados a un archivo. Este objeto podría a continuación volver a exportarse al directorio, si fuera necesario. Este método sólo guarda la información de LDAP del objeto de plantilla. Otra información, principalmente la de seguridad (como propiedad y permisos), no se conserva con este proceso.

Nota: la única forma totalmente admitida para realizar una copia de seguridad y restaurar objetos de Active Directory consiste en utilizar un método dedicado de copia de seguridad de directorios como la copia de seguridad del estado del sistema de Windows. Sin embargo, la restauración de una versión anterior de un objeto modificado requiere una restauración con autorización de Active Directory. Este procedimiento describe una forma sencilla de realizar una copia de seguridad y restaurar una instantánea de un objeto de plantilla de certificados.

Para exportar un objeto de plantilla de certificados

1. Especifique el nombre de la plantilla de la que desea realizar una copia de seguridad. No se trata necesariamente del mismo nombre para mostrar de la plantilla. Consulte las propiedades de plantilla en la ficha **General** de la plantilla (con el complemento Plantillas de certificados de MMC) para ver el **Nombre de la plantilla** y el **Nombre para mostrar plantilla**.

2. Inicie una sesión en un servidor miembro de dominio o en un controlador de dominio utilizando una cuenta de usuario de dominio.

3. Ejecute el siguiente comando para guardar los detalles de la plantilla en el archivo *templatename*.ldif y reemplace *templatename* por el nombre de la plantilla de certificados y *DC=woodgrovebank,DC=com* por el nombre de dominio (DN) de su bosque:

   ldifde -f *templatename*.ldif -d "cn=*templatename*, cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,*DC=woodgrovebank,DC=com*"

   Este comando se muestra en varias líneas; escríbalo en una sola.)

4. El archivo *templatename*.ldif se guardará en el directorio actual. Guarde el archivo *templatename*.ldif en una ubicación segura.

Importación de una plantilla de certificados a Active Directory
Cuando desee restaurar una plantilla desde una copia de seguridad, por ejemplo, para revertir una modificación no deseada de una plantilla, puede volver a importar una definición de plantilla de certificados guardada anteriormente a Active Directory.

Información de resumen
- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: ldifde.exe

Detalles de la tarea
Este procedimiento describe cómo restaurar una definición de plantilla de certificados desde archivo. El archivo se debe haber creado anteriormente mediante el procedimiento "Exportación de una plantilla de certificados desde Active Directory". Este método sólo restaura la información de LDAP del objeto de plantilla. Otra información, principalmente la información de seguridad (propiedad, permisos, etc.) no se conserva al utilizar este proceso.

Nota: la única forma totalmente admitida para realizar una copia de seguridad y restaurar objetos de Active Directory consiste en utilizar un método dedicado de copia de seguridad de directorios como la copia de seguridad del estado del sistema de Windows. Sin embargo, la restauración de una versión anterior de un objeto modificado requiere una restauración con autorización de Active Directory. Este procedimiento describe una forma sencilla de realizar una copia de seguridad y restaurar una instantánea de un objeto de plantilla de certificados.

No reemplaza la copia de seguridad y la restauración de Active Directory y sólo debe utilizarse en las circunstancias especiales mencionadas.

Para importar un objeto de plantilla de certificados

1. Recupere el archivo de definición de plantilla exportado que se creó en el procedimiento "Exportación de una plantilla de certificados desde Active Directory".
2. Inicie una sesión en un servidor miembro de dominio o en un controlador de dominio como miembro del grupo Administradores de PKI de empresa.
3. Si va a reemplazar una plantilla existente, realice una copia de seguridad de la plantilla no deseada (mediante el procedimiento anterior), anote los permisos de plantilla y, a continuación, elimínela.
4. Abra el archivo en el Bloc de notas (o un editor de textos similar) y busque comienza con "objectGUID:" al comienzo de una línea. La línea será similar a la siguiente, aunque los caracteres después de los dos puntos pueden ser distintos:

   GUID:: b/pVt//+I0i9hp8aJ7IWRg==
5. Elimine esta línea, procurando no realizar ningún otro cambio en el archivo y guárdelo.
6. Ejecute el siguiente comando para importar la plantilla a Active Directory desde el archivo *nombreplantilla*.ldif, reemplazando *nombreplantilla* por el nombre de la plantilla de certificados:

   ldifde -f *nombreplantilla*.ldif -i
7. Compruebe que el procedimiento haya funcionado abriendo Plantillas de certificados de MMC y viendo la plantilla restaurada.
8. Aplique a la plantilla restaurada los permisos registrados en el paso 3 o los que sean más adecuados para esta plantilla.

Supervisión y control de servicios

La supervisión del servicio permite al personal de operaciones observar la salud de un servicio de TI en tiempo real.

Cuando se hace referencia a MOM en esta sección, se asume que la implementación MOM que tiene sigue las instrucciones de la MOM Operations Guide. No se requiere MOM; sólo se utiliza como ilustración. Consulte la sección "Información adicional" que aparece al final de este capítulo para obtener más información acerca de la MOM Operations Guide.

División en categorías de las alertas de supervisión

El sistema de supervisión sólo debe mostrar las alertas más importantes al personal de operaciones. Si todos los errores menores se trasladan a un nivel superior para producir alertas de incidentes, el personal de operaciones se confundirá rápidamente en relación con lo que es urgente y lo que no lo es.

Información de resumen

- **Requisitos de seguridad**: ninguno
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**: consola de alertas operativa (como MOM)

Detalles de la tarea

En este capítulo, se utilizan las categorías de alerta siguientes. De ellas, sólo las tres primeras (Servicio no disponible, Infracción de seguridad y Error crítico) deben producir alertas en la consola del operador que requieran atención inmediata. Los errores y advertencias no se consideran urgentes y se deben dirigir al personal de soporte técnico operativo de PKI para su resolución. Estas categorías de sucesos son las predeterminadas que utiliza MOM y en las descripciones de tarea más adelante de esta sección se hará referencia a ellas.

Tabla 11.9: Categorías de alerta

Categoría de alerta	Descripción
Servicio no disponible	Cuando la aplicación o el componente está completamente no disponible.

Infracción de seguridad	Cuando se detecta un intruso o compromiso de seguridad en la aplicación.
Error crítico	Cuando la aplicación experimenta un error crítico que requiere una acción administrativa pronto (pero no inmediatamente). La aplicación o componente funciona con un nivel de rendimiento inferior, pero todavía puede realizar las operaciones más importantes.
Error	Cuando la aplicación experimente un problema transitorio que no necesita ninguna acción o resolución administrativa inmediata. La aplicación o componente funciona con un nivel de rendimiento aceptable y todavía puede realizar todas las operaciones más importantes.
Advertencia	Cuando la aplicación genera un mensaje de aviso que no necesita ninguna acción o resolución administrativa inmediata. La aplicación o componente funciona con un nivel de rendimiento aceptable y todavía puede realizar todas las operaciones más importantes. Sin embargo, esta situación podría convertirse en Error, Error crítico o Servicio no disponible si el problema continúa.
Información	Cuando la aplicación genera un evento informativo. La aplicación o componente funciona con un nivel de rendimiento aceptable y realiza todas las operaciones importantes y secundarias.
Correcto	Cuando la aplicación genera un evento de éxito. La aplicación o componente funciona con un nivel de rendimiento aceptable y realiza todas las operaciones importantes y secundarias.

Supervisión de restricciones de capacidad de Servicios de Certificate Server

La detección de las restricciones de la capacidad potencial resulta esencial para mantener el servicio a un nivel óptimo. A medida que los subsistemas se aproximan a los límites de sus capacidades operativas, el rendimiento se reduce drásticamente (normalmente, de forma no lineal). En consecuencia, es importante supervisar las tendencias de capacidad e identificarlas para hacer frente a restricciones futuras lo más pronto posible.

Información de resumen

- **Requisitos de seguridad**: el permiso necesario lo indica la solución de supervisión
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Monitor del sistema
  - Consolidador de contador de rendimiento (como MOM)
  - Consola de alertas operativa (como MOM)
  - Herramientas de planeamiento de capacidad

Detalles de la tarea

Los siguientes contadores de rendimiento son los más útiles para la identificación de restricciones de capacidad en Servicios de Certificate Server. El procesador y el disco físico son dos de los recursos más utilizados por Servicios de Certificate Server y probablemente indicarán restricciones antes que la interfaz de red o la memoria.

Tabla 11.10: Principales contadores de supervisión de capacidad para Servicios de Certificate Server

Objeto de rendimiento	Contador de rendimiento	Instancia
Procesador	% de tiempo de procesador	_Total
Disco físico	% Tiempo de disco	_Total
Disco físico	Long. promedio de cola de lectura	_Total

	de disco	
Disco físico	Long. promedio de cola de escritura de disco	D: (base de datos de CA) C: (registro de CA)
Interfaz de red	Total de bytes/s.	Adaptador NW
Memoria	% de bytes asignados en uso	–––

Para obtener más información general acerca de las restricciones de capacidad y los contadores de rendimiento relacionados, consulte la referencia en la sección "Información adicional" al final de este capítulo.

También resulta esencial supervisar los indicadores de capacidad en cualquier infraestructura auxiliar. Los elementos clave son:

- **Comunicaciones de Servicios de Certificate Server con Active Directory**. Las entidades emisoras de certificados de empresa utilizan Active Directory para los servicios de autenticación y autorización, la lectura y el almacenamiento de información de configuración de entidad emisora de certificados y PKI y, según el tipo de certificado, la publicación de certificados emitidos en el directorio.
- **Comunicaciones con Active Directory relacionadas con certificados cliente**. Los clientes leen la información de CA y de PKI de Active Directory. Esta actividad incluye descargar listas CRL que pueden tener un tamaño de varios megabytes, por cliente y por semana.
- **Comunicaciones con servidores Web relacionadas con certificados cliente**. Los clientes pueden recuperar listas CRL y certificados de entidad emisora del servidor Web, aunque no es probable que esta actividad produzca una carga que origine restricciones de capacidad, a menos que el servidor ya esté muy cargado.

Supervisión del estado y la disponibilidad de Servicios de Certificate Server

Generalmente, las entidades emisoras de certificados no suministran servicios en línea o en tiempo real (en comparación con servicios como Active Directory o Microsoft SQL Server&™, por ejemplo, que deben estar en línea continuamente para suministrar un servicio útil.) Sin embargo, varios aspectos del funcionamiento de entidad emisora de certificados son fundamentales y requieren una respuesta en línea del servicio:

- **Disponibilidad de información de revocación**. Una lista CRL actual debe estar disponible para todo usuario de un certificado que desee comprobar el estado de revocación de dicho certificado.
- **Validad del certificado de entidad emisora**. Una entidad emisora de certificados debe tener un certificado que sea válido actualmente. Un certificado de entidad emisora no válido impide la validación de todo certificado emitido por dicha entidad emisora de certificados o sus niveles secundarios. También impide la emisión de nuevos certificados.
- **Disponibilidad de un servicio de inscripción de certificados**. Nadie puede inscribir o renovar un certificado si el servicio de entidad emisora de certificados no se encuentra disponible.

La falta de disponibilidad de alguno de los dos primeros aspectos normalmente tiene un mayor impacto que los últimos.

Información de resumen

- **Requisitos de seguridad:** administrador de MOM (o sistema de supervisión)
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Secuencias de comandos MSS
  - Consola de alertas operativa (como MOM o una infraestructura de correo electrónico)
  - Agentes de MOM o Servicio del programador de tareas de Windows para la ejecución

Detalles de la tarea

Los sucesos incluidos en la siguiente tabla son los sucesos más importantes para los Servicios de Certificate Server. En la tabla se describe la importancia de cada tipo de suceso y la gravedad de alerta (para la consola operativa) que se debe asignar a dicho suceso. En la segunda tabla se enumeran los métodos de detección de estas incidencias; la mayoría se detectan con las secuencias de comandos operativas suministradas con esta solución.

La columna Gravedad se relaciona con las categorías de alerta definidas anteriormente en el procedimiento "División en categorías de las alertas de supervisión".

Tabla 11.11: Gravedad de los principales sucesos de Servicios de Certificate Server

Estado de Servicios de Certificate Server	Importancia	Gravedad
Lista CRL caducada	No se puede obtener acceso a una lista CRL válida; esta situación está provocando actualmente una pérdida de servicio.	Servicio no disponible
Lista CRL atrasada	La lista CRL aún es válida pero una lista CRL nueva que debería haberse publicado está atrasada.	Crítico
Lista CRL no disponible Sucesos secundarios: No se puede recuperar la lista CRL de Active Directory No se puede recuperar la lista CRL del servidor Web	Una lista CRL no se encuentra disponible en un punto de distribución de la lista CRL publicada. Esta situación puede originar una pérdida de servicio.	Crítico
Error del servidor de entidad emisora de certificados	El servidor no es visible en la red.	Servicio no disponible
Estado crítico del sistema operativo de entidad emisora de certificados	Se ha producido un problema grave subyacente con el hardware del servidor o Windows.	Crítico
Estado de error/advertencia del sistema operativo de entidad emisora de certificados	Se han producido problemas subyacentes con el hardware del servidor o Windows que no son muy importantes.	Error o advertencia (según lo definido por las reglas de MOM)
Servicios de Certificate Server está sin conexión Sucesos secundarios: La interfaz de cliente está sin conexión La interfaz de administrador está sin conexión	La interfaz de llamadas a procedimiento remoto (RPC) de Servicios de Certificate Server está sin conexión y los certificados no pueden emitirse.	Crítico
Certificado de entidad emisora caducado Sucesos secundarios: Este certificado de entidad emisora ha caducado La entidad emisora de certificados principal ha caducado	El certificado de la entidad emisora ha caducado. Esta situación provoca actualmente una pérdida de servicio.	Servicio no disponible
Al certificado de entidad emisora le queda menos de un mes de validez	El certificado de entidad emisora pronto caducará, problema que originará la pérdida del servicio si no	Error

	se corrige. Sólo se emiten los certificados con una duración muy breve.	
La validez del certificado de entidad emisora ha llegado a la mitad de su duración	Un certificado de entidad emisora debe renovarse al alcanzar la mitad de su período de validez. Esto podría significar que se están emitiendo certificados de menor duración que la prevista.	Advertencia
Error en la copia de seguridad de entidad emisora de certificados	Error en la copia de seguridad del estado del sistema de entidad emisora de certificados; posible pérdida de información.	Importante o Error

Puede utilizar la secuencia de comandos suministrada (ca_monitor.wsf en la siguiente tabla) para comprobar estos sucesos. La secuencia de comandos tiene lógica para escribir elementos de suceso en el registro de aplicación de Windows cuando se produce cualquier error detectado. Posteriormente, los agentes de MOM, u otra solución de supervisión, pueden anotar estos sucesos. Tendrá que configurar reglas de filtrado para comprobar el origen del suceso y los Id. de suceso producidos por las secuencias de comandos enumeradas en la siguiente tabla.

Las secuencias de comandos también pueden enviar un mensaje de correo electrónico en respuesta a condiciones de alerta. Cuando se utiliza MOM (u otro sistema de supervisión basado en un agente), el agente cliente de MOM debe ejecutar las secuencias de comandos. Si no hay un agente de administración que pueda ejecutar la secuencia de comandos, utilice el programador de tareas de Windows para ejecutar estas comprobaciones cada hora como mínimo. Las alertas se pueden enviar por correo electrónico o se puede utilizar una herramienta de supervisión de registros de sucesos.

Las secuencias de comandos están diseñadas para ejecutarse en la entidad emisora de certificados en línea, aunque también comprueban el estado de certificados y listas CRL publicados desde entidades emisoras de certificados principales sin conexión hasta la entidad emisora raíz. En la siguiente tabla se muestran los Id. de suceso generados por la secuencia de comandos de supervisión, donde corresponda. La sintaxis de la secuencia de comandos se muestra después de la tabla.

Tabla 11.12: Secuencias de comandos de supervisión de Servicios de Certificate Server

Evento	**Secuencia de comandos o método de detección**	**Origen eId. de suceso**
Lista CRL caducada	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCRLs	Operaciones de CA 20
Lista CRL atrasada	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCRLs	Operaciones de CA 21
Lista CRL no disponible Sucesos secundarios: No se puede recuperar la lista CRL de Active Directory No se puede recuperar la lista CRL del servidor Web	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCRLs	Operaciones de CA 22 23
Error del servidor de entidad emisora de certificados	Detección de error en el servidor MOM nativo	
Estado crítico del sistema operativo de entidad emisora de certificados	Control de estado del servidor MOM nativo	

Estado de error/advertencia del sistema operativo de entidad emisora de certificados	Control de estado del servidor MOM nativo	
Servicios de Certificate Server está activo Sucesos secundarios: La interfaz de cliente está sin conexión La interfaz de administrador está sin conexión	Secuencia de comandos: Ca_monitor.wsf Trabajo: IsCAAlives	Operaciones de CA 1 2
Certificado de entidad emisora caducado Sucesos secundarios: Este certificado de entidad emisora ha caducado La entidad emisora de certificados principal ha caducado	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCACerts	Operaciones de CA 10
Al certificado de entidad emisora le queda menos de un mes de validez	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCACerts	Operaciones de CA 11
La validez del certificado de entidad emisora ha llegado a la mitad de su duración	Secuencia de comandos: Ca_monitor.wsf Trabajo: CheckCACerts	Operaciones de CA 12
Copia de seguridad bloqueada (la secuencia de comandos de la copia de seguridad no pudo ejecutarse porque aún se encontraba presente un archivo de bloqueo de la copia de seguridad anterior)	Secuencia de comandos: Ca_operations.wsf Trabajo: BackupCADatabase	Operaciones de CA 30
Error en la copia de seguridad de entidad emisora de certificados	El código de error de NTBackup.exe se proporciona aquí, aunque debe basarse en las capacidades de MOM o de otro sistema de supervisión para recibir advertencias sobre problemas de copia de seguridad. (Tenga en cuenta que necesitará comprobar la copia de seguridad del estado del sistema y la copia de seguridad de la organización.)	Ntbackup 8019
Otros sucesos	Error de ejecución de Ca_monitor.wsf	Operaciones de CA 100

Antes de implementar las secuencias de comandos, actualice el archivo constants.vbs con los parámetros de alerta correctos. Aquí se muestran las secciones pertinentes del archivo y los elementos que puede cambiar se muestran en cursiva:

```
'Alerting parameters
CONST ALERT_EMAIL_ENABLED = FALSE'set to true/false to enable/disable email
CONST ALERT_EVTLOG_ENABLED= TRUE'set to true/false to enable/disable event
'log entries
' set to comma-separated list of recipients to get email alerts
CONST ALERT_EMAIL_RECIPIENTS= "Admin@woodgrovebank.com,Ops@woodgrovebank.com"
'SMTP host to use
CONST ALERT_EMAIL_SMTP= "mail.woodgrovebank.com"
```

```
'String used as the Source in event log events
CONST EVENT_SOURCE= "MSS Tools"
CONST CA_EVENT_SOURCE= "CA Operations"

'CA Event IDs
CONST CA_EVENT_CS_RPC_OFFLINE=1
CONST CA_EVENT_CS_RPC_ADMIN_OFFLINE=2
CONST CA_EVENT_CA_CERT_EXPIRED=10
CONST CA_EVENT_CA_CERT_NEARLY_EXPIRED=11
CONST CA_EVENT_CA_CERT_RENEWAL_DUE=12
CONST CA_EVENT_CRL_EXPIRED=20
CONST CA_EVENT_CRL_OVERDUE=21
CONST CA_EVENT_CRL_NOT_AVAILABLE_LDAP=22
CONST CA_EVENT_CRL_NOT_AVAILABLE_HTTP=23
CONST CA_EVENT_BACKUP_LOCKED=30
CONST CA_EVENT_CA_OTHER=100
```

Es necesario especificar si desea que los errores produzcan mensajes de correo electrónico, entradas de registro de sucesos o ambos. El valor predeterminado es que sólo se produzcan entradas de registro de sucesos. Si especifica alertas de correo electrónico, *debe* suministrar una lista válida de destinatarios de correo electrónico (separados por comas) y el nombre de host de SMTP o la dirección de IP. Ambas cadenas deben estar entre comillas.

Si especifica una alerta de registro de sucesos, quizás desee cambiar los parámetros CA_EVENT_SOURCE (utilizado para todos los sucesos relacionados con la entidad emisora de certificados) o EVENT_SOURCE (utilizado para sucesos no relacionados con la entidad emisora de certificados).

La sintaxis y el uso de las secuencias de comandos de supervisión se describen en la siguiente sección.

Para comprobar la caducidad del certificado de entidad emisora

Ejecute el siguiente comando para comprobar el certificado de la entidad emisora (donde se ejecuta la secuencia de comandos) y los certificados publicados de cualquier entidad emisora principal hasta la jerarquía de la entidad emisora raíz.

Cscript //job:CheckCACerts C:\MSSScripts\ca_monitor.wsf

Este comando proporciona alertas en las condiciones siguientes:

- El certificado de entidad emisora ha caducado (Id. de suceso 12)
- Al certificado de entidad emisora le queda menos de un mes de validez (Id. de suceso 11)
- El certificado de entidad emisora ha pasado el punto intermedio de su período de validez (Id. de suceso 12)

Para comprobar la caducidad de la lista CRL

Ejecute el siguiente comando para comprobar la lista CRL de entidad emisora y las listas CRL publicadas para todas las entidades emisoras principales hasta la entidad emisora raíz.

Cscript //job:CheckCRLs C:\MSSScripts\ca_monitor.wsf

Este comando proporciona alertas en las condiciones siguientes:

- La lista CRL ha caducado (Id. de suceso 20)
- La lista CRL ha superado su fecha de "Siguiente lista CRL publicada" y su validez ha caducado (Id. de suceso 21)
- La lista CRL no puede recuperarse desde el CDP de LDAP (Id. de suceso 22)
- La lista CRL no puede recuperarse desde el CDP de HTTP (Id. de suceso 23)

Actualmente, los CDP de FTP y FILE no se comprueban en esta secuencia de comandos.

Para comprobar que el servicio CA está en ejecución

Ejecute el siguiente comando para comprobar la entidad emisora en la que se ejecuta la secuencia de comandos.

Cscript //job:IsCAAlive C:\MSSScripts\ca_monitor.wsf

Este comando proporciona alertas en las condiciones siguientes:

- La Interfaz cliente de RPC de entidad emisora de certificados no responde (Id. de suceso 1)
- La Interfaz de administración de RPC de entidad emisora de certificados no responde (Id. de suceso 2)

Supervisión de seguridad de la entidad emisora de certificados
Los Servicios de Certificate Server producen distintas entradas de registro de auditoría en respuesta a diferentes sucesos de seguridad. La mayoría de estas entradas serán el resultado de tareas operativas diarias. Sin embargo, algunos sucesos indican cambios de configuración importantes y quizás sea necesario estudiarlos más detenidamente.

Información de resumen
- **Requisitos de seguridad**:
  - Auditores de entidad emisora de certificados (para revisar el registro de seguridad)
  - Cuenta de supervisión de seguridad designada para supervisión a través de MOM (o sistema similar)
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Consola de alertas operativa (como MOM)
  - Visor de eventos
  - Eventquery.vbs (herramienta de la línea de comandos de Windows)

Detalles de la tarea
La siguiente tabla enumera los sucesos de auditoría que producen los Servicios de Certificate Server, junto con una categorización de alerta recomendada. Configure su sistema de supervisión para buscar estos sucesos y mostrar el nivel de alerta correcto. Alternativamente, si no tiene un sistema de supervisión de sucesos centralizado, revise los registros de seguridad del servidor de entidad emisora periódicamente (si es posible, diariamente) para comprobar estos elementos.
La categoría de alerta predeterminada para los sucesos Correctos es **Información**. Los sucesos Correctos que se originen a partir de probables cambios en la configuración de seguridad de la entidad emisora de certificados se consideran como una **advertencia**. Todos los sucesos con nivel de **advertencia** indican sucesos significativos que generalmente no se producirán en las operaciones diarias. Todos los sucesos de **advertencia** deben correlacionarse con una solicitud de cambio aprobada. Si no se produce dicha correlación, considere el suceso como un posible error de seguridad e investíguelo inmediatamente.

Los sucesos **erróneos** generalmente no se producen durante las operaciones diarias o durante los cambios estándar realizados en la entidad emisora de certificados. La gran mayoría de los sucesos erróneos son significativos y requieren investigación (aunque quizás sólo indiquen una asignación de permiso incorrecta más que un ataque malintencionado).

Nota: hay unas pocas excepciones, como el Suceso 792, donde **Servicios de Certificate Server rechaza una solicitud de certificado**. Esta situación produce sucesos correctos y erróneos para una solicitud legítimamente rechazada por un administrador de certificados, pero sólo un suceso erróneo cuando una persona sin permiso suficiente intenta realizar un rechazo de solicitud.

Las excepciones adicionales a la lista de la siguiente tabla se deben a las distintas formas en que se pueden efectuar cambios en la entidad emisora. Los sucesos 789 (cambio de filtro de auditoría) y 795 y 796 (cambio de la configuración o propiedad de entidad emisora) sólo se registrarán si se efectúan cambios mediante el complemento Entidad emisora de certificados de MMC. No se registrarán si algún usuario intenta editar el Registro de la entidad emisora directamente (o utiliza el comando certutil -setreg) para cambiar los valores de configuración de la entidad emisora. En su lugar, estos sucesos se registran como errores de auditoría de acceso al objeto Suceso 560 (consulte la última entrada en la siguiente tabla). La auditoría se encuentra activada para las

subclaves de configuración de Registro de entidad emisora de certificados y registra los cambios correctos y todos los accesos erróneos. Para realizar un seguimiento de las claves del Registro de la entidad emisora, utilice el parámetro **Nombre de objeto** del suceso de auditoría junto con **Id. de suceso** y **Tipo de suceso** para crear un filtro con el fin de producir las alertas correctas.

Además de auditar los sucesos de Servicios de Certificate Server, también debe supervisar y generar alertas de los sucesos de seguridad del sistema operativo estándar, como los sucesos de inicio de sesión, el uso de privilegios y los accesos a objeto. El registro y la base de datos de entidad emisora y los directorios de registro se configuran para generar alertas para todos los accesos erróneos y los cambios correctos. También debe considerar el establecimiento de auditoría en el contenedor de los Servicios de claves públicas (en Configuración\Servicios) y en los grupos de administración de PKI. Estas opciones no se han establecido como parte de esta solución debido a la dificultad de supervisar sucesos de auditoría distribuidos entre diferentes controladores de dominio. Si dispone de un sistema (como MOM) que pueda consolidar y filtrar estos registros, habilite la auditoría en todos los objetos y contenedores de administración y configuración de PKI de Active Directory.

Nota: la supervisión de seguridad en el sistema operativo de entidad emisora se encuentra fuera del alcance de esta guía y puede incluir la administración de sucesos de seguridad de agentes especializados en la detección de intrusiones. Si alguno de estos orígenes indica una infracción de seguridad, investigue exhaustivamente los sucesos de auditoría de la entidad emisora de certificados junto con el resultado de estos orígenes.

Las categorías de alerta Correcto y Erróneo de la siguiente tabla se relacionan con las categorías de alerta definida en el procedimiento "División en categorías de las alertas de supervisión".

Tabla 11.13: Sucesos de auditoría de Servicios de Certificate Server

Id. de suceso	Descripción del suceso	Categoría de alerta Correcto	Categoría de alerta Erróneo
772	El administrador de certificados rechazó una solicitud de certificado pendiente	Advertencia	Error
773	Servicios de Certificate Server recibió una solicitud de certificado reenviada	Advertencia	Error
774	Servicios de Certificate Server revocó un certificado	Información	Error
775	Servicios de Certificate Server recibió una solicitud de publicación de la lista de revocación de certificados (CRL)	Información	Advertencia
776	Servicios de Certificate Server publicó la lista de revocación de certificados (CRL)	Información	Error
777	Cambio en una extensión de solicitud de certificado	Información	Error
778	Cambio en uno o varios de los atributos de solicitudes de certificados	Información	Error
779	Servicios de Certificate Server recibió una solicitud de cierre	Advertencia	Error
780	Se inició la copia de seguridad de Servicios de Certificate Server	Información	–
781	Se completó la copia de seguridad de Servicios de Certificate Server	Información	–
782	Se inició la restauración de Servicios de Certificate Server	Advertencia	–
783	Se completó la restauración de Servicios de Certificate Server	Advertencia	–
784	Se inició Servicios de Certificate Server	Información	–

785	Se detuvo Servicios de Certificate Server	Advertencia	–
786	Cambio en los permisos de seguridad de Servicios de Certificate Server	Advertencia	Error
787	Servicios de Certificate Server recuperó una clave archivada	Información	Error
788	Servicios de Certificate Server importó un certificado a su base de datos	Información	Advertencia
789	Cambio en el filtro de auditoría de Servicios de Certificate Server	Advertencia	Error
790	Servicios de Certificate Server recibió una solicitud de certificado	Información	Error
791	Servicios de Certificate Server aprobó una solicitud de certificado y emitió un certificado	Información	Error
792	Servicios de Certificate Server denegó una solicitud de certificado	Advertencia	
793	Servicios de Certificate Server ha establecido el estado de una solicitud de certificado en Pendiente	Información	
794	Cambio en la configuración del administrador de certificados correspondiente a Servicios de Certificate Server	Advertencia	
795	Cambio en una entrada de configuración de Servicios de Certificate Server	Advertencia	Error
	Nodo: Entrada: CRLPeriod, CRLPeriodUnits, CRLDeltaPeriod o CRLDeltaPeriodUnits Describa el cambio en el programa de publicación de la lista CRL. El valor 0 para CRLDeltaPeriodUnits significa que la publicación de diferencias entre listas CRL se encuentra deshabilitada.		
	Nodo: PolicyModules\CertificateAuthority_Microsoft Default.Policy Entrada: RequestDisposition Valor: 1 Establezca la entidad emisora para emitir solicitudes entrantes a menos que se especifique lo contrario.		
	Nodo: PolicyModules\CertificateAuthority_Microsoft Default.Policy Entrada: RequestDisposition Valor: 257 Establezca la entidad emisora para mantener las solicitudes entrantes como solicitudes pendientes.		
	Nodo: ExitModules\CertificateAuthority_Microsoft Default.Exit Entrada: PublishCertFlags Valor: 1 Permita que los certificados se publiquen en el sistema de archivos.		

	Nodo: ExitModules\CertificateAuthority_Microsoft Default.Exit Entrada: PublishCertFlags Valor: 0 No permita que los certificados se publiquen en el sistema de archivos.		
	Nodo: ExitModules Entrada: Active Cambio en módulo de salida activo. El valor especifica el nombre del módulo nuevo. Un valor en blanco significa ninguno.		
	Nodo: PolicyModules Entrada: Active Cambio en el módulo de directiva activo. El valor especifica el nombre del módulo nuevo.		
	Nodo: Entrada: CRLPublicationURLs Cambio en los CDP o AIA. El valor especifica el conjunto resultante de los CDP	Nodo: Entrada: CACertPublicationURLs Cambio en los AIA o CDP. El valor especifica el conjunto resultante de los AIA	
796	Cambio en una propiedad de Servicios de Certificate Server (consulte los subtipos incluidos a continuación).	Advertencia	Error
	Tipo: 4 Adición/eliminación de una plantilla a/de una entidad emisora. El valor es una lista de las plantillas resultantes por nombre y OID.		
	Tipo: 3 Adición de un certificado de KRA a la entidad emisora. El valor es la representación Base64 del certificado.		
	Tipo: 1 Eliminación del certificado de KRA de la entidad emisora. El valor es el recuento total de certificados de KRA.		
	Tipo: 1 Adición/eliminación de un número de certificados de KRA que se utilizarán para el almacenamiento de claves. El valor es el número resultante de los certificados que se van a utilizar.		
797	Los Servicios de Certificate Server archivaron una clave.	Información	–
798	Los Servicios de Certificate Server importaron y archivaron una clave.	Información	–
799	Los Servicios de Certificate Server publicaron el certificado de entidad emisora en Active Directory.	Información	
800	Se han eliminado una o varias filas de la base de datos de certificados.	Advertencia	Error
801	Separación de funciones activada.	Advertencia	Error

560	Acceso a objetos donde: Tipo de objeto: **Clave** Nombre de objeto: **\REGISTRY\MACHINE\SYSTEM\ ControlSet001\Services\CertSvc\Configuration**	Información	Error

Configuración de alertas de SMTP para solicitudes de certificados pendientes

Si tiene algunos tipos de certificado configurados para requerir la aprobación del administrador de certificados, quedarán en la cola de la carpeta Solicitudes pendientes (del complemento Entidad emisora de certificados de MMC) hasta que la solicitud se apruebe. Quizás desee configurar que se envíen alertas por correo electrónico cada vez que una solicitud se coloque en la cola. Las solicitudes aprobadas automáticamente no enviarán alertas de correo electrónico.

Las alertas de correo electrónico también pueden configurarse para otros sucesos de entidad emisora. Los documentos de la ayuda en pantalla de Servicios de Certificate Server proporcionan información acerca de cómo configurarlos.

Información de resumen

- **Requisitos de seguridad**: Administradores de CA
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Editor de texto
  - Servidor SMTP y buzón del destinatario

Detalles de la tarea

Los valores del servidor SMTP y la lista de destinatarios SMTP configurados en el archivo constants.vbs y utilizados por este procedimiento también se emplean en las alertas SMTP descritas en el procedimiento "Supervisión del estado y la disponibilidad de Servicios de Certificate Server". Si tiene que utilizar otras opciones para el servidor y los destinatarios SMTP para estos dos procedimientos, puede cambiar los valores en constants.vbs temporalmente y, a continuación, ejecutar este procedimiento actual. La secuencia de comandos de este procedimiento guarda estos valores en el Registro de la entidad emisora. Una vez ejecutado, el archivo constants.vbs se puede volver a cambiar a los valores anteriores que utilizará la secuencia de comandos de supervisión del procedimiento "Supervisión del estado y la disponibilidad de Servicios de Certificate Server". (La opción para habilitar o deshabilitar las alertas de correo electrónico en dicho procedimiento, ALERT_EMAIL_ENABLED, no tiene efecto alguno en las alertas de este procedimiento.)

Para habilitar las alertas de correo electrónico para solicitudes pendientes

1. Configure los valores correctos para los destinatarios de correo electrónico y el servidor SMTP en el archivo de secuencias de comandos C:\MSSScripts\constants.vbs:

```
'Alerting parameters
' set to comma-separated list of recipients to get email alerts
CONST ALERT_EMAIL_RECIPIENTS= "Admin@woodgrovebank.com,
PKIOps@woodgrovebank.com"
CONST ALERT_EMAIL_SMTP= "mail.woodgrovebank.com" 'SMTP host to use
```

   Nota: la línea con sangría de este extracto de archivo es la continuación de la línea anterior, que se ha ajustado a la siguiente línea para su presentación; debe estar en una sola línea en el archivo.

2. Ejecute el comando siguiente para habilitar las alertas de correo electrónico para las solicitudes pendientes en cola:

   cscript //job:SetupSMTPAlerts C:\MSSScripts\ca_monitor.wsf

Programación de trabajos

La programación de trabajos consiste en la organización continua de trabajos y procesos en la secuencia más efectiva, maximizando el rendimiento y la utilización del sistema para cumplir con los requisitos del contrato de nivel de servicio (SLA). La programación de trabajos está estrechamente ligada a la supervisión y control del servicio, así como a la administración de la capacidad.

Programación de trabajos en la entidad emisora

Es necesario ejecutar una determinada cantidad de tareas repetitivas en las entidades emisoras para mantener el correcto funcionamiento de la infraestructura de Servicios de Certificate Server. Estas tareas se automatizan para reducir la sobrecarga operativa.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**:
  - Programador de tareas de Windows
  - MOM (si corresponde)

Detalles de la tarea

En la siguiente tabla se enumeran los trabajos automatizados que se ejecutan en la entidad emisora. Estos trabajos están definidos en tareas de otras partes de este capítulo (mostradas en la columna **Tarea de referencia**); la tabla siguiente únicamente es de referencia.

Sólo la entidad emisora tiene trabajos automatizados en ejecución. La entidad emisora raíz puede estar apagada durante períodos largos, por lo que no se puede mantener una programación confiable en este equipo.

Tabla 11.14: Lista de trabajos programados en la entidad emisora

Descripción del trabajo	Programación	Ejecutado por	Tarea de referencia
Copia de seguridad del Estado del sistema de la entidad emisora al archivo	Diariamente	Programador de tareas de Windows	Configuración y ejecución de una copia de seguridad de la base de datos de entidad emisora Configuración y ejecución de una copia de seguridad de la base de datos de entidad emisora raíz
Copia de seguridad de archivos de la entidad emisora para almacenamiento de copias de seguridad	Diariamente (a continuación de la copia de seguridad del Estado del sistema)	Programador de copias de seguridad organizativas	Ninguno (definido por su organización)
Publicación de listas CRL en IIS	Cada hora	Programador de tareas de Windows	Publicación de la entidad emisora y el certificado en IIS
Supervisión del estado de la entidad emisora en línea	Cada hora	MOM o Programador de tareas de Windows	Supervisión del estado y la disponibilidad de Servicios de Certificate Server
Supervisión del estado de emisión y publicación de la lista CRL	Cada hora	MOM o Programador de tareas de Windows	Supervisión del estado y la disponibilidad de Servicios de Certificate Server
Supervisión de la validez del certificado de entidad emisora	Diariamente	MOM o Programador de tareas de Windows	Supervisión del estado y la disponibilidad de Servicios de Certificate Server

Tareas operativas adicionales

El mantenimiento de una PKI implica numerosas tareas operativas. Normalmente no es necesario realizar muchas de estas tareas de forma periódicamente, pero pueden ser necesarias ocasionalmente o como parte de la resolución de una incidencia de soporte técnico.

En la documentación del producto Servicios de Certificate Server de Windows Server 2003 se describen varias de estas tareas y se proporciona información general acerca de la administración. Muchas de estas tareas no se describen en este capítulo ni en el capítulo de la guía de generación adjunta ("Implementación de la infraestructura de claves públicas"). Aunque la tarea se describa en esta guía de solución, la documentación del producto proporciona información complementaria que resulta útil.

Consulte la sección "Información adicional" al final de este capítulo para obtener un vínculo al documento, donde podrá encontrar instrucciones para realizar las siguientes tareas administrativas:

- Iniciar o detener el servicio de la entidad emisora de certificados.
- Establecer permisos de seguridad y delegar el control de una entidad emisora de certificados.
- Ver el certificado de la entidad emisora de certificados.
- Establecer la seguridad para el acceso a las páginas Web de la entidad emisora de certificados.
- Configurar las restricciones del administrador de certificados.
- Publicar los certificados en un bosque externo de Active Directory.
- Enviar mensajes de correo electrónico cuando se produce un suceso de certificación.
- Utilizar el complemento Entidad emisora de certificados.
- Administrar la revocación de certificados.
- Administrar las solicitudes de certificados en una entidad emisora de certificados autónoma.
- Administrar plantillas de certificados para una entidad emisora de certificados de empresa.
- Administrar el archivo y la recuperación de claves.
- Cambiar la configuración de directivas para una entidad emisora de certificados.
- Cambiar la directiva o salir de módulos de una entidad emisora de certificados.
- Controlar la administración basada en funciones.

Principio de la página

Tareas del cuadrante de compatibilidad

Las SMF del cuadrante de compatibilidad incluyen tareas reactivas y preventivas para mantener los niveles de servicio deseados. Las funciones reactivas dependen de la capacidad de la organización para reaccionar y resolver incidentes y problemas rápidamente. Las funciones preventivas más interesantes intentan evitar interrupciones en el servicio. Mediante una buena supervisión de los servicios de la solución con los umbrales predefinidos, estas funciones identifican los problemas antes de que se vean afectados los niveles de servicio. Esto proporciona al personal de operaciones el tiempo suficiente para reaccionar y resolver problemas potenciales.

El cuadrante de compatibilidad está estrechamente relacionado con la SMF de control y supervisión de servicios que se describe en el cuadrante operativo. El control y supervisión de servicios proporciona la información esencial mediante la que el personal de operaciones y de soporte puede detectar los problemas. Los procedimientos descritos en esta sección están diseñados para solucionar las incidencias más comunes que se pueden producir y permiten recuperarse de ellas.

Esta sección contiene información relevante para la siguiente función de administración de servicios:

- Administración de incidentes

No hay tareas que correspondan al resto de las SMF:

- Administración de problemas (el diagnóstico de problemas se describe en la sección "Solución de problemas" más adelante en este capítulo)
- Soporte técnico del servicio

  Nota: cada descripción de tarea incluye la siguiente información de resumen: requisitos de seguridad, frecuencia y requisitos de tecnología.

Administración de incidentes

La administración de incidentes es el proceso de administración y control de errores e interrupciones en el uso o implementación de servicios de TI a partir de su informe por parte de clientes o asociados de TI. El objetivo principal de la administración de incidentes consiste en restaurar el funcionamiento normal del servicio tan rápido como sea posible, minimizar el impacto adverso sobre las operaciones de negocio y garantizar el mantenimiento de la mayor calidad y disponibilidad posibles de los niveles de servicio. El "funcionamiento normal del servicio" se define como el funcionamiento del servicio dentro de los límites del SLA.

Esta sección está estrechamente relacionada con "Solución de problemas". No obstante la sección "Solución de problemas" implica la identificación y diagnóstico de los problemas, mientras que esta sección contiene las tareas más comunes utilizadas para solucionar estos problemas.

Los incidentes que se analizan en la sección "Solución de problemas" son:

- El servidor no responde
- Error en la publicación de la lista CRL
- Lista CRL no emitida
- El cliente no puede inscribirse
- Se ha instalado una actualización de seguridad que requiere reinicio
- Error de servidor permanente
- Debe revocarse el certificado huérfano
- El servidor no puede restaurarse a tiempo para la emisión de la lista CRL o el certificado
- El certificado de entidad final ha quedado comprometido
- El certificado de la entidad emisora ha quedado comprometido
- El certificado de la entidad emisora raíz ha quedado comprometido

La mayoría de dichos incidentes se relacionan directamente con uno o más de los procedimientos detallados en las siguientes secciones. En otros casos, como por ejemplo un error en la inscripción de un cliente, el proceso de respuesta a incidentes requerido es más complejo y se describe en la sección "Solución de problemas".

Reinicio de Servicios de Certificate Server

Debe reiniciar Servicios de Certificate Server por diversas razones operativas. (Por ejemplo, después de reconfigurar varias propiedades de la entidad emisora, deberá reiniciar Servicios de Certificate Server para que los cambios tengan efecto.) En algunos casos, quizás sea necesario reiniciar Servicios de Certificate Server si el servicio ha dejado de responder o funciona en forma imprevista.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: según sea necesario

- **Requisitos de tecnología**:
  - Complemento Entidad emisora de certificados de MMC
  - Net.exe

Detalles de la tarea
Hay numerosos métodos para reiniciar un servicio y todos son aceptables para esta tarea.

Para reiniciar el servicio de la entidad emisora

1. Compruebe que no haya nadie realizando una transacción con la entidad emisora. Si dispone del tiempo necesario, envíe un aviso a los usuarios que puedan verse afectados.
2. En la MMC de Entidad emisora de certificados, seleccione el objeto CA.
3. En el menú **Tareas**, haga clic en **Detener servicio** o, en un símbolo del sistema, escriba:

   net stop "Certificate Services"
4. En el menú **Tareas**, haga clic en **Iniciar servicio** o, en un símbolo del sistema, escriba:

   net start "Certificate Services"

   Nota: cuando la auditoría está habilitada, es posible que Servicios de Certificate Server tarde bastante en cerrarse e iniciarse de nuevo. Puede tardar más de 10 minutos si se trata de una base de datos muy grande. El uso de la característica de auditoría prolongará todo el proceso de cierre e inicio del servidor, ya que Servicios de Certificate Server debe calcular un valor hash de toda la base de datos para crear entradas de auditoría de inicio y cierre. Este retardo no se produce si no se auditan el inicio ni el cierre.

Reinicio del servidor de la entidad emisora
Es posible que tenga que reiniciar el servidor de entidad emisora por varios motivos operativos, incluida la aplicación de una actualización del sistema operativo. Es posible que también tenga que reiniciar el servidor si el servicio ha dejado de responder o se comporta de un modo imprevisto y no se reinicia de un modo limpio mediante el procedimiento Reinicio del servicio.

Información de resumen
- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Net.exe

Detalles de la tarea
Para reiniciar el servicio de la entidad emisora

1. Compruebe que no haya nadie realizando una transacción con la entidad emisora. Si dispone del tiempo necesario, envíe un aviso a los usuarios que puedan verse afectados.
2. Si fuera posible, ejecute el siguiente comando para detener Servicios de Certificate Server e impedir que los usuarios se conecten a la entidad emisora durante el cierre:

   net stop "Certificate Services"
3. Siga los procedimientos normales del sistema operativo para reiniciar su PC. A menos que esté claro que el proceso de Servicios de Certificate Server ha dejado de responder, no intente cancelar dicho proceso ni apagar el servidor. La cancelación del proceso de Servicios de Certificate Server puede dañar su respectiva base de datos y requerir una restauración a partir de la copia de seguridad.

   Nota: como se ha indicado en la tarea anterior, la auditoría de los procesos de inicio y cierre puede provocar que Servicios de Certificate Server tarde mucho tiempo en cerrarse y volver a iniciarse. El retardo no se produce si no se auditan el inicio ni el cierre.

Restauración de la entidad emisora a partir de una copia de seguridad
Si no puede iniciar una entidad emisora debido a un daño grave de software o hardware, será necesario restaurar

el servidor y el material importante a partir de una copia de seguridad.

Información de resumen

- **Requisitos de seguridad**:
  - Administradores locales en la entidad emisora
  - Operadores de copia de seguridad de entidad emisora (sólo para realizar la restauración)
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Copia de seguridad de Windows
  - Sistema de copia de seguridad organizativo

Detalles de la tarea

Realice los siguientes pasos para restaurar una entidad emisora a partir de una copia de seguridad.

Precaución: si utiliza un HSM, este procedimiento no funcionará como se indica. Siga las instrucciones del proveedor de HSM para realizar la copia de seguridad, restaurar y proteger el material importante y las claves de acceso.

Para restaurar una entidad emisora a partir de una copia de seguridad

1. Es necesario que el sistema operativo se recupere hasta el punto en el que se pueda volver a ejecutar Servicios de Certificate Server, lo que puede requerir la reinstalación de Windows. En tal caso, siga las instrucciones detalladas en la guía de generación para instalar el sistema operativo y los componentes básicos del sistema. No hay necesidad de aplicar medidas de seguridad u otras medidas de configuración.

   Advertencia: si tiene que reinstalar Windows en la entidad emisora, no vuelva a formatear ni a crear particiones en la segunda unidad. Esta unidad contiene la base de datos de la entidad emisora, que puede estar intacta.

2. Si fuera posible, mantenga la base de datos de la entidad emisora (en %systemroot%\System32\CertLog de la entidad emisora raíz o en D:\CertLog en la entidad emisora) y los registros de la entidad emisora (en %systemroot%\System32\CertLog). Realice una copia de seguridad de archivo de estas carpetas antes de restaurar la entidad emisora. Es posible que la base de datos y los registros no se hayan visto afectados por el error del sistema. Los registros contienen información necesaria para volver a ejecutar todas las transacciones en la entidad emisora que se produjeron entre la última copia de seguridad y el error del servidor. No obstante, al restaurar una copia de seguridad del estado del sistema se pueden sobrescribir los registros y la base de datos existente, por lo que debe preservarlos antes de iniciar una restauración del sistema.

3. Inserte los medios de copia de seguridad con la copia de seguridad más reciente en la entidad emisora y restaure el archivo de copia de seguridad del estado del sistema en un área del disco apropiada (se recomienda una segunda unidad, si está disponible).

4. Inicie el programa de copia de seguridad de Windows. En la ficha **Restaurar**, haga clic con el botón secundario del mouse en el objeto **Archivo** en el panel izquierdo y, a continuación, haga clic en **Catalogar archivo**.

5. Asegúrese de que se seleccione **Ubicación original** como destino para la restauración de archivos y, a continuación, haga clic en **Iniciar restauración** para restaurar el estado del sistema. Al finalizar, reinicie el servidor y detenga Servicios de Certificate Server una vez reiniciado el sistema.

6. Si se han preservado los registros de la entidad emisora en el paso 2, cópielos en la carpeta de registros de Servicios de Certificate Server (%systemroot%\System32\CertLog). Los registros están preparados para volver a ejecutarse en la base de datos restaurada con el fin de insertar las transacciones que se han producido después de la última copia de seguridad.

   Nota: si ha podido guardar intactos la base de datos y los registros de la entidad emisora en el paso 2,

puede restaurarlos en el servidor en vez de realizar el procedimiento de este paso (paso 6). Para volver a copiar la base de datos y los registros de la entidad emisora en el servidor, se debe detener el servicio Servicios de Certificate Server.

7. Inicie Servicios de Certificate Server.

Restauración del certificado de la entidad emisora y el par de claves en un equipo temporal
Si una entidad emisora con errores no puede restaurarse a tiempo para la emisión de una nueva lista CRL (o renovar un certificado crítico), tendrá que instalar el certificado y las claves de la entidad emisora en un equipo temporal para poder utilizarlos con el fin de volver a firmar y ampliar el período de validez de una lista CRL o certificado existente.

Información de resumen

- **Requisitos de seguridad**: administradores locales en el equipo local
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Certutil.exe
  - Cipher.exe

Detalles de la tarea
Esta tarea describe cómo debe restaurarse el certificado y las claves privadas de la entidad emisora en un equipo temporal. Si la entidad emisora se ha renovado, dispondrá de copias de seguridad de varios certificados y par de claves. Debe restaurar el archivo de clave y certificado más reciente para este procedimiento.

Importante: aunque este equipo tiene instalada la clave de la entidad emisora, debe adoptar las mismas precauciones de seguridad que utiliza con la entidad emisora. Si está restaurando la clave de una entidad emisora sin conexión, asegúrese de que el equipo esté sin conexión. Considere formatear nuevamente los discos del equipo una vez que haya terminado con la clave.

Precaución: si utiliza un HSM, este procedimiento no funcionará como se indica. Siga las instrucciones del proveedor de HSM para realizar la copia de seguridad, restaurar y proteger el material importante y las claves de acceso.

Para restaurar las claves y el certificado de la entidad emisora en un equipo temporal

1. Asegúrese de que el equipo se ha desconectado de la red. Inicie la sesión como miembro de los administradores locales y, a continuación, cree CAKeySigner como cuenta de usuario local.
2. Inicie la sesión con esta cuenta nueva.
3. Inserte un disco que contenga la copia de seguridad de las claves de la entidad emisora que debe probarse.
4. Utilice el Explorador de Windows para buscar los archivos de clave P12, seleccione el archivo más reciente y haga doble clic para iniciar el Asistente para importación.
5. Escriba la contraseña cuando se le solicite. No active las casillas de verificación para proporcionar alta protección para las claves o para hacerlas exportables.
6. Seleccione **Almacén personal** como ubicación en la que van a restaurar las claves de la entidad emisora.
7. Abra el complemento Certificados de MMC y busque el almacén personal. Busque el certificado de entidad emisora para la entidad emisora restaurada y ábralo para comprobar que tiene la clave privada correspondiente.

Puede realizar las tareas de nuevas firmas requeridas con las claves de la entidad emisora restauradas. Consulte el siguiente procedimiento, "Nueva firma de una lista CRL o un certificado para extender su validez". Cuando termine, limpie las claves de su PC utilizando el siguiente procedimiento.

Para limpiar las claves del sistema

1. Inicie la sesión como miembro de los administradores locales y elimine el perfil de usuario de la cuenta CAKeySigner (mediante **Propiedades avanzadas** en Mi PC).
2. Elimine la cuenta CAKeySigner.
3. Borre de forma segura las áreas sin asignar del disco para quitar permanentemente todo rastro de las claves. Para ello, ejecute el comando siguiente:

   Cipher /W:%AllUsersProfile%

   Nota: al especificar %allusersprofile% como ruta de acceso, se asegura de que Cipher.exe se ejecutará en la unidad que contiene los perfiles de usuario. Esto limpia toda la unidad, no sólo la ruta indicada.

Nueva firma de una lista CRL o un certificado para extender su período de validez

Si una entidad emisora no se encuentra disponible debido a algún tipo de error del servidor, puede extender la duración de listas CRL o certificados volviendo a firmar el archivo de CRL o certificados. Esta acción puede resultar esencial para mantener el servicio.

Información de resumen

- **Requisitos de seguridad:** cuenta temporal creada durante la restauración de la clave de la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Certutil.exe

Detalles de la tarea

La nueva firma de una lista CRL o un certificado extenderá su período de validez. De forma predeterminada, se utiliza el período de validez existente y se reinicia desde la fecha de la firma. Por ejemplo, si el período de validez original de la lista CRL era de un mes, el nuevo período de validez será de un mes a partir del momento de la nueva firma. Si es necesario, se puede especificar un período de validez distinto en la línea de comandos de Certutil.

Para volver a firmar una lista CRL o un certificado

1. Obtenga una copia de la lista CRL o el certificado que desea volver a firmar.
2. Inicie la sesión en un equipo donde la clave y el certificado de la entidad emisora empleados para firmar originalmente la lista CRL o certificado se han restaurado. (Consulte el procedimiento anterior, "Restauración del certificado de la entidad emisora y el par de claves en un equipo temporal".) Inicie sesión utilizando la cuenta creada en dicho procedimiento.
3. Ejecute el siguiente comando, sustituyendo *ArchivoAntiguo.ext* por el nombre del archivo de CRL o certificados y *ArchivoNuevo.ext* por el nombre del resultado requerido.

   Certutil -sign *ArchivoAntiguo.ext ArchivoNuevo.ext*

4. Cuando se le solicite indicar el certificado que desea utilizar, seleccione el certificado de la entidad emisora.
5. Si va a volver a firma una lista CRL, debe publicarla en los CDP según sea necesario (consulte los procedimientos para publicar listas CRL en la sección "Tareas del cuadrante operativo").

Revocación de un certificado de entidad final

Quizás sea necesario revocar un certificado por determinados motivos, incluido:

- La funcionalidad o los privilegios asociados con el certificado fueron revocados para el titular del certificado.
- La clave del certificado ha quedado comprometida.
- La entidad emisora que emitió el certificado ha quedado comprometida.

Información de resumen

- **Requisitos de seguridad**: administradores de certificados
- **Frecuencia**: según sea necesario

- **Requisitos de tecnología:** complemento Entidad emisora de certificados de MMC

Detalles de la tarea
En este procedimiento se describen los pasos para la revocación de un certificado de entidad final (es decir, un certificado emitido a una entidad que no es la entidad emisora). Siga los procedimientos detallados en otras secciones para la revocación de un certificado de entidad emisora.

Para revocar un certificado

1. Inicie sesión como miembro de Administradores de certificados y busque los certificados que desea revocar en la base de datos de la entidad emisora de certificados (en Entidad emisora de certificados de MMC). Utilice la opción **Filtro** (en el menú **Ver** de la carpeta **Certificados emitidos**) de la entidad emisora para buscar los certificados.

2. Seleccione los certificados y, a continuación, haga clic en **Revocar** en el menú **Tareas**.

3. Seleccione un código de motivo adecuado para la revocación. A menos que la razón de la revocación se incluya en uno de los códigos de razón predefinidos, seleccione **No especificado**.

   Importante: el único motivo que permite la posterior reinstalación del certificado es **Posesión de certificado**. Todos los demás motivos darán como resultado la deshabilitación permanente del certificado. No obstante, no utilice sólo **Posesión de certificado** porque existe la posibilidad de que el certificado se pueda rehabilitar. Utilice este código sólo cuando realmente deba suspender de forma temporal el certificado.

Revocación de un certificado huérfano
Al restaurar una entidad emisora desde una copia de seguridad después de algún tipo de error del servidor, es posible que los certificados emitidos entre la última copia de seguridad y el error no se encuentren en la base de datos de certificados. Estos certificados se denominan "huérfanos". Esta situación se producirá si los registros de la entidad emisora están destruidos y no se pueden volver a ejecutar en la base de datos de la entidad emisora después de su restauración de la copia de seguridad. Si se produce esta situación, es imposible revocar ninguno de estos certificados "huérfanos" con el procedimiento estándar.

Información de resumen
- **Requisitos de seguridad**: administradores de certificados
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Certutil.exe

Detalles de la tarea
Para revocar un certificado huérfano, es necesario obtener una copia del certificado que se desea revocar o el número de serie de dicho certificado.

Para revocar un certificado huérfano

1. Inicie sesión en la entidad emisora que emitió el certificado que se desea revocar como miembro de Administradores de certificados.

2. Si no puede obtenerse una copia del certificado, ejecute el siguiente comando para crear un certificado ficticio y guárdelo como CertToRevoke.cer. Sustituya *NúmeroSerie* por el número de serie del certificado que desea revocar.

   Certutil -sign *NúmeroSerie* CertToRevoke.cer

3. Cuando se le solicite, seleccione el certificado de la entidad emisora actual para firmar el certificado ficticio.

4. Después de crear un certificado ficticio (u obtener una copia del certificado real que se revocará), tiene que importarlo en la base de datos de la entidad emisora. Ejecute el siguiente comando para importar el certificado en la base de datos de certificados. CertToRevoke es una copia del certificado real que se va a revocar o el certificado ficticio creado en los pasos anteriores.

   Certutil -importcert CertToRevoke.cer

5. Realice el procedimiento estándar para revocar un certificado (detallado en el procedimiento anterior, "Revocación de un certificado de entidad final").

   Importante: existe un problema con las versiones de Certutil anteriores a SP1 de Windows Server 2003 que provoca que se produzca un error en la creación de certificados ficticios en un equipo con Windows Server 2003. Si utiliza una versión anterior a esta y no puede encontrar una copia del certificado original, un método alternativo es tomar un certificado existente y utilizar un editor binario para reemplazar el número de serie por el del certificado que se va a revocar. Este certificado modificado se puede volver a firma con el siguiente comando:

   Certutil -sign ModifiedCert.cer CertToRevoke.cer
   A continuación, el certificado recién creado se puede importar en la base de datos con el paso 4 de este procedimiento.

Revocación y reemplazo de un certificado de entidad emisora
Si la clave privada de una entidad emisora ha quedado comprometida de alguna manera (o incluso si solamente se sospecha que ha quedado comprometida), revoque el certificado de la entidad emisora y emita uno nuevo utilizando un nuevo par de claves.

Información de resumen
- **Requisitos de seguridad**: administradores de certificados
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología:** complemento Entidad emisora de certificados de MMC

Detalles de la tarea
Debido a que el certificado de entidad emisora raíz tiene un período de publicación de la lista CRL muy largo, la simple revocación del certificado de entidad emisora y la publicación de una nueva lista CRL provocarán una gran demora entre dicha revocación y la recepción por parte de los usuarios de la misma. Para garantizar que todos los certificados emitidos anteriormente por la entidad emisora comprometida se rechazan tan pronto como sea posible, todos los certificados que ésta ha emitido también se revocan individualmente.

Importante: todos los usuarios de certificados deberán volver a inscribirse para obtener certificados nuevos.

Para revocar un certificado de CA emisora

1. Inicie sesión en la entidad emisora como miembro de Administradores de certificados y abra el complemento Entidad emisora de certificados de MMC.
2. Seleccione todos los certificados de la carpeta Certificados emitidos y, a continuación, en el menú **Todas las tareas**, haga clic en **Revocar certificado**. Seleccione **Compromiso de CA** como código de motivo.
3. Aumente el Intervalo de publicación CRL para ajustarlo al tiempo de vida restante del certificado de entidad emisora. Al aumentar este intervalo se garantizará que sea más largo que el tiempo de vida restante de todos los certificados que ha emitido la entidad emisora.
4. Desactive casilla de verificación **Publicar diferencias CRL**, si está seleccionada.
5. En el menú **Todas las tareas** de la carpeta Certificados revocados, haga clic en **Publicar** y, a continuación, haga clic en **Lista de revocación de certificados (CRL) nueva**.
6. Inicie sesión en la entidad emisora raíz como miembro de Administradores de certificados y abra el complemento Entidad emisora de certificados de MMC.
7. Busque el certificado de entidad emisora que desea revocar en la carpeta Certificados emitidos y, a continuación, en el menú **Todas las tareas**, haga clic en **Revocar certificado**. Seleccione **Compromiso de clave** como código de motivo.
8. Siga el procedimiento "Publicación de una lista CRL y un certificado de entidad emisora fuera de línea" de la sección "Tareas del cuadrante operativo" (puede omitir las partes de publicación de certificados de entidad emisora del procedimiento).

9. Vuelva a la entidad emisora y siga el procedimiento "Renovación del certificado de entidad emisora de certificados" de la sección "Tareas del cuadrante operativo".

Una vez completados los procedimientos anteriores, los usuarios de certificados ya pueden volver a inscribirse con la entidad emisora nueva. Los certificados de inscripción automática se inscribirán automáticamente.

Revocación y reemplazo de un certificado de entidad emisora raíz
Si la clave privada de una entidad emisora raíz ha quedado comprometida de alguna manera (o incluso si solamente se sospecha que ha quedado comprometida), debe eliminar el certificado de la entidad emisora de su punto confiable y revocar todos los certificados que éste y cualquiera de sus entidades emisoras subordinadas hayan emitido. Debe renovar el certificado de la entidad emisora raíz y los certificados de todas sus entidades emisoras subordinadas con nuevas claves y, a continuación, volver a publicarlos en Active Directory. Normalmente no es posible revocar un certificado de entidad emisora raíz. Frecuentemente, el certificado de la entidad emisora no incluye un CDP a partir del que se pueda comprobar el estado de revocación. En cualquier caso, no es estrictamente lega que una entidad emisora afirme su propia revocación. (Se tendría que utilizar el certificado comprometido para firmar la lista CRL que contiene su propio certificado revocado.)

Información de resumen
- **Requisitos de seguridad**:
  - Administradores de certificados
  - Administradores locales en entidades emisoras (para subtareas de renovación de entidad emisora)
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología:** complemento Entidad emisora de certificados de MMC

Detalles de la tarea
Nota: todos los usuarios de certificados deberán volver a inscribirse para obtener certificados nuevos después de completar este procedimiento.

Para revocar un certificado de entidad emisora raíz

1. Inicie sesión en la entidad emisora como miembro de Administradores de certificados y abra el complemento Entidad emisora de certificados de MMC.
2. Seleccione todos los certificados de la carpeta Certificados emitidos y, a continuación, en el menú **Todas las tareas**, haga clic en **Revocar certificado**. Seleccione **Compromiso de CA** como código de motivo.
3. Aumente el Intervalo de publicación de CRL para ajustarlo a la duración restante del certificado de la entidad emisora. Al aumentar este intervalo se garantizará que sea más largo que el tiempo de vida restante de todos los certificados que ha emitido la entidad emisora.
4. Desactive casilla de verificación **Publicar diferencias CRL**, si está seleccionada.
5. En el menú **Todas las tareas** de la carpeta Certificados revocados, haga clic en **Publicar** y, a continuación, haga clic en **Lista de revocación de certificados (CRL) nueva**. Repita los pasos del 1 al 5 para todas las entidades emisoras subordinadas.
6. Inicie sesión en la entidad emisora raíz como miembro de Administradores de certificados y abra el complemento Entidad emisora de certificados de MMC.
7. Seleccione todos los certificados de la carpeta Certificados emitidos y, a continuación, en el menú **Todas las tareas**, haga clic en **Revocar certificado**. Seleccione **Compromiso de CA** como código de motivo.
8. Aumente el Intervalo de publicación de CRL para ajustarlo a la duración restante del certificado de la entidad emisora. Al aumentar este intervalo se garantizará que sea más largo que el tiempo de vida restante de todos los certificados que ha emitido la entidad emisora.
9. Desactive casilla de verificación **Publicar diferencias CRL**, si está seleccionada.
10. Siga el procedimiento operativo "Renovación del certificado de la entidad emisora raíz".

11. Vuelva a la entidad emisora y siga el procedimiento operativo "Renovación del certificado de entidad emisora de certificados".

    Una vez completados los procedimientos anteriores, los usuarios de certificados ya pueden volver a inscribirse con la entidad emisora nueva. Los certificados de inscripción automática se inscribirán automáticamente.

    Importante: la renovación de un certificado de entidad emisora raíz es un suceso muy importante, en concreto cuando se produce la revocación de entidades emisoras secundarias y certificados emitidos. Asegúrese de informar a los propietarios de la aplicación afectados del nuevo certificado raíz en caso de que deban configurar esta nueva raíz en su aplicación.

Principio de la página

Tareas del cuadrante de optimización

El cuadrante de optimización incluye las SMF necesarias para administrar costos y mantener o mejorar los niveles de servicio. En las tareas se incluyen la revisión de interrupciones/incidentes, el examen de estructuras de costos, las evaluaciones del personal, la disponibilidad y el análisis del rendimiento, así como el pronóstico de capacidad.

Esta sección contiene información relevante para las SMF siguientes:

- Administración de capacidad

No hay tareas que correspondan al resto de las SMF:

- Administración de nivel de servicio
- Administración financiera
- Administración de disponibilidad
- Administración de continuidad del servicio de TI
- Administración de personal

Nota: cada descripción de tarea incluye la siguiente información de resumen: requisitos de seguridad, frecuencia y requisitos de tecnología.

Administración de capacidad

La administración de capacidad es el proceso de planear, ajustar el tamaño y controlar la capacidad de la solución del servicio para satisfacer la demanda del usuario dentro de los niveles de rendimiento establecidos en el SLA. Satisfacer esta demanda requiere información acerca de las situaciones de uso, patrones y características de carga máxima de la solución del servicio, así como los requisitos de rendimiento establecidos.

Determinación de la carga máxima de la entidad emisora

En esta sección se brinda información acerca de la carga máxima probable en la entidad emisora.

Si bien las entidades emisoras generalmente no experimentan una carga muy importante, hay ocasiones en las que las cargas pueden elevarse considerablemente. La mayor carga en una entidad emisora se produce generalmente en el inicio de sesión a horas punta o en el momento de iniciar durante la ejecución de un nuevo tipo de certificado. Del mismo modo, aunque con muchísima menos frecuencia, una revocación masiva de certificados o de certificados de entidad emisora provocará una carga máxima anómala de actividad debida a la nueva inscripción de usuarios y equipos.

Información de resumen

- **Requisitos de seguridad**: ninguno
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología**: ninguno

Detalles de la tarea

Las pruebas internas de Microsoft han demostrado que, en una entidad emisora de certificados de empresa

normal, el cuello de botella de rendimiento en situaciones de alta carga se debe a la interacción con Active Directory. La tarea de firmar y emitir certificados es relativamente liviana comparada con la sobrecarga de realizar una búsqueda de directorios para recuperar información sobre el sujeto del certificado y, a continuación, volver a publicar dicho certificado en Active Directory.
Considere, por ejemplo, los números generados en un escenario de carga máxima donde se ha habilitado un nuevo tipo de certificado y todos los usuarios y equipos tienen que inscribir certificados de este tipo:

- Número de usuarios: 3000
- Número de equipos: 3000
- La velocidad de emisión máxima aproximada de una entidad emisora de certificados de empresa es de tres certificados por segundo (o 1800 por minuto).

Estos números indican un tiempo de inscripción total mínimo de 3,3 minutos. Para 15.000 usuarios y el mismo número de equipos inscribiéndose simultáneamente, el tiempo de inscripción se ampliaría a 16,6 minutos.

Debe determinar la carga de inscripción máxima probable para su organización y calcular la duración de inscripción total. Si el tiempo es inaceptablemente largo y no puede dividir en partes la inscripción de ningún modo, debe considerar la posibilidad de implementar varias entidades emisoras. Dichas entidades emisoras se implementarán en sitios de Active Directory independientes para que utilicen controladores de dominio distintos.

Determinación de los requisitos de almacenamiento y copia de seguridad para una entidad emisora

Esta sección brinda detalles de capacidad de los parámetros de almacenamiento de la entidad emisora. Esta información ayudará a los planeadores de capacidad a calcular los requisitos futuros de almacenamiento para el disco en línea y los medios de almacenamiento de copia de seguridad sin conexión.

Información de resumen

- **Requisitos de seguridad**: ninguno
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: ninguno

Detalles de la tarea

En las siguientes secciones se enumeran los supuestos y los resultados de los cálculos de tamaño para la base de datos de la entidad emisora, el tamaño del registro de base d datos de la entidad, el tamaño de la lista CRL y el intervalo de copia de seguridad (tiempo para realizar la copia de seguridad de la base de datos de la entidad emisora).

Los siguientes cálculos se basan en estos supuestos:

- Una población de 3000 usuarios, 3000 equipos y de 100 a 300 servidores.
- Cada entidad final se emite con cinco certificados por año, con un período de validez de un año cada uno.
- Los certificados se mantienen en la base de datos durante cinco años.
- Se realiza una copia de seguridad de la base de datos diariamente (truncando los registros de dicha base de datos).

Tamaño de la base de datos de certificados

Cada entrada de certificado ocupa 20 KB aproximadamente en la base de datos (para los tipos de certificado que archivan la clave privada con el certificado, se debe permitir 10 KB adicionales de almacenamiento por certificado). Un cálculo rápido indica lo siguiente:

- Hay 150.000 certificados guardados en la base de datos en un momento determinado.
- El tamaño total de la base de datos de certificados es de 3 GB.

Para una organización de 15.000 usuarios, el tamaño de la base de datos de certificados es de 15 GB.

Tamaño promedio del registro de la base de datos de certificados

- Hay 750 certificados por día.
- El tamaño promedio del registro es de 5 MB.

Para una organización de 15.000 usuarios, se emiten 3.350 certificados cada, lo que crea un tamaño de registro máximo de 25 MB.

Tamaño de la lista CRL

Una entrada de lista CRL ocupa 30 bytes aproximadamente. Por lo general, se revocará aproximadamente el diez por ciento de los certificados emitidos. Los certificados revocados que estén fuera de su período de validez no se incluyen en la lista CRL.

- Hay 30.000 certificados que se encuentran dentro de su período de validez en un momento determinado.
- Habrá 3.000 certificados en la lista CRL.
- El tamaño de la lista CRL es de 90 KB.

Para una organización de 15.000 usuarios, habrá 15.000 certificados en la lista CRL, lo que crea un tamaño de lista CRL de 440 KB.

Intervalo de copia de seguridad para la base de datos de certificados

Si supone que una copia de seguridad de red funcionando en condiciones ideales en un conmutador dedicado de 100 Mbps (megabits por segundo) al servidor de copia de seguridad, en aproximadamente 15-20 minutos se puede realizar la copia de seguridad de una base de datos de 3 GB con 500 MB adicionales de estado del sistema. En menos de dos horas se puede realizar la copia de seguridad de una organización de 15.000 usuarios con una base de datos de certificados de 15 GB.

Principio de la página

Tareas del cuadrante de cambio

El cuadrante de cambio incluye los procesos y procedimientos requeridos para identificar, revisar, aprobar e incorporar cambios en un entorno administrado de TI. Los cambios incluyen activos de hardware y software, así como cambios específicos en procesos y procedimientos.

El objetivo del proceso de cambio es introducir tecnologías, sistemas, aplicaciones, hardware, herramientas y procesos nuevos y realizar cambios en las funciones y responsabilidades dentro del entorno de TI rápidamente y con una mínima interrupción del servicio.

Esta sección contiene información relevante para las SMF siguientes:

- Administración de cambios
- Administración de la configuración
- Administración de versión

Nota: cada descripción de tarea incluye la siguiente información de resumen: requisitos de seguridad, frecuencia y requisitos de tecnología.

Administración de cambios

La SMF de administración de cambios es la responsable de administrar los cambios en un entorno de TI. Un objetivo clave del proceso de administración de cambios consiste en asegurar que todas las partes afectadas por el cambio conocen y entienden el impacto del cambio. Dado que la mayor parte de sistemas están estrechamente interrelacionados, cualquier cambio que se realice en una parte del sistema podría tener un profundo impacto en otra. Para mitigar o eliminar los efectos adversos, cambie los intentos de administración para identificar todos los sistemas y procesos afectados antes de que el cambio se implemente. Normalmente, el “objetivo” o entorno administrado es el entorno de producción, pero también debe incluir los entornos clave de integración, pruebas y

almacenamiento temporal.

Todos los cambios realizados en la PKI deben seguir el siguiente proceso de administración de cambios de MOF estándar:

1. **Solicitud de cambio**. La iniciación formal de un cambio a través del envío de una solicitud de cambio (RFC).
2. **Clasificación de cambio**. La acción de asignar una prioridad y una categoría al cambio, utilizando como criterios su urgencia e impacto sobre la infraestructura o los usuarios. Esta asignación afecta a la ruta y la velocidad de implementación.
3. **Autorización de cambio**. La consideración, la aprobación o la desaprobación del cambio por parte del administrador de cambios y la junta consultiva de cambios (CAB), una junta que incluye a los representantes empresariales y de TI.
4. **Desarrollo de cambio**. El planeamiento y el desarrollo del cambio, un proceso que puede variar inmensamente de ámbito e incluye revisiones en etapas interinas importantes.
5. **Lanzamiento de cambio**. El lanzamiento y la implementación del cambio en el entorno de producción.
6. **Revisión de cambio**. Un proceso posterior a la implementación que revisa si el cambio ha logrado los objetivos establecidos para el mismo y determina si debe mantenerse en vigencia o desactivarse.

En esta sección se describen los procedimientos de desarrollo de cambios para algunos de los cambios clave que podrían requerirse normalmente en el entorno. Cada procedimiento de desarrollo de cambio vendrá acompañado de un procedimiento de lanzamiento del cambio que describe cómo se debe implementar el cambio en la producción.

Administración de actualizaciones del sistema operativo

La administración de actualizaciones de seguridad de Servicios de Certificate Server forma parte de la administración de revisiones de Windows general. Se trata en las dos guías de solución de Microsoft que describen el suministro de las actualizaciones de sistemas operativos Windows mediante Microsoft Systems Management Server (SMS) o Servicios de actualización de software de Microsoft (SUS). Consulte la sección "Información adicional" que aparece al final de este capítulo para obtener información acerca de cómo obtenerlas.

La administración de revisiones incluye componentes de administración de lanzamiento y configuración, así como un componente de administración de cambios. Sin embargo, las tres SMF se tratan en los documentos a los que se hace referencia en el párrafo anterior.

Información de resumen

- **Requisitos de seguridad**: administradores locales en la entidad emisora
- **Frecuencia**: tarea de configuración
- **Requisitos de tecnología:** infraestructura de distribución de actualizaciones de seguridad (como SMS o SUS)

Adición de una plantilla de certificados

Puede agregar una nueva plantilla de certificado para permitir la emisión de un nuevo tipo de certificado, que se puede necesitar debido a que se está implementando una nueva aplicación o una existente necesita nueva funcionalidad. Esta tarea también puede formar parte de un proceso de actualización de un tipo de certificado existente.

Información de resumen

- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología:** complemento Plantillas de certificados de MMC

Antes de enviar una solicitud de un nuevo tipo de certificado, pruébelo en un entorno de prueba que sea representativo del entorno de producción.

Documente la solicitud de un nuevo tipo de certificado e incluya:

- Las razones para la creación de la plantilla nueva
- Una evaluación del impacto en los usuarios y la infraestructura
- Una evaluación del impacto originado por no realizar el cambio
- Resultados de las pruebas del cambio

La documentación debe incluir las actualizaciones relevantes en las directivas de certificados y en la declaración de prácticas del certificado (CPS). A continuación, es necesario evaluarlo en relación con su prioridad e impacto. Después de que el cambio se haya aprobado, puede implementarse (aunque no se haya lanzado todavía).

Detalles de la tarea
El siguiente procedimiento debe llevarse a cabo sólo en un entorno de prueba. El proceso para la realización de este cambio en el entorno de producción se documenta en el procedimiento "Lanzamiento de una plantilla de certificados nueva".

Para implementar una plantilla de certificados nueva

1. Inicie sesión como miembro de Administradores de PKI de empresa y abra el complemento Plantillas de certificados de MMC.
2. Las plantillas nuevas se crean duplicando una existente. Seleccione la plantilla adecuada en la que se basará la nueva, una que sea lo más similar posible a la que desea crear.

   Importante: asegúrese de hacer coincidir el tipo de plantilla básico, usuario o equipo, de la plantilla de origen con el tipo de sujeto de la nueva plantilla; el tipo no se puede cambiar en el editor de plantillas.
3. Edite los detalles de la plantilla como corresponda. Para obtener información detallada acerca de este paso, consulte la documentación del producto en el sistema de ayuda local o en línea en la referencia de la sección "Información adicional".
4. Si esta plantilla va a reemplazar una existente, tiene que agregar las plantillas reemplazadas a la lista de **Plantillas reemplazas** en las propiedades de la nueva plantilla. Debe ser extremadamente cuidadoso al comprobar que la plantilla de reemplazo brinde la misma funcionalidad o un superconjunto de funcionalidades de la plantilla reemplazada. Nunca reduzca la funcionalidad a menos que esté seguro de que ninguna aplicación utiliza la funcionalidad que se elimina.
5. Pruebe los cambios para asegurarse de que funcionan del modo previsto y que no afectan negativamente a las aplicaciones existentes.
6. Cree los cambios adecuados para el documento de directivas de certificados y la CPS.
7. Siga los pasos de los procedimientos "Lanzamiento de una plantilla de certificados nueva" y "Lanzamiento de una CPS nueva" (si publica su CPS).

Actualización de una plantilla de certificados

Esta tarea describe cómo realizar cambios menores en las plantillas de certificados. Los cambios principales se deben realizar mediante la duplicación de plantillas y forzando que la nueva plantilla reemplace a la siguiente (tal como se ha descrito en la tarea anterior, "Adición de una plantilla de certificados").

Información de resumen
- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología:** complemento Plantillas de certificados de MMC

Detalles de la tarea
Sólo debe realizar cambios menores, que no tenga un efecto importante en los usuarios de certificado, en una plantilla de certificados. Resulta mucho más difícil controlar el impacto de las modificaciones de plantillas y es

considerablemente más complejo deshacer los cambios en las plantillas.

Entre los ejemplos de cambios menores se incluyen:

- Cambio del período de validez o renovación
- Adición (pero no eliminación) de un tipo de CSP admitido

Implemente los cambios que afecten a la funcionalidad de los certificados (como el cambio de las directivas de certificados, la eliminación de tipos de CSP y el cambio de criterios de emisión) mediante la creación de un nuevo tipo de plantilla y el reemplazo de la plantilla anterior.

Evalúe y apruebe la solicitud de cambio según se describe en el procedimiento "Adición de una plantilla de certificados".

Puede implementar y probar el cambio de plantilla propuesto pasando el cambio para su lanzamiento en producción. Consulte el procedimiento "Lanzamiento de una actualización de plantilla".

Para actualizar una plantilla de certificados

1. Inicie sesión como miembro de Administradores de PKI de empresa y cargue el complemento Plantillas de certificados en una MMC.
2. Abra la plantilla que se va a modificar y realice los cambios requeridos. Para obtener información detallada al respecto, consulte la documentación del producto en el sistema de ayuda local o en línea en la referencia de la sección "Información adicional".
3. Pruebe la actualización para asegurarse de que produzca la funcionalidad requerida.
4. Siga los pasos de los procedimientos "Lanzamiento de una plantilla de certificados nueva" y "Lanzamiento de una CPS nueva" (si corresponde).

Eliminación de una plantilla de certificados

Cuando una plantilla de certificados ya no es necesaria, puede eliminarse de su estado activo o bien del directorio por completo.

Información de resumen

- **Requisitos de seguridad**: Administradores de CA
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Plantilla de certificados de MMC
  - Complemento Entidad emisora de certificados de MMC

Detalles de la tarea

Sólo debe eliminar una plantilla cuando esté seguro de que no haya aplicaciones que dependan de la disponibilidad de certificados de ese tipo. Evalúe y apruebe la solicitud de eliminación de la plantilla de la misma manera descrita en el procedimiento "Adición de una plantilla de certificados". Siga siempre el primer procedimiento para eliminar una plantilla del uso activo y pruebe los efectos de esto antes de eliminar completamente una plantilla del directorio.

Puede implementar y probar la eliminación del cambio de plantilla antes del lanzamiento de dicho cambio en producción. Consulte el procedimiento "Lanzamiento de una eliminación de plantilla".

Para eliminar una plantilla de certificados de su uso activo

1. Inicie sesión como miembro de Administradores de entidad emisora y cargue el complemento Entidad emisora de certificados en una MMC.
2. En la carpeta Plantillas de certificados, haga clic con el botón secundario del mouse en la plantilla que desea quitar y seleccione **Eliminar**.

3. Repita los pasos 1 y 2 en todas entidades emisoras que actualmente emiten este tipo de certificado.
4. Pruebe las aplicaciones que utilizaron esta plantilla anteriormente para garantizar que ya no dependan de este tipo de certificado.
5. Siga los pasos de los procedimientos "Lanzamiento de una eliminación de plantilla" y "Lanzamiento de una CPS nueva" (si corresponde).

Para quitar definitivamente una plantilla de certificados del directorio

1. Inicie sesión como miembro de Administradores de PKI de empresa y cargue el complemento Plantillas de certificados en una MMC.
2. Haga clic con el botón secundario del mouse en la plantilla que desea quitar y seleccione **Eliminar**.

Administración de la configuración

La SMF de la administración de configuración se ocupa de la identificación, el registro, el seguimiento y el informe de los componentes o activos de TI importantes denominados elementos de configuración (CI). La información capturada y rastreada dependerá del CI específico, pero incluirá frecuentemente una descripción del CI, la versión, los componentes que lo conforman, las relaciones con otros CI, la ubicación/asignación y el estado actual.

La administración de configuración de una PKI se puede agrupar en diversas áreas importantes:

- **Configuración de PKI de empresa**. Información común almacenada en Active Directory.
- **Configuración de plantilla de certificados**. Detalles de configuración de todas las plantillas activas.
- **Configuración de entidad emisora**. Detalles de configuración específicos de la entidad emisora.
- **Grupos de administración de entidad emisora y PKI**. Detalles de los grupos y usuarios de administración de PKI y sus correspondientes permisos.
- **Configuración de cliente**. Configuración de parámetros de usuarios y equipos mediante la directiva de grupo (u otro método).

En cada una de las siguientes secciones se describen estos elementos con más detalle y se incluyen métodos para automatizar la recopilación de esta información si es posible.

Para obtener otras referencias acerca de Administración de configuración, consulte la sección "Información adicional" al final de este capítulo.

Recopilación de información de Configuración de PKI de empresa

La información relacionada con la configuración de empresa se almacena en Active Directory, incluida la publicación de entidades emisoras raíz confiables, la configuración de la entidad emisora de certificados de empresa y la información de anuncios. También incluye las plantillas de certificados, aunque éstos se tratan en otro procedimiento posterior.

Información de resumen

- **Requisitos de seguridad**: usuarios de dominio
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Certutil.exe
  - DSQuery.exe

Detalles de la tarea

Mantenga registros de la siguiente información guardada en Active Directory:

- Entidades emisoras raíz confiables
- Almacén NTAuth

- Servicios de inscripción (entidades emisoras de certificados de empresa)
- Certificados cruzados
- Listas CRL publicadas

Los comandos para recopilar esta información se proporcionan en los siguientes procedimientos.

Importante: en los siguientes comandos debe reemplazar el nombre distintivo (DN) de dominio raíz de ejemplo, *DC=woodgrovebank,DC=com*, por el DN de *su* raíz del bosque.

Nota: algunos de los comandos siguientes se muestran en varias líneas, pero se deben introducir en una sola.

Para mostrar las entidades emisoras raíz confiables

certutil -store -enterprise Root

Para mostrar los almacenes NT Auth

certutil -store -enterprise NTAuth

Para mostrar los certificados de entidades emisoras de certificados de empresa actuales

certutil -store -enterprise "ldap:///cn=Enrollment Services,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cACertificate?one? objectClass=pkiEnrollmentService"

Para mostrar los certificados intermedios y cruzados

certutil -store -enterprise CA

Para mostrar los certificados de entidad emisora intermedios solos

certutil -store -enterprise "ldap:///cn=AIA,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cACertificate?one? objectClass=certificationAuthority"

Para mostrar los certificados cruzados solos

certutil -store -enterprise "ldap:///cn=AIA,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?cRossCertificatePair?one? objectClass=certificationAuthority"

Para mostrar las listas CRL publicadas actualmente

1. Este comando mostrará los **nombres de servidores** de todas las entidades emisoras que publicaron CDP en el contenedor CDP de Active Directory:

   dsquery * "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration,*DC=woodgrovebank,DC=com*" -attr cn -scope onelevel

2. Este comando mostrará los CDP de cada entidad emisora que tenga listas CRL publicadas en el contenedor CDP de Active Directory. Los CDP son objetos secundarios de los objetos de servidor mostrados en la lista anterior. La entidad emisora utiliza su nombre común para asignar un nombre a cada objeto CDP. Tenga en cuenta que una entidad emisora creará un nuevo objeto CDP por cada versión de entidad emisora (incrementada cada vez que se renueva la entidad); dichos nombres se almacenan como "NombreComúnCA(X)" donde X es el número de versión de entidad emisora:

   dsquery * "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration, *DC=woodgrovebank,DC=com*" -attr cn -filter (objectclass=crlDistributionPoint)

3. 3. Puede utilizar la información de los pasos anteriores para mostrar la lista CRL de un determinado CDP (utilizando los nombres comunes de entidad emisora del paso 2 y los nombres de servidor de entidad

emisora obtenidos en el paso 1):

certutil -store -enterprise "ldap:///cn=*Entidad emisora raíz de Woodgrove Bank*,cn=*HQ-CA-01*,cn=CDP,CN=Public Key Services,CN=Services,CN=Configuration, *DC=woodgrovebank,DC=com*?certificateRevocationList?base?objectClass=cRlDistributionPoint"

Importante: reemplace "Entidad emisora raíz de Woodgrove Bank" por el nombre común de la entidad emisora, "HQ-CA-01" por el nombre de host de la entidad emisora y "DC=woodgrovebank,DC=com" por el nombre de dominio de su dominio raíz del bosque.

Nota: puede escribir una secuencia de comandos de un archivo de comandos (lote) individual para automatizar esta tarea, si tiene que ejecutarla periódicamente.

Recopilación de información de configuración de la plantilla de certificados

Las plantillas de certificados se guardan en Active Directory. Mantenga un registro de la configuración de cada plantilla y de los permisos de inscripción de certificados utilizados para cada plantilla.

Información de resumen

- **Requisitos de seguridad**: usuarios de dominio
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Certutil.exe

Detalles de la tarea

Utilice los siguientes comandos para recopilar esta información de configuración:

Para crear una lista de las plantillas configuradas en Active Directory

Certutil -template

Para volcar la configuración de estas plantillas

Certutil -dsTemplate

Para volver los permisos de una plantilla

Dsacls "cn=TemplateName,cn=Certificate Templates,cn=Public Key Services,cn=Services,cn=Configuration,*DC=woodgrovebank,DC=com*"

No existe ninguna herramienta que exporte los permisos de plantilla completos en un formato fácilmente legible. Dsacls.exe muestra los permisos en una plantilla. No obstante, la versión actual no muestra el permiso "Inscripción automática" de derechos extendidos (aunque muestra "Inscripción" y otros permisos de derechos extendidos). Esto significa que debe conservar un registro manual de los permisos "Inscripción automática". Si lo desea, puede escribir una secuencia o una herramienta mediante Interfaz de servicios de Active Directory (ADSI) para leer y mostrar todos los permisos correctamente.

Recopilación de información de Configuración de la entidad emisora

En esta sección se describe el modo de recuperar la información de configuración guardada localmente en cada entidad emisora y, en el caso de entidades emisoras de certificado de empresa, parte de la información almacenada en Active Directory.

Información de resumen

- **Requisitos de seguridad**: administradores locales de la entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Certutil.exe

Detalles de la tarea

Mantenga registros de la siguiente información:

- Información de registro de la entidad emisora
-

Información de certificado de la entidad emisora

- Permisos de la entidad emisora
- Plantillas asignadas de la entidad emisora
- CPS de la entidad emisora
- Utilice los siguientes comandos para recopilar esta información de configuración:

Para mostrar la configuración de registro de la entidad emisora

Certutil -getreg

Certutil -getreg CA

Para mostrar el certificado de la entidad emisora actual

certutil -f -ca.cert %temp%\CAcert.cer > nul && certutil -dump %temp%\CACert.cer

Nota: algunos de estos comandos se muestran en varias líneas, pero se deben introducir en una sola.

No existe ninguna herramienta para exportar los permisos completos de la entidad emisora en un formato que se pueda utilizar. No obstante, puede escribir una secuencia de comandos ADSI para leer y mostrar todos los permisos correctamente. Si lo desea, puede conservar un registro manual de esta información.

Para mostrar las plantillas asignadas actualmente a esta entidad emisora

Certutil -CATemplates

El archivo CPS de la entidad emisora debe mantenerse con un control de versión adecuada para poder identificar y recuperar fácilmente el CPS que estaba en efecto en un determinado momento.

Recopilación de información de grupos de administración de CA y PKI

La pertenencia a los grupos de administración de PKI es una parte importante de la información de configuración, porque estos grupos controlan todos los aspectos de la información de entidades emisoras y la PKI de empresa.

Información de resumen

- **Requisitos de seguridad**: usuario de dominio
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Net.exe

Detalles de la tarea

En cada uno de los grupos de administración de PKI y entidad emisora, incluya y registre la pertenencia actual. Si algunos de los miembros son grupos (se indica con un asterisco delante del nombre), enumere la pertenencia a estos grupos hasta que disponga de una lista completa de todos los usuarios que sean miembros de los grupos de PKI.

Los grupos predeterminados son:

- Administradores de PKI de empresa
- Editores de PKI de empresa
- Administradores de entidad emisora
- Administradores de certificados
- Auditores de entidad emisora
- Operadores de copia de seguridad de CA

También debe incluir cualquier grupo de administración adicional que pueda haber creado.

Para enumerar la pertenencia a cada grupo

Net groups *nombregrupo* /domain

Recopilación de información de configuración del cliente del certificado

Esta tarea hace referencia a la información de configuración de cliente implementada mediante Directiva de grupo. Si utiliza otro mecanismo (por ejemplo, secuencias de comandos de SMS o de inicio de sesión) para implementar la configuración de cliente relacionada con la PKI, también debe documentarlo aquí.

Información de resumen

- **Requisitos de seguridad**: administrador con permisos para administrar objetos de directiva de grupo
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: consola de administración de directivas de grupo

Detalles de la tarea

Utilice la consola de administración de directivas de grupo (GPMC) para recopilar y detallar la información de configuración del cliente de PKI. Consulte la referencia en la sección "Información adicional" para obtener y utilizar GPMC.

Administración de versión

El enfoque de la administración de versión consiste en facilitar la introducción de versiones de software y hardware en los entornos de TI administrados. Por lo general, esto incluye el entorno de producción y los entornos de preproducción administrados. La administración de versión es el punto coordinación entre el equipo de desarrollo/proyecto de la versión y los grupos operativos responsables de la implementación de dicha versión en la producción.

En esta sección se tratará el cambio más común: agregar, cambiar y eliminar tipos de certificados (mediante las plantillas de certificados). Hay otros tipos de cambios que también debe lanzar de la misma manera sistemática, entre los que se incluyen:

- **Cambios en la configuración de PKI**. Por ejemplo, plantillas y OID.
- **Cambios en la configuración de la entidad emisora**. Registro local más la configuración de Active Directory en los objetos de inscripción.
- **Cambios en la configuración de cliente**. Cambios de GPO.

Todos estos procedimientos de lanzamiento utilizan el siguiente proceso general:

1. Prepárese para el lanzamiento del cambio: realice una copia de seguridad de la configuración existente.
2. Pruebe el cambio de manera controlada.
3. Ejecute el cambio de manera controlada en un número limitado de usuarios o equipos.
4. Deshaga el cambio si se produce algún error: configuración de Active Directory y de la entidad emisora.

Lanzamiento de una nueva plantilla de certificados

La introducción de un nuevo tipo de certificado representa un cambio importante en el entorno de TI, por lo que el lanzamiento debe manejarse en forma controlada y reversible.

Información de resumen

- **Requisitos de seguridad**:
  - Administradores de PKI de empresa
  - Administradores de entidad emisora
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:

- Complemento Entidad emisora de certificados de MMC
- Complemento Plantilla de certificados de MMC
- Otras herramientas requeridas por tareas dependientes

Detalles de la tarea
El procedimiento para lanzar una nueva plantilla de certificado en el entorno de producción es el siguiente:

Para lanzar una plantilla de certificados nueva

1. Realice una copia de seguridad de la configuración de la plantilla de certificados existente. Esta copia de seguridad se puede hacer como parte de la copia de seguridad habitual de Active Directory backup o con la técnica descrita en el procedimiento "Exportación de una plantilla de certificados desde Active Directory".
2. Cree la plantilla nueva como se describe en el procedimiento "Adición de una plantilla de certificados".
3. Elimine todos los permisos de inscripción e inscripción automática de los grupos (busque objetos como Usuarios autenticados y Usuarios del dominio). Cree el grupo de inscripción de certificados (o el grupo de inscripción automática) de la plantilla según se describe en el procedimiento "Creación de grupos de inscripción de plantillas de certificados".
4. Agregue la plantilla de certificados nueva a la entidad emisora. Si no es miembro además de Administradores de entidad emisora, deberá iniciar sesión (o utilizar el comando runas) como miembro de este grupo y ejecutar la MMC de Entidad emisora de certificados. Haga clic con el botón secundario del mouse en la carpeta Plantillas de certificados y seleccione **Nuevo**, **Plantilla de certificado que se va a emitir**. Agregue la plantilla desde la lista.
5. Agregue usuarios o equipos piloto o de prueba al grupo de inscripción de certificados como se describe en el procedimiento "Activación de inscripción (o inscripción automática) de un tipo de certificado para un usuario o equipo".
6. Pruebe la inscripción del nuevo tipo de certificado para asegurarse de que se realiza según lo previsto.
7. Pruebe la funcionalidad del certificado para asegurarse de que es la prevista.
8. Después de comprobar que la prueba es satisfactoria, agregue los usuarios, equipos o grupos de seguridad de producción finales al grupo o a los grupos de inscripción de certificados como se describe en el procedimiento "Activación de inscripción (o inscripción automática) de un tipo de certificado para un usuario o equipo".
9. Si esta plantilla reemplaza a una o varias plantillas existentes, puede eliminar las plantillas reemplazadas de la entidad emisora (utilizando el complemento Entidad emisora de certificados de MMC) para impedir que un usuario se inscriba en estos tipos de certificados reemplazados. No elimine esta plantilla del directorio hasta que esté seguro de que todos hayan realizado la transición al nuevo tipo de plantilla.
10. Si corresponde, actualice su CPS para reflejar la nueva funcionalidad del certificado.

No es difícil deshacer un nuevo tipo de plantilla siempre que no se hayan eliminado las plantillas reemplazadas. Si se ha eliminado la plantilla reemplazada, tendrá que restaurar una copia de la copia de seguridad con una restauración con autorización de Active Directory o los procedimientos de exportación e importación de plantillas descritos en la sección "Administración de almacenamiento" anterior ("Exportación de una plantilla de certificados desde Active Directory" e "Importación de una plantilla de certificados a Active Directory").

Para deshacer la adición de una plantilla nueva

1. Si no ha reemplazado otras plantillas con esta plantilla, puede eliminarla sin problemas.
2. Si ha eliminado las plantillas reemplazadas por esta plantilla, primero restáurelas. Siga los pasos del procedimiento "Importación de una plantilla de certificados a Active Directory". Será necesario restaurar los permisos de plantillas según se describe en dicho procedimiento.

Lanzamiento de una CPS nueva

Si publica su CPS, deberá actualizarla para que refleje los cambios producidos en las directivas y prácticas de certificados de su organización.

Información de resumen

- **Requisitos de seguridad**: administrador con permisos para modificar un archivo CPS en un servidor Web
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**: Editor de HTML o de texto, según corresponda, en el formato de la CPS

Detalles de la tarea

La CPS generalmente se guarda como simple archivo HTML o de texto en un servidor Web o de archivos. Si varias entidades emisoras utilizan la misma CPS, la norma es que todas hagan referencia al mismo archivo.

Para lanzar una CPS nueva

1. Realice una copia de seguridad de la CPS existente.
2. Realice los cambios requeridos en una copia sin conexión.
3. Reemplace la CPS.
4. Realice una prueba para asegurarse de que el nuevo archivo CPS se puede leer desde los clientes; para ello, emule los tipos de plataforma y las ubicaciones a los que normalmente se ofrecerá servicio.

Lanzamiento de una actualización de plantilla

Esta tarea describe cómo realizar cambios de versión en las plantillas de certificados existentes en forma controlada y reversible.

Información de resumen

- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Plantilla de certificados de MMC
  - Otra tecnología requerida por los procedimientos mencionados

Detalles de la tarea

Sólo debe realizar cambios en las plantillas de certificados que sean relativamente pequeños y no tengan un efecto importante en los usuarios de certificados. Resulta mucho más difícil controlar el impacto de las modificaciones de plantillas y es considerablemente más complejo deshacer los cambios en las plantillas.

Para lanzar una actualización de plantilla de certificados

1. Exporte la plantilla actual al archivo mediante el procedimiento "Exportación de una plantilla de certificados desde Active Directory".
2. Inicie sesión como miembro de Administradores de PKI de empresa y cargue el complemento Plantillas de certificados en una MMC. Realice los cambios en la plantilla según se describe en "Actualización de una plantilla de certificados".
3. Actualice la CPS y siga los pasos del procedimiento "Lanzamiento de una CPS nueva" (si corresponde).

Para deshacer una actualización de plantilla de certificados

- Siga los pasos del procedimiento "Importación de una plantilla de certificados a Active Directory" (en la sección "Administración de almacenamiento").

Lanzamiento de una eliminación de plantilla

Cuando una plantilla de certificados ya no es necesaria, puede eliminarla de su uso activo o del directorio.

Información de resumen

- **Requisitos de seguridad**: Administradores de PKI de empresa
- **Frecuencia**: según sea necesario
- **Requisitos de tecnología**:
  - Complemento Entidad emisora de certificados de MMC
  - Otra tecnología requerida por las tareas mencionadas

Detalles de la tarea
El procedimiento de lanzamiento para eliminar una plantilla del uso activo es relativamente directo, porque es fácil de revertir. La eliminación de la plantilla del directorio es más problemática, porque requiere una nueva importación de la plantilla para revertir el cambio.

Para eliminar una plantilla de certificados de su uso activo

1. Elimine la plantilla de las entidades emisoras actuales como se describe en el procedimiento "Eliminación de una plantilla de certificados".
2. Actualice la CPS y siga los pasos del procedimiento "Lanzamiento de una CPS nueva" (si corresponde).

Para deshacer la eliminación de una plantilla de su uso activo

1. Inicie sesión como miembro de Administradores de entidad emisora y utilice el complemento Entidad emisora de certificados de MMC para volver a agregar las plantillas a las entidades emisoras.
2. Actualice la CPS y siga los pasos del procedimiento "Lanzamiento de una CPS nueva" (si corresponde).

Para quitar definitivamente una plantilla de certificados del directorio

1. Sólo debe llevar a cabo este procedimiento después de eliminar la plantilla de certificados del uso activo y de probar las aplicaciones dependientes para garantizar que no hayan sufrido efectos adversos.
2. Exporte la plantilla actual a un archivo con el procedimiento "Exportación de una plantilla de certificados desde Active Directory".
3. Siga el procedimiento descrito en "Eliminación de una plantilla de certificados" para eliminar definitivamente una plantilla de certificados del directorio.

Para deshacer la eliminación de una plantilla del directorio

- Siga el procedimiento para volver a importar la plantilla eliminada en "Importación de una plantilla de certificados en Active Directory".

Principio de la página

Solución de problemas

La solución de problemas se refiere a la Administración de incidentes y a las SMF de Administración de problemas. La Administración de incidentes se ocupa de restaurar el servicio lo antes posible. La Administración de problemas se ocupa principalmente de identificar las causas de origen de los incidentes e intentar impedir que vuelvan a producirse.

Esta sección se relaciona estrechamente con la sección "Tareas del cuadrante de compatibilidad". Muchos de los procedimientos de solución de problemas aquí indicados hacen referencia a tareas definidas en dicha sección.

En esta sección se identifican los incidentes de compatibilidad más habituales que pueden producirse, junto con las estrategias y los procedimientos para solucionarlos. Se resalta el hecho de poder restaurar el servicio lo antes posible. En algunos casos, el procedimiento de solución de problemas es una simple referencia a un procedimiento de compatibilidad. No obstante, en otros casos es necesario utilizar un procedimiento de diagnóstico más complejo.

La siguiente tabla enumera algunos de los principales incidentes de compatibilidad y sus posibles soluciones. La columna **Proceso de compatibilidad** enumera los procedimientos que se deben seguir. Estos procedimientos se

describen en detalle en la sección "Tareas del cuadrante de compatibilidad". Si no hay procesos en la lista, consulte el procedimiento de diagnóstico adecuado al problema de la siguiente sección.

Tabla 11.15: Principales incidentes de compatibilidad

Incidente	Descripción	Proceso de compatibilidad
El servidor no responde	El proceso del software no responde a las solicitudes del cliente ni a las herramientas administrativas.	Reinicio de Servicios de Certificate Server o bien Reinicio del servidor de la entidad emisora
Error en la publicación de la lista CRL	La lista CRL fue emitida por la entidad emisora, pero la última lista CRL no se ha publicado en Active Directory o en el Web.	Consulte el siguiente procedimiento de solución de problemas.
Lista CRL no emitida	La lista CRL actualizada no ha sido emitida por la entidad emisora.	Consulte el siguiente procedimiento detallado para la solución de problemas.
El cliente no puede inscribir el certificado	Error en la solicitud de inscripción del cliente.	Consulte el siguiente procedimiento detallado para la solución de problemas.
El cliente no puede inscribir un certificado automáticamente	Error en la solicitud de inscripción automática del cliente.	Consulte el siguiente procedimiento detallado para la solución de problemas.
Se ha instalado una actualización de seguridad que requiere reinicio	Se ha instalado una actualización de seguridad que requiere un reinicio de Windows.	Reinicio del servidor de la entidad emisora
Error de servidor permanente	Daños o error de hardware que requiere una restauración.	Restauración de la entidad emisora a partir de una copia de seguridad
Debe revocarse el certificado huérfano	Tras la restauración de la entidad emisora, los certificados emitidos después de la última copia de seguridad no estarán en la base de datos y no pueden revocarse de la manera habitual.	Revocación de un certificado huérfano
El servidor no puede restaurarse a tiempo para la emisión de la lista CRL o el certificado	La lista CRL o el certificado se tiene que volver a firmar con la clave de la entidad emisora para ampliar su período de validez.	Secuencia de tareas: 1. Restauración del certificado de la entidad emisora en un equipo temporal 2. Nueva firma de una lista CRL o un certificado para extender su validez
El certificado de entidad final perdió su carácter confidencial	La clave privada del certificado se ha perdido, revelado o ha quedado comprometida.	Revocación de un certificado de entidad final
El certificado de la entidad emisora perdió su carácter confidencial	La clave privada del certificado de la entidad emisora se ha perdido, revelado o ha quedado comprometida.	Revocación y reemplazo de una entidad emisora

El certificado de la entidad emisora raíz perdió su carácter confidencial	La clave privada del certificado de la entidad emisora se ha perdido, revelado o ha quedado comprometida.	Revocación y reemplazo de una entidad emisora raíz

Procedimientos adicionales para solución de problemas

Esta sección describe algunos procedimientos de solución de problemas que pueden resultar útiles para diagnosticar y solucionar algunos de los problemas que aparecen en la tabla anterior. Los procedimientos analizan la solución de los siguientes problemas habituales:

- Problemas de publicación de listas CRL
- Lista CRL no emitida
- El cliente no puede inscribirse
- El cliente no puede inscribir un certificado automáticamente

Problemas de publicación de listas CRL

Los problemas de publicación de listas CRL se indicarán mediante una alerta producida por la secuencia de comandos CheckCRLs descrita en la sección "Supervisión y control de servicios". Esta alerta se desencadenará cuando una lista CRL no se pueda publicar en Active Directory y/o servidor Web de modo oportuno. Las aplicaciones que requieren comprobaciones de revocación comenzarán a causar errores si el problema no se corrige.

Examine la entrada del registro de sucesos de aplicación producido por CheckCRLs. Esta entrada debe indicar de modo más preciso cuál es el problema, así como indicar también a qué entidad emisora pertenece el CDP o la lista CRL con problemas. El problema será uno de los siguientes:

- La entidad emisora no ha emitido una lista CRL actualizada. Este problema indica un problema con la propia entidad emisora de certificados.
- La lista CRL se ha emitido, pero no se ha publicado correctamente en uno o varios CDP. Este error puede indicar un problema con la entidad emisora, con las comunicaciones entre la entidad y el CDP o con el servicio de CDP (Active Directory o IIS).
- La lista CRL se ha creado y publicado, pero no puede recuperarse de una o varias ubicaciones de CDP. Este error indica un problema con el servicio CDP.

Para solucionar los problemas de publicación de listas CRL

1. Inicie sesión en la entidad emisora donde hay problemas y compruebe si la lista CRL de la entidad emisora está actualizada. Escriba los siguientes comandos para ver la lista CRL de la entidad emisora (tiene que ser miembro de Administradores de entidad emisora para ejecutar el primer comando).

   Certutil -getCRL %temp%\CA.crl

   Certutil -dump %temp%\CA.crl

2. Si la lista CRL no está actualizada, consulte el procedimiento "Lista CRL no emitida" que se indica más adelante.

3. Abra la herramienta Estado de PKI y observe las entradas de CDP de la entidad emisora dudosa. La herramienta indicará los CDP inaccesibles y las listas CRL caducadas. (No obstante, la herramienta no advertirá sobre las listas CRL que aún no caducaron pero cuya renovación está atrasada; es decir, cuando haya pasado la fecha de **Siguiente publicación de lista CRL**.)

   Nota: puede obtener la herramienta Estado de PKI del Kit de recursos de Windows Server 2003, al que se hace referencia al final de este capítulo.

4. Si alguno de los CDP se muestra como inaccesible, investigue el servicio de publicación de dicho CDP.

5. Si se muestra un error (desde el registro de sucesos) con el CDP de LDAP, compruebe el vínculo al controlador de dominio de Active Directory desde la entidad emisora con DCDiag de las herramientas de soporte técnico de Windows Server 2003. Esta herramienta indicará si hay problemas con el controlador de dominio o con la conexión de la entidad emisora al controlador de dominio. Investigue los errores.

6. Compruebe los permisos en el contenedor de CDP de la entidad emisora con el complemento Sitios y servicios de Active Directory de MMC. (En "cn=CDP,cn=Public Key Services,cn=Services, cn=Configuration,*DC=woodgrovebank,DC=com"*, reemplace los elementos que aparecen en cursiva por el DN de su propia raíz de bosque.)

7. Cree una cuenta temporal y agréguela al grupo Publicadores de certificados. Inicie la sesión con dicha cuenta e intente publicar manualmente la lista CRL que se ha recuperado en el paso 1 en el directorio. Utilice el siguiente comando:

   certutil -dspublish CA.crl *NombreHostCA NombreSujetoCA*.

   Este comando indicará si las entidades emisoras tienen permisos suficientes para publicar en Active Directory.

8. Si se muestra un error (en la entrada del registro de sucesos) con el CDP de HTTP, compruebe el servidor IIS que está implicado. Compruebe la conectividad y los permisos. Ejecute manualmente la secuencia de comandos para publicar listas CRL en el servidor IIS (consulte "Publicación de las listas CRL de entidad emisora en el servidor Web" en la sección "Tareas del cuadrante operativo") y compruebe si hay errores. Intente utilizar la misma pertenencia a cuenta/grupo como la propia entidad emisora al realizar esta tarea.

9. Si las listas CRL se publican en los servicios CDP correctamente pero Estado de PKI muestra un error, esto indica un problema con el servicio de CDP (Active Directory o el propio IIS). La solución de problemas de estos servicios se encuentra fuera del ámbito de este documento.

Lista CRL no emitida

Ésta es una situación improbable en el funcionamiento normal. Una entidad emisora generalmente puede publicar siempre una lista CRL localmente a menos que haya vuelto a configurar la entidad emisora para que deje de publicar listas CRL en su carpeta de sistema local (%windir%\system32\certsrv\certenroll). Si no ha vuelto a configurar la ruta de acceso de publicación local, es posible que se haya producido un problema grave con su entidad emisora. Realice el siguiente procedimiento de solución de problemas para determinar la causa del problema. Si bien este procedimiento se centra en los problemas de listas CRL, la mayoría de los pasos son genéricos y pueden utilizarse con cualquier problema de Servicios de Certificate Server de bajo nivel.

Para solucionar el problema de emisión de listas CRL

1. Examine el registro de sucesos para ver si hay errores registrados por Servicios de Certificate Server.

2. Intente forzar manualmente una emisión de lista CRL (inicie sesión como miembro de Administradores de entidad emisora) con el siguiente comando:

   Certutil -CRL

3. Si se produce un error en este paso, vuelva a examinar el registro de sucesos para ver si hay nuevos errores.

4. Examine el certificado de la entidad emisora y todos los certificados en la cadena a la entidad emisora raíz para ver si hay problemas con los certificados, como certificados que hayan caducado o se hayan revocado.

5. Compruebe que puede volver a firmar un certificado o una lista CRL con la clave de entidad emisora (consulte el procedimiento "Nueva firma de una lista CRL o un certificado para extender su validez" en la sección "Tareas del cuadrante de compatibilidad").

6. Reinicie la entidad emisora y vuelva a ejecutar estas comprobaciones.

   Si sigue sin emitirse la lista CRL, active el registro de depuración (consulte "Registro de Servicios de

7. Certificate Server" más adelante en este capítulo). A continuación, intente emitir la lista CRL y examine el registro para ver si hay errores.

El cliente no puede inscribir un certificado

Siga este procedimiento para diagnosticar problemas con la inscripción de certificados.

Para diagnosticar un problema de inscripción de certificados

1. Compruebe que la plantilla de certificados se haya asignado a una entidad emisora.
2. Compruebe que el usuario o el equipo tenga permisos para inscribirse en la entidad emisora donde se ha asignado la plantilla.
3. Compruebe que la plantilla corresponde al tipo de sujeto. Los usuarios sólo pueden inscribirse a plantillas de usuario y los equipos sólo pueden inscribirse a plantillas de equipo.
4. Compruebe que la entidad emisora tenga acceso a sus propias listas CRL publicadas y a las de su entidad emisora principal. La entidad emisora siempre realiza una comprobación de revocación antes de emitir un certificado.
5. Compruebe que la plantilla de certificados no imponga el uso de CSP no disponibles para el sujeto que realiza la inscripción. Por ejemplo, CSP de tarjeta inteligente para un equipo o (si el usuario no tiene una tarjeta inteligente) CPS de SChannel de RSA para usuarios.
6. Compruebe que la plantilla de certificados no requiera introducir información en los campos **Sujeto** o **Sujeto alternativo**, que no existen en Active Directory. Un problema habitual consiste en especificar que la dirección de correo electrónico se incluya en el nombre del sujeto sin tener completamente rellenado el campo de correo electrónico en el objeto Active Directory del usuario.

El cliente no puede inscribir un certificado automáticamente

La guía definitiva para la comprensión y solución de problemas de inscripción automática puede encontrarse en el artículo "Inscripción automática de certificados en Windows XP" (consulte la referencia al final de este capítulo).

Compruebe que un cliente pueda inscribir manualmente el certificado que está tratando de inscribir automáticamente. Cargue el complemento Certificados de MMC y solicite un certificado nuevo. Si el tipo de certificado no aparece o si aparece pero se produce un error al intentar inscribir, siga el procedimiento de la sección anterior "El cliente no puede inscribir un certificado".

Si puede realizarse una inscripción manual, siga con los siguientes pasos.

1. Compruebe que se utilice la plataforma correcta. Sólo Windows 2000 y versiones posteriores admiten la inscripción automática de certificados de equipo. Sólo Windows XP y Windows Server 2003 admiten la inscripción automática de certificados de usuario.
2. Compruebe que el usuario o el equipo tenga permisos de Inscripción automática en la plantilla de certificados para el tipo de certificado requerido.
3. Compruebe que el parámetro Directiva de grupo de inscripción automática se haya especificado correctamente. Para que la inscripción automática funcione correctamente, es necesario que el GPO en el que está configurada la inscripción automática tenga una prioridad más alta que los otros GPO. Por ejemplo, si el GPO de inscripción automática se crea en el nivel de dominio, es necesario que el mismo tenga una prioridad más alta que la directiva de dominio predeterminada. Puede comprobar esta prioridad de los GPO con el complemento Conjuntos resultantes de directivas de MMC.
4. Compruebe que la plantilla de certificados no requiera una aprobación manual o firmas de la Autoridad de registro (RA). Las solicitudes de certificado que requieran la aprobación del administrador de certificados se enviarán para su aprobación, pero el certificado no se emitirá al usuario hasta que se apruebe manualmente. Las solicitudes que requieran firmas de la RA se rechazarán porque no hay ningún mecanismo para agregar firmas adicionales a una solicitud de inscripción automática.
5. Compruebe que la plantilla de certificados no esté establecida para que la información del sujeto se suministre en la solicitud. Los certificados con inscripción automática deben tener el sujeto (y el sujeto

alternativo) establecido por la entidad emisora.

Herramientas y técnicas para solución de problemas

Esta sección analiza algunas herramientas que son útiles para diagnosticar y solucionar problemas con la PKI. También describe el registro de Servicios de Certificate Server y cómo se activa un registro más detallado para Servicios de Certificate Server y la inscripción automática de clientes.

Estado de PKI

El Estado de PKI es fundamentalmente una herramienta de diagnóstico de CDP y AIA que intenta generar una vista de todas las entidades emisoras de la empresa. Resulta muy útil para diagnosticar la conectividad y problemas de publicación de CDP y AIA; permite descargar y ver las listas CRL o los certificados a los que hace referencia el CDP o AIA. La herramienta se encuentra disponible como parte del Kit de recursos de Windows Server 2003.

Certutil

Certutil es la herramienta individual más importante para administrar y solucionar problemas de las entidades emisoras de Windows. Para analizar algunos de los usos principales de la herramienta, consulte las notas del producto "Utilización de Certutil.exe para administrar y solucionar problemas de Servicios de Certificate Server, a las que se hace referencia al final de este capítulo.

Sin embargo, también hay otras opciones (que no se describen en estas notas del producto) disponibles para una amplia variedad de propósitos de administración y diagnóstico. Puede mostrar la lista completa de las acciones (o verbos) de Certutil disponibles si escribe el comando con el parámetro "-?". Si inserta el verbo acerca del que necesite más ayuda se mostrará la sintaxis detallada de dicha acción. Por ejemplo:

Certutil -dsPublish -?

Otras herramientas de diagnóstico

Otras herramientas de diagnóstico y administración útiles son:

- **Certreq.exe**. Permite crear, enviar y recuperar solicitudes de certificados desde la línea de comandos.
- **DCDiag.exe**. Resulta útil para diagnosticar problemas de Active Directory que pueden afectar a las entidades emisoras.

Registro de Servicios de Certificate Server

Servicios de Certificate Server y sus herramientas asociadas producen diversos tipos de registros que pueden resultar indispensables para la solución de problemas.

- Servicios de Certificate Server (el propio proceso de entidad emisora) se registra en %systemroot%\certsrv.log (cuando el registro de depuración se encuentra activado).
- Certutil.exe se registra en %systemroot%\certutil.log.
- Entidad emisora de certificados de MMC se registra en %windir%\certmmc.log.

Para activar el registro de depuración en Servicios de Certificate Server

- Ejecute el siguiente comando:

  certutil -setreg CA\Debug 0xfffffffe3

Las entradas se registro se guardarán en %windir%\certsrv.log

Para desactivar el registro de depuración

- Ejecute el siguiente comando:

  certutil -delreg CA\Debug

Registro de inscripciones automáticas

Tiene que agregar un valor del Registro para habilitar el registro adicional de los sucesos de inscripción automática. El registro mejorado se habilita individualmente para la inscripción automática de certificados de

usuarios y equipos.

Para activar el registro de inscripciones automáticas de usuarios

1. Cree un nuevo valor de Registro DWORD denominado **AEEventLogLevel** en la clave HKEY_CURRENT_USER\Software\Microsoft\Cryptography\Autoenrollment.
2. Establezca el valor en **0**.

Para activar el registro de inscripciones automáticas de equipos

1. Cree un nuevo valor de Registro DWORD denominado **AEEventLogLevel** en la clave HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Autoenrollment.
2. Establezca el valor en **0**.

   Nota: todos los errores se registran automáticamente. No es necesario activar la clave de registro para activar el registro de errores.

Principio de la página

Tablas de configuración

En las tablas siguientes encontrará los valores de configuración específicos del sitio y de la solución que se utilizan en los procedimientos descritos en este capítulo. Estas tablas constituyen un subconjunto de las tablas de configuración de planeamiento del capítulo 7, "Implementación de la infraestructura de claves públicas" y sólo se muestran como referencia.

Tabla 11.16: Elementos de la configuración definidos por el usuario

Elemento de configuración	Configuración
Nombre DNS del dominio raíz del bosque de Active Directory	woodgrovebank.com
Nombre de dominio de la raíz del bosque	DC=woodgrovebank,DC=com
Nombre del servidor de la entidad emisora raíz	HQ-CA-01
Nombre del servidor de la entidad emisora	HQ-CA-02
X.500 CN de la entidad emisora raíz	Entidad emisora raíz de Woodgrove Bank
X.500 CN de la entidad emisora	Entidad emisora de Woodgrove Bank 1
Nombre de host completo del servidor Web utilizado para publicar información de certificados de entidad emisora y revocaciones	www.woodgrovebank.com

Tabla 11.17: Elementos de configuración definidos por la solución

Elemento de configuración	Configuración
Contenedor de configuración de los administradores de servicios de claves públicas	Administradores de PKI de empresa
Pueden publicar listas CRL y certificados de entidad emisora en el contenedor de configuración de la empresa	Editores de PKI de empresa
Grupo administrativo que configura y mantiene las entidades emisoras; también controla la posibilidad de asignar todas las demás funciones de entidad emisora y de renovar el certificado de entidad emisora	Administradores de entidad emisora
Grupo administrativo que aprueba la inscripción de certificados y las	Administradores de certificados

solicitudes de revocación; función Directivo de entidad emisora	
Grupo administrativo que administra las auditorías y los registros de seguridad de la entidad emisora	Auditores de entidad emisora
Grupo administrativo que administra las copias de seguridad de la entidad emisora	Operadores de copia de seguridad de CA
Nombre del directorio virtual de IIS utilizado para publicar información de certificados de entidad emisora y lista de revocación de certificados (CRL)	pki
Ruta de acceso física en la entidad emisora que se asigna al directorio virtual de IIS	C:\CAWWWPub
Unidad y ruta de acceso para guardar los archivos de solicitud de Servicios de Certificate Server	C:\CAConfig
Unidad y ruta de acceso para guardar la base de datos de Servicios de Certificate Server	%systemroot%\System32\CertLog
Unidad y ruta de acceso para guardar los registros de base de datos de Servicios de Certificate Server	D:\CertLog
Ruta de acceso de las secuencias de comandos de instalación	C:\MSSScripts

Principio de la página

Información adicional

- Un documento actualizado, "Managing a Windows Server 2003 PKI ", basado en este capítulo también está disponible en www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/mngpki.mspx.
- Para obtener más información acerca del modelo de proceso y el modelo de equipo de MOF, consulte la página de Microsoft Operations Framework en www.microsoft.com/technet/itsolutions/techguide/mof/default.mspx.
- Para obtener más información acerca de las restricciones de capacidad y los contadores de rendimiento relacionados, consulte el artículo Q146005 de Microsoft Knowledge Base, "Optimizing Windows NT for Performance", en http://support.microsoft.com/default.aspx?kbid=146005.
- Para obtener información acerca de la implementación de MOM, descargue la guía *Microsoft Operations Manager 2000 (MOM) Service Pack 1 (SP1) Operations Guide* en www.microsoft.com/downloads/details.aspx?FamilyID=556A7746-75DF-4ACD-8CDE-26CB12148161&displaylang=en.
- Para obtener más información acerca de las tareas operativas adicionales, consulte la página Administer a certification authority en www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_CS_procs_admin.mspx.
- Para obtener más información acerca de la administración de revisiones de seguridad en la plataforma de Microsoft, consulte "Improve Platform Manageability – Best Practice: Security Patch Management" en http://go.microsoft.com/fwlink/?LinkId=16284.
- Para obtener información acerca de la administración de revisiones con Microsoft SMS 2003, consulte "Patch Management Using Microsoft Systems Management Server 2003" en www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/2003/pmsms031.mspx.
- Para obtener información acerca de la administración de revisiones con Microsoft SMS 2.0, consulte "Patch Management Using Microsoft Systems Management Server 2.0" en www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsms/20/pmsmsin.mspx.
- Para obtener información acerca de la administración de revisiones con los Servicios de actualización de

software de Microsoft, consulte "Patch Management Using Microsoft Software Update" en www.microsoft.com/technet/itsolutions/techguide/msm/swdist/pmsus/pmsus251.mspx.

- Para obtener información detallada acerca de las propiedades de las plantillas de certificados, consulte "Plantillas de certificados" en la Ayuda del producto en línea en www.microsoft.com/technet/prodtechnol/windowsserver2003/proddocs/entserver/ctcon_concepts_under.mspx.
- Para obtener más información acerca de cómo obtener y utilizar la Consola de administración de directivas de grupo, consulte "Enterprise Management with the Group Policy Management Console" en www.microsoft.com/windowsserver2003/gpmc/default.mspx.
- Para obtener más información acerca de los problemas de publicación de listas CRL, consulte Troubleshooting Certificate Status and Revocation en www.microsoft.com/technet/prodtechnol/WinXPPro/support/tshtcrl.mspx.
- Para obtener la herramienta Estado de PKI (PKIView.msc), descargue las herramientas del Kit de recursos de Windows Server 2003 en www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-96ee-b18c4790cffd&DisplayLang=en.
- Para obtener instrucciones de solución de problemas de Certutil, consulte las notas del producto "Utilización de Certutil.exe para administrar y solucionar problemas de Servicios de Certificate Server" en www.microsoft.com/windows2000/techinfo/administration/security/certutil.asp.
- Para obtener la guía definitiva para la comprensión y la solución de problemas de inscripción automática, consulte el artículo "Inscripción automática de certificados en Windows XP" en www.microsoft.com/technet/prodtechnol/winxppro/maintain/certenrl.mspx.

Principio de la página

Administre su perfil

©2008 Microsoft Corporation. Todos los derechos reservados. Póngase en contacto con nosotros | Aviso Legal | Marcas registradas | Privacidad