

Publique los Lista de revocación de certificados (CRL) para el ISE en un ejemplo de configuración del Microsoft CA server

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Configuraciones](#)

[La sección 1. crea y configura una carpeta en CA para contener los archivos CRL](#)

[La sección 2. crea un sitio en el IIS para exponer el nuevo CRL Distribution Point](#)

[Microsoft CA server de la configuración de la sección 3. para publicar los archivos CRL al punto de distribución](#)

[La sección 4. verifica el archivo CRL existe y es accesible vía el IIS](#)

[Configuración ISE de la sección 5. para utilizar el nuevo CRL Distribution Point](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración de un servidor de Microsoft Certificate Authority (CA) que dirija los Servicios de Internet Information Server (IIS) para publicar las actualizaciones de Listas de revocación de certificados (CRL). También explica cómo configurar el Cisco Identity Services Engine (ISE) (versiones 1.1 y posterior) para extraer las actualizaciones para el uso en la validación de certificado. El ISE se puede configurar para extraer los CRL para los diversos certificados raíz de CA que utiliza en la validación de certificado.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y

hardware.

- Versión 1.1.2.145 del Cisco Identity Services Engine
- R2 2008 del [®] del servidor del [®] de Microsoft Windows

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

En este documento, se utilizan estas configuraciones:

- La sección 1. crea y configura una carpeta en CA para contener los archivos CRL
- La sección 2. crea un sitio en el IIS para exponer el nuevo CRL Distribution Point
- Microsoft CA server de la configuración de la sección 3. para publicar los archivos CRL al punto de distribución
- La sección 4. verifica el archivo CRL existe y es accesible vía el IIS
- Configuración ISE de la sección 5. para utilizar el nuevo CRL Distribution Point

La sección 1. crea y configura una carpeta en CA para contener los archivos CRL

La primera tarea es configurar una ubicación en el servidor de CA para salvar los archivos CRL. Por abandono, el Microsoft CA server publica los archivos a C:\Windows\system32\CertSrv\CertEnroll\. Bastante que esta carpeta del sistema, crean una nueva carpeta para los archivos.

1. En el servidor IIS, elija una ubicación en el sistema de archivos y cree una nueva carpeta. En este ejemplo, se crea la carpeta C:\CRLDistribution.
2. Para que CA escriba los archivos CRL a la nueva carpeta, compartiendo debe ser habilitado. Haga clic con el botón derecho del ratón la nueva carpeta, elija las **propiedades**, haga clic la lengüeta de **distribución**, y después haga clic la **distribución avanzada**.
3. Para compartir la carpeta, marque la **parte esto casilla de selección de carpeta** y después agregue una muestra de dólar (\$) al final del nombre de la parte en el campo de nombre de la parte de ocultar la parte.

4. Haga clic los **permisos** (1), el tecleo **agrega** (2), hace clic los **tipos de objeto** (3), y marca la casilla de verificación de las **Computadoras** (4).
5. Para volver a la ventana selecta de los usuarios, de las Computadoras, de las Cuentas de servicio, o de grupos, **AUTORIZACIÓN** del tecleo. En el ingresar los nombres del objeto para seleccionar el campo, ingresar el nombre de computadora del servidor y del tecleo CA **marcan los nombres**. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click OK.
6. En el grupo o el campo de Nombres de usuario, elija el ordenador de CA. El control **permite** para que el control total conceda el acceso total al Haga Click en OK CA. Haga Click en OK otra vez para cerrar la ventana de distribución avanzada y a volver a la ventana de pPropiedades.
7. Para permitir que CA escriba los archivos CRL a la nueva carpeta, configure los permisos de seguridad apropiados. Haga clic la **ficha de seguridad** (1), el tecleo **edita** (2), el tecleo **agrega** (3), hace clic los **tipos de objeto** (4), y marca la casilla de verificación de las **Computadoras** (5).
8. En el ingresar los nombres del objeto para seleccionar el campo, ingresar el nombre de computadora del servidor y del tecleo CA **marcan los nombres**. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click OK.
9. Elija el ordenador de CA en el grupo o el campo de Nombres de usuario y después marque **tienen en cuenta** para que el control total conceda el acceso total al Haga Click en OK CA y después haga clic **cerca de** completo la tarea.

[La sección 2. crea un sitio en el IIS para exponer el nuevo CRL Distribution Point](#)

Para que el ISE acceda los archivos CRL, haga el directorio que contiene los archivos CRL accesibles vía el IIS.

1. En el taskbar del servidor IIS, haga clic el **comienzo**. Elija **Administrative Tools > administrador de los Servicios de Internet Information Server (IIS)**.
2. En el panel izquierdo (conocido como el árbol de la consola), amplíe el nombre de servidor IIS y después amplíe los **sitios**.
3. Haga clic con el botón derecho del ratón el **Sitio Web predeterminado** y elija **agregan el directorio virtual**.
4. En el campo del alias, ingrese un nombre del sitio para el CRL Distribution Point. En este ejemplo, se ingresa CRLD.
5. Haga clic los puntos de suspensión (...) a la derecha del campo de la ruta física y hojee a la carpeta creada en la sección 1. selecta la carpeta y haga clic la **AUTORIZACIÓN**. Haga Click en OK para cerrar la ventana del directorio virtual del agregar.
6. El nombre del sitio ingresado en el paso 4 se debe resaltar en el panel izquierdo. Si no, ahora elíjalo. En el centro cristal, **directorio del clic doble que hojea**.
7. En el panel derecho, **permiso del tecleo** para habilitar el directorio que hojea.
8. En el panel izquierdo, elija el nombre del sitio otra vez. En el centro cristal, **editor de la configuración del clic doble**.
9. En la lista desplegable de la sección, elija **system.webServer/la Seguridad/requestFiltering**. **En la lista desplegable allowDoubleEscaping**, elija verdad. **En el panel derecho**, el tecleo se aplica.

La carpeta debe ahora ser accesible vía el IIS.

Microsoft CA server de la configuración de la sección 3. para publicar los archivos CRL al punto de distribución

Ahora que una nueva carpeta se ha configurado para contener los archivos CRL y la carpeta se ha expuesto en el IIS, configure el Microsoft CA server para publicar los archivos CRL a la nueva ubicación.

1. En el taskbar del servidor de CA, haga clic el **comienzo**. Elija **Administrative Tools > Certificate Authority**.
2. En el panel izquierdo, haga clic con el botón derecho del ratón el nombre de CA. Elija las **propiedades** y después haga clic las **Extensiones** cuadro para agregar un nuevo CRL Distribution Point, haga click en Add
3. En el campo de la ubicación, ingrese la trayectoria a la carpeta creada y compartida en la sección 1. En el ejemplo en la sección 1, la trayectoria es:
`\\RTPAAA-DC1\CRLDistribution$\`
4. Con el campo de la ubicación poblado, elija el **<CaName>** de la lista desplegable variable y después haga clic el **separador de millares**.
5. De la lista desplegable variable, elija el **<CRLNameSuffix>** y después haga clic el **separador de millares**.
6. En el campo de la ubicación, añada .crl al final del fichero al final de la trayectoria. En este ejemplo, la ubicación es:
`\\RTPAAA-DC1\CRLDistribution$\<CaName><CRLNameSuffix>.crl`
7. Haga Click en OK a volver a la lengüeta de las Extensiones. Marque la **publicación CRL a esta** casilla de verificación de la **ubicación** (1) y después haga clic la **AUTORIZACIÓN** (2) para cerrar la ventana de pPropiedades. Un prompt aparece para que el permiso recomience los servicios de certificados del Active Directory. Tecleo **sí** (3).
8. En el panel izquierdo, el click derecho **revocó los Certificados**. Elija **todas las tareas > publican**. Asegúrese de que el nuevo CRL esté seleccionado y después haga clic la **AUTORIZACIÓN**.

El Microsoft CA server debe crear un nuevo archivo .crl en la carpeta creada en la sección 1. Si el nuevo archivo CRL se crea con éxito se hace clic no habrá diálogo después de que sea ACEPTABLE. Si un error se vuelve con respecto a la nueva carpeta del punto de distribución, relance cuidadosamente cada paso en esta sección.

La sección 4. verifica el archivo CRL existe y es accesible vía el IIS

Verifique los nuevos archivos CRL existen y eso son accesibles vía el IIS de otro puesto de trabajo antes de que usted comience esta sección.

1. En el servidor IIS, abra la carpeta creada en la sección 1. Debe haber un solo archivo .crl presente con la forma **<CANAME>.crl** donde está el nombre **<CANAME>** del servidor de CA. En este ejemplo, el nombre de fichero es:
`rtptaaa-CA.crl`
2. De un puesto de trabajo en la red (idealmente en la misma red que el nodo primario ISE Admin), abra a un buscador Web y hojee a `http:// <SERVER>/<CRLSITE>` donde está **<SERVER>** Nombre del servidor del servidor IIS configurado en la sección 2 y **<CRLSITE>** es el nombre del sitio elegido para el punto de distribución en la sección 2. En este ejemplo, el URL es:

Las visualizaciones del índice del directorio, que incluye el archivo observaron en el paso 1.

[Configuración ISE de la sección 5. para utilizar el nuevo CRL Distribution Point](#)

Antes de que el ISE se configure para extraer el CRL, defina el intervalo para publicar el CRL. La estrategia para determinar este intervalo está fuera del alcance de este documento. Los valores potenciales (en Microsoft CA) son 1 hora a 411 años, de inclusivo. El valor predeterminado es 1 semana. Una vez que un intervalo apropiado para su entorno se ha determinado, fije el intervalo con estas instrucciones:

1. En el taskbar del servidor de CA, haga clic el **comienzo**. Elija **Administrative Tools > Certificate Authority**.
2. En el panel izquierdo, amplíe el click derecho CA la carpeta **revocada de los Certificados** y elija las **propiedades**.
3. En los campos del intervalo de la publicación del CRL, ingrese el número requerido y elija el período de tiempo. Haga Click en OK para cerrar la ventana y para aplicar el cambio. En este ejemplo, un intervalo de la publicación de 7 días se configura. Usted debe ahora confirmar varios valores de registro, que ayudarán a determinar las configuraciones de la extracción del CRL en el ISE.
4. Ingrese el **certutil - el getreg CA \ comando de Clock*** de confirmar el valor de ClockSkew. El valor predeterminado es 10 minutos. Salida de ejemplo:

```
Values:
    ClockSkewMinutes      REG_DWORDS = a (10)
CertUtil: -getreg command completed successfully.
```

5. Ingrese el **certutil - el getreg CA \ comando de CRLOv*** de verificar si el CRLOverlapPeriod se ha fijado manualmente. Por abandono el valor de CRLOverlapUnit es 0, que indica que no se ha fijado ningún valor manual. Si el valor es un valor con excepción de 0, registre el valor y las unidades. Salida de ejemplo:

```
Values:
    CRLOverlapPeriod      REG_SZ = Hours
    CRLOverlapUnits       REG_DWORD = 0
CertUtil: -getreg command completed successfully.
```

6. Ingrese el **certutil - el getreg CA \ comando de CRLpe*** de verificar el CRLPeriod, que fue fijado en el paso 3. Salida de ejemplo:

```
Values:
    CRLPeriod             REG_SZ = Days
    CRLUnits               REG_DWORD = 7
CertUtil: -getreg command completed successfully.
```

7. Calcule el período de gracia CRL como sigue: Si CRLOverlapPeriod fue fijado en el paso 5: COINCIDENCIA = CRLOverlapPeriod, en los minutos; COINCIDENCIA = (CRLPeriod/10), en los minutos Si COINCIDENCIA > entonces COINCIDENCIA 720 = 720 Si COINCIDENCIA < (1.5 * COINCIDENCIA de ClockSkewMinutes) entonces = (1.5 * ClockSkewMinutes) Si COINCIDENCIA > CRLPeriod, en la COINCIDENCIA de los minutos entonces = CRLPeriod en los minutos Período de gracia = 720 minutos + 10 minutos = 730 minutos Ejemplo:

```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and
CRLOverlapPeriod was not set.
```

a. OVERLAP = (10248 / 10) = 1024.8 minutes

- b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
- c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes
- d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
- e. Grace Period = 720 minutes + 10 minutes = 730 minutes

El período de gracia calculado es la cantidad de tiempo entre cuando CA publica el CRL siguiente y cuando expira el CRL actual. El ISE necesita ser configurado para extraer los CRL por consiguiente.

8. Inicie sesión al nodo primario Admin y elija la **administración > el sistema > los Certificados**. En el panel izquierdo, seleccione el **almacén de certificados**.
9. Marque la casilla de verificación del almacén de certificados al lado del certificado de CA para las cuales usted se prepone configurar los CRL. Haga clic en **Editar**.
10. Cerca de la parte inferior de la ventana, marque la casilla de verificación de la **descarga CRL**.
11. En el campo URL de la distribución CRL, ingrese la trayectoria al CRL Distribution Point, que incluye el archivo .crl, creado en la sección 2. En este ejemplo, el URL es:
`http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl`
12. El ISE se puede configurar para extraer el CRL a intervalos regulares o basar en la expiración (que, es generalmente también un intervalo regular). Cuando el CRL publica se obtiene el intervalo es parásitos atmosféricos, actualizaciones más oportunas CRL cuando se utiliza la última opción. Haga clic **automáticamente** el botón de radio.
13. Fije el valor para la extracción a un valor menos que el período de gracia calculado en el paso 7. Si el valor establecido valor establecido es más largo que el período de gracia, el ISE marca el CRL Distribution Point antes de que CA haya publicado el CRL siguiente. En este ejemplo, el período de gracia se calcula para ser 730 minutos, o 12 horas y 10 minutos. Un valor de 10 horas será utilizado para la extracción.
14. Fije el intervalo entre reintentos como apropiado para su entorno. Si el ISE no puede extraer el CRL en el intervalo configurado en el paso anterior, revisará en este intervalo más corto.
15. Marque la **verificación de puente CRL si el CRL no es** casilla de verificación **recibida** para permitir que proceda la autenticación basada en el certificado normalmente (y sin un control CRL) si el ISE no podía extraer el CRL para este CA en su tentativa más reciente de la descarga. Si esta casilla de verificación no se marca, toda la autenticación basada en el certificado con los Certificados publicados por este CA fallará si el CRL no puede ser extraído.
16. Marque la **negligencia que el CRL no es** casilla de verificación **todavía válida o expirada** para permitir que el ISE utilice (o no todavía válido) los archivos expirados CRL como si eran válidos. Si esta casilla de verificación no se marca, el ISE considera un CRL ser inválido antes de su fecha de entrada en vigor y después de sus horas de actualización próximas. **Salvaguardia del teclado** para completar la configuración.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Soporte Técnico y Documentación - Cisco Systems](#)