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

Contenido

Introducción prerrequisitos Requisitos **Componentes Utilizados Convenciones** Configurar Configuraciones La sección 1. crea y configura una carpeta en el CA para contener los ficheros CRL La sección 2. crea un sitio en el IIS para exponer la nueva punta de la distribución CRL La sección 3. configura el servidor de Microsoft CA para publicar los ficheros CRL a la punta de la distribución La sección 4. verifica que el fichero CRL exista y que sea accesible vía el IIS La sección 5. configura ISE para utilizar la nueva punta de la distribución CRL 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 del Listas de revocación de certificados (CRL). También explica cómo configurar el Cisco Identity Services Engine (ISE) (versiones 1.1 y más adelante) para extraer las actualizaciones para el uso en la validación de certificado. ISE se puede configurar para extraer los CRL para los diversos certificados raíz 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
- [®] 2008 R2 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 <u>Convenciones de Consejos Técnicos de Cisco</u> para obtener más información sobre las convenciones sobre documentos.

Configurar

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

Nota: Utilice la <u>herramienta de búsqueda de comandos</u> (<u>clientes registrados</u> solamente) para obtener más información sobre los comandos usados en esta sección.

Configuraciones

Este documento utiliza estas configuraciones:

- La sección 1. crea y configura una carpeta en el CA para contener los ficheros CRL
- La sección 2. crea un sitio en el IIS para exponer la nueva punta de la distribución CRL
- La sección 3. configura el servidor de Microsoft CA para publicar los ficheros CRL a la punta de la distribución
- La sección 4. verifica que el fichero CRL exista y que sea accesible vía el IIS
- La sección 5. configura ISE para utilizar la nueva punta de la distribución CRL

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

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

 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 el CA escriba los ficheros CRL a la nueva carpeta, compartiendo debe ser activado. Haga clic derecho la nueva carpeta, elija las **propiedades**, haga clic la tabulación de **distribución**, y después haga clic la **distribución**

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	
CRLDistribution Not Shared	
Network Path: Not Shared	
Share	
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	
Close Cancel App	y

- avanzada. 3. Para compartir la carpeta, controle 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

Ad	vanced Sharing
	Share this folder
	Settings
	Share name:
	CRLDistribution\$
	Add Remove
	Limit the number of simultaneous users to: 77216 芸
	Comments:
	Permissions Caching
	OK Cancel Apply

4. Haga clic los **permisos** (1), el tecleo **agrega** (2), hace clic los **tipos de objeto** (3), y controla la casilla de verificación de los **ordenadores**

Idvanced Sharing	🔋 Permissions for CRLDistribution\$	Select Users, Computers, Service Accounts, or Groups	7 3
V Share this folder	Share Permissions	Select this object type:	
Setting	Group or user names	Users, Groups, or Built in security principals 3	Object Types
Share name:	& Everyone	From this location	-
CRUDistribution\$		Inpasalocal	Locations
Add Remove		Enter the object names to select (examples):	
Limit the number of simultaneous us		Object Tymes	Chari Martan
Committee	2 Add. B	300 Calest the uses of chiects usu used to find	
Comments:		a seed me gres of objects you want to the	
	Permissions for Everyone Allow L	ery Object types:	
	Change	Generative Accounts	
1 Permissions Cadhing	Read	🗆 🛛 🦉 🕵 Computers 👍	
OK C			
	Learn about access control and permissions		
	OK Currel	Over A	Cancel

5. Para volver a la ventana selecta de los usuarios, de los ordenadores, 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 controlan los nombres. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click

Select Users, Computers, Service Accounts, or G	iroups	? ×
Select this object type:		
Users, Computers, Groups, or Built-in security principal	s	Object Types
From this location:		
rtpaaa.local		Locations
Enter the object names to select (examples):		
RTPAAA-DC1		Check Names
	_	
Advanced	OK	Cancel
	120	11

6. En el grupo o el campo de Nombres de usuario, elija el ordenador CA. El control **permite** para que el control total conceda el acceso total a la **AUTORIZACIÓN del** tecleo CA. Haga clic la **AUTORIZACIÓN** otra vez para cerrar la ventana de distribución avanzada y para volver a la ventana de

	Permissions for CRLDistribut	ion\$	×			
	Share Permissions					
	Group or user names:					
	Everyone	PAAA-DC1\$)				
	A-10.	Add	Remove			
	Permissions for RTPAAA-DC1	Allow	Deny			
	Full Control					
	Change					
	nead	M				
	Learn about access control and permissions					
nPropiedades	ОК	Cancel	Apply			

 Para permitir que el CA escriba los ficheros CRL a la nueva carpeta, configure los permisos de seguridad apropiados. Haga clic la ficha de seguridad (1), el tecleo corrige (2), el tecleo agrega (3), hace clic los tipos de objeto (4), y controla la casilla de verificación de los ordenadores



8. En el ingresar los nombres del objeto para seleccionar el campo, ingresar el nombre de computadora del servidor y del tecleo CA **controlan los nombres**. Si el nombre ingresado es válido, el nombre restaura y aparece subrayado. Click

elect Users, Computers, Service Accounts, or Groups	?
Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
rtpaaa.local	Locations
Enter the object names to select (<u>examples)</u> :	
RTPAAA-DC1	Check Names
Advanced OK	Cancel

OK.

9. Elija el ordenador CA en el grupo o el campo de Nombres de usuario y después controle **tienen en cuenta** para que el control total conceda el acceso total a la **AUTORIZACIÓN del** tecleo CA y después haga clic **cerca de** completo la

Security Object name: C:\CRLDistribution Group or user names: CREATOR OWNER SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAA-DC1\$) Users (RTPAAA\Users) Add Remove Permissions for RTPAAA\Users) Full control Modify Read & execute List folder contents Read	Permissions for CRLDistribution	on	
Object name: C:\CRLDistribution Group or user names: Image: CREATOR OWNER Image: SYSTEM SYSTEM Image: Administrators (RTPAAA\Administrators) Image: RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Image: RTPAAA-DC1 (RTPAAA\Users) Image: Add Remove Image: RTPAAA-DC1 Image: Add Remove Image: RTPAAA-DC1	Security		
Group or user names: CREATOR OWNER Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Object name: C:\CRLDistribution	n	
Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Group or user names:		
SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Add Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read Ist folder contents	& CREATOR OWNER		
Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	SYSTEM		
Add Add Add Add Remove Add Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read Ist folder contents Read Ist folder contents Ist folder contents <t< td=""><td>Administrators (RTPAAA\Adm</td><td>inistrators)</td><td></td></t<>	Administrators (RTPAAA\Adm	inistrators)	
Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control image: Cont		AAA-DUI\$j	
Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control image: Cont			
Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Image: Second s	1		_
Permissions for RTPAAA-DC1 Allow Deny Full control Image: Second se		Add	Remove
Full control Image: Control Modify Image: Control Read & execute Image: Control List folder contents Image: Control Read Image: Control	Permissions for RTPAAA-DC1	Allow	Deny
Modify Image: Constant series Read & execute Image: Constant series List folder contents Image: Constant series Read Image: Constant series	Full control		
Read & execute List folder contents Read	Modify		
List folder contents Read	Read & execute		
Read 🗹 🗖 🖵	List folder contents		
	Read		
			0
	OK	Cancel	Apply
OK Cancel Apply			

La sección 2. crea un sitio en el IIS para exponer la nueva punta de la distribución CRL

Para que ISE tenga acceso a los ficheros CRL, haga el directorio que contiene los ficheros CRL accesibles vía el IIS.

- 1. En el servidor IIS taskbar, haga clic el **comienzo**. Elija las **herramientas > al encargado** administrativos de los Servicios de Internet Information Server (IIS).
- 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 derecho el Sitio Web predeterminado y elija agregan el directorio

Threffier Information 3	Services (115) Manager
G S RTPA	AA-DC1 🔸 Sites 🔸 Default Web Sit
File View Help	
Connections	1.
Start Page Start Page RTPAAA-DC1 (RTPAA Application Pools Sites Default Web	AA\Administrator) Site Explore Edit Permissions Add Application Add Virtual Directory
	Edit Bindings Manage Web Site Refresh Remove Rename Switch to Content View

4. En el campo del alias, ingrese un nombre del sitio para la punta de la distribución CRL. En este ejemplo, se ingresa

Add	Virtual Di	rectory				?
S F	iite name: Path:	Default Wel	o Site			
A	ias:	_				
CF	RLD					
E>	ample: ima	ges				
Ph	ysical path					
Pa	ass-through	authenticatio	n			
	ionnect as.	Test Se	ettings			
				OK	Can	icel
)						

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. AUTORIZACIÓN del tecleo para cerrar la ventana del directorio virtual del

dd ¥irtual Di	rectory			?
Site name: Path:	Default Web Site /			
Alias:				
CRLD				
Example: ima	ges			
Physical path	:			
C:\CRLDistrib	ution			
Pass-through	authentication			
Connect as,	Test Settings	[
		ОК	Can	cel

agregar.

 El nombre del sitio ingresado en el paso 4 se debe destacar en el panel izquierdo. Si no, ahora elíjalo. En el centro cristal, directorio del doble clic que hojea.



7. En el panel derecho, **permiso del** tecleo para activar el directorio que hojea.

	Alerts
Directory Browsing	Directory bro
Use this feature to specify the information that displays in a directory listing.	Actions
Ime	E Apply
Size	Ex Cancel
Kension	Enable
M Date	🕜 Help
Long date	Online Help

8. En el panel izquierdo, elija el nombre del sitio otra vez. En el centro cristal, **editor de la configuración del** doble clic.



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.

► CRLD ►				
Section: system.webServer/security/reque	stFikering + From: Default Web Site/CRLD Web.config +	Actions		
Deepest Path: MACHINE (WERPOOT	ADDHOST	Generate Script		
allowDoubleEscaping	True	Configuration		
alowHighBitCharacters	True	Search Configuration		
alwaysAllowedQueryStrings	False	Search Configurat		
alwaysAllowedUrls	(count=o)	Section		
denyQueryStringSequences	(Count=0)	Lock Section		
denyUrlSequences	(Count=0)	LOCK SECOUR		
fileExtensions		allowDoubleEscapi		
filteringRules	(Count=0)	Attribute		
hidden5egments		Lock Attribute		
requestLimits		D Heb		
unescapeQueryString	True	a rich		
verbs		Online Help		

La carpeta debe ahora ser accesible vía el IIS.

La sección 3. configura el servidor de Microsoft CA para publicar los ficheros CRL a la punta de la distribución

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

- 1. En el servidor CA taskbar, haga clic el **comienzo**. Elija las **herramientas > la autoridad de certificación administrativas**.
- 2. En el panel izquierdo, haga clic derecho el nombre CA. Elija las **propiedades** y después haga clic las **Extensiones** cuadro para agregar una nueva punta de la distribución CRL, tecleo

Enrollment Agents	Auditing Recovery Agents Secur
General	Policy Module Exit Module
Extensions	Storage Certificate Managers
Select extension:	
CRL Distribution Point	: (CDP)
Specify locations from ((CRL).	which users can obtain a certificate revocation list
C:\Windows\system3.	2\CertSrv\CertEnroll\ <caname><crlnamesuffix catedName><cblnamesuffix>_CN=<servershort1< td=""></servershort1<></cblnamesuffix></crlnamesuffix </caname>
http:// <serverdnsna< td=""><td>ame>/CertEnroll/<caname><crlnamesuffix><de< td=""></de<></crlnamesuffix></caname></td></serverdnsna<>	ame>/CertEnroll/ <caname><crlnamesuffix><de< td=""></de<></crlnamesuffix></caname>
Tile://KServerUNSNar	me>/CertEnroll/ <caname><crenamesurfix><del< td=""></del<></crenamesurfix></caname>
	Add Remove
Publish CRLs to thi	Add Remove
 Publish CRLs to thi Include in all CRLs when publishing matching 	Add Remove is location . Specifies where to publish in the Active Directory anually.
 Publish CRLs to thi Include in all CRLs when publishing main Include in CRLs. Cl 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations.
 Publish CRLs to thi Include in all CRLs when publishing maintening maintening Include in CRLs. C Include in the CDP 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations. ' extension of issued certificates
 Publish CRLs to thi Include in all CRLs when publishing main include in CRLs. C Include in the CDP Publish Delta CRLs 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations. ' extension of issued certificates s to this location
 Publish CRLs to thi Include in all CRLs when publishing main include in CRLs. Cline in the CDP Include in the CDP Publish Delta CRLs 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations. ' extension of issued certificates s to this location extension of issued CBL s.
 Publish CRLs to thi Include in all CRLs when publishing main include in CRLs. C Include in the CDP Publish Delta CRLs Include in the IDP 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations. extension of issued certificates s to this location extension of issued CRLs
 Publish CRLs to thi Include in all CRLs when publishing mains Include in CRLs. C Include in the CDP Publish Delta CRLs Include in the IDP 	Add Remove is location . Specifies where to publish in the Active Directory anually. lients use this to find Delta CRL locations. extension of issued certificates s to this location extension of issued CRLs

- agregan. . En el campo de la ubio
- 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\$\

Add Location 🔀
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.
Location:
\\RTPAAA-DC1\CRLDistribution\$\
Variable:
<caname> Insert</caname>
Description of selected variable:
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""></crlna<></caname></serverdnsname>
•
OK Cancel

4. Con el campo de la ubicación poblado, elija el **<CaName> de la** lista desplegable variable y después haga clic el **separador de**

Add Location		
A location can be any valid U or enter a UNC or local path. the variable below and click I	IRL or path. Enter an HTTP, LD To insert a variable into the UR Insert.	AP, file addr L or path, se
Location:		
VRTPAAA-DC1\CRLDistribu	ution\$\ <caname></caname>	
Variable:		
<caname></caname>	<u> </u>	Insert
Description of selected variab	ole:	
Used in URLs and paths Inserts the DNS name of the Example location: http:// <se< td=""><td>server erverDNSName>/CertEnroll/<ca< td=""><td>aName><cr< td=""></cr<></td></ca<></td></se<>	server erverDNSName>/CertEnroll/ <ca< td=""><td>aName><cr< td=""></cr<></td></ca<>	aName> <cr< td=""></cr<>
•		
•	 ОК	Cance

5. De la lista desplegable variable, elija el **<CRLNameSuffix>** y después haga clic el **separador**

dd Location	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file address or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.	
Location:	
\\RTPAAA-DC1\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	
Variable:	1
<crlnamesuffix> Insert</crlnamesuffix>	J.
Description of selected variable:	-12
Used in URLs and paths for the CRL Distribution Points extension Appends a suffix to distinguish the CRL file name Example location: http:// <servername>/CertEnroll/<caname><crlnames< td=""><td>1</td></crlnames<></caname></servername>	1
<u>د</u>	
OK Cancel	

de millares.

6. En el campo de la ubicación, añada .crl al final del fichero al extremo de la trayectoria. En este ejemplo, la ubicación es:

\\RTPAAA-DC1\CRLDistribution\$\<CaName><CRLNameSuffix>.crl

dd Location			×
A location can be any valid URL or path or enter a UNC or local path. To insert a the variable below and click Insert.	. Enter ar variable i	h HTTP, LD nto the URI	AP, file address, L or path, select
Location:			_
\\RTPAAA-DC1\CRLDistribution\$\ <ca< td=""><td>Name><c< td=""><td>RLNameSu</td><td>uffix>.crl</td></c<></td></ca<>	Name> <c< td=""><td>RLNameSu</td><td>uffix>.crl</td></c<>	RLNameSu	uffix>.crl
Variable:			
<crlnamesuffix></crlnamesuffix>		-	Insert
Description of selected variable:			
Used in URLs and paths for the CRL Di Appends a suffix to distinguish the CRL Example location: http:// <servername></servername>	istribution file name >/CertEnro	Points exte oll/ <canam< td=""><td>nsion e><crlnamesi< td=""></crlnamesi<></td></canam<>	nsion e> <crlnamesi< td=""></crlnamesi<>
•			×
		ОК	Cancel

7. Haga clic la AUTORIZACIÓN para volver a las Extensiones cuadro. Controle 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 mensaje aparece para que el permiso recomience los servicios del certificado del Active Directory. Tecleo sí (3).

rtpaaa-CA Properties	
Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers	
Select extension:	
CRL Distribution Point (CDP)]]
Specify locations from which users can obtain a certificate revocation list (CRL).	a
Idap:///CN= <catruncatedname><crlnamesuffix>,CN=<servershortna http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta \\\RTPAAA-DC1\\CRLDistribution\$\\<caname><crlnamesuffix>.crl</crlnamesuffix></caname></delta </crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortna </crlnamesuffix></catruncatedname>	a a C
	1
Add Remove	1
1. Publish CRLs to this location	- 11
Include in all C Certification Authority when publishin	×
Include in CRL Include in the I Include in the I Include in the I	ate Services for the estart the service now?
🗖 Publish Delta (
Include in the I	Yes No
2 OK Cancel Apply Help	

8. En el panel izquierdo, el clic derecho **revocó los Certificados**. Elija **todas las tareas > publican**. Asegúrese de que el nuevo CRL esté seleccionado y después haga clic la **AUTORIZACIÓN**.



El servidor de Microsoft CA debe crear un nuevo fichero .crl en la carpeta creada en la sección 1. Si el nuevo fichero 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 de la punta de la distribución, relance cuidadosamente cada paso en esta sección.

La sección 4. verifica que el fichero CRL exista y que sea accesible vía el IIS

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

 En el servidor IIS, abra la carpeta creada en la sección 1. Debe haber un solo fichero .crl presente con la forma <CANAME>.crl donde está el nombre <CANAME> del servidor CA. En este ejemplo, el nombre de fichero es: rtpaaa-CA.crl

CRLDistribution\$				_ 🗆 🗵
Network -	rtpaaa-dc1 + CRLDistribution\$	÷ 🛱	Search CRLDistribution\$	2
Organize 🔻 📆 Open 👻	New folder		8=	• 🔟 😧
☆ Favorites	Name *	Date modified	Туре	Size
🧮 Desktop	E rtpaaa-CA	12/19/2012 5:45 PM	Certificate Revocation List	5 KB
🎉 Downloads 🔛 Recent Places	web.config	12/17/2012 5:04 PM	CONFIG File	1 KB
🥞 Libraries				
Documents				
Pictures				
Videos				
📜 Computer				
🕌 Local Disk (C:)				

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 el nombre <SERVER> de servidor del servidor IIS configurado en la sección 2 y <CRLSITE> es el nombre del sitio elegido para la punta de la distribución en la sección 2. En este ejemplo, el URL es:

http://RTPAAA-DC1/CRLD

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

	rtpaaa-dc1/	CRLD/			
🗍 rtpaaa-dc1 - /CRLD/	(+	-		
		ODI			
rtpaaa-d	c1 - /	CRL	D/		
rtpaaa-d	c1 - /(CRL	D/		
rtpaaa-d	c1 - /(4437	D/	·1	

La sección 5. configura ISE para utilizar la nueva punta de la distribución CRL

Antes de que 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 servidor CA taskbar, haga clic el **comienzo**. Elija las herramientas > la autoridad de

certificación administrativas.

- 2. En el panel izquierdo, amplíe el clic derecho CA la carpeta **revocada de los Certificados** y elija las **propiedades.**
- 3. En los campos del intervalo de la publicación CRL, ingrese el número requerido y elija el período de tiempo. Haga clic la AUTORIZACIÓN para cerrar la ventana y para aplicar el cambio. En este ejemplo, un intervalo de la publicación de 7 días se configura

a certsry - [Certification Aul	thority (Local)\rtpaa	a-CA\	Revoked Certificates]				
File Action View Help							
🗢 🧼 🖄 🔚 🖸 🕞	?						
Certification Authority (Local)	Request ID	Rev	Revoked Certificates Prope	rties			? × 🔺
🖂 🧖 rtpaaa-CA	6	5/8	CRL Publishing Parameters	/iew CRLs			
Revoked Certificates	Tasks	5/8					
Pending Reque		5/8	A Certificate Revocation List consider invalid	(CRL) desc	ribes certificates t	that clients sho	uld
Failed Request		5/8		_			
Certificate Ter Rel	fresh	5/8	CHL publication interval:	7	Days	-	
Exp	port List	5/8	Next update:	12/20	/2012 8:45 AM		
Pro	operties	5/8					
Hei	lp 5	5/8	Publish Delta CRLs				
	20	5/8	Publication interval:	1	Hours	-	
	29	5/8		1.	Jerours		
	2	5/8	Next update:				
	200134 C 105	5/8					
	Sel 36	5/8					
	37	5/8					
	39	5/8					
	40	5/9					
	41	5/3					
	201 46	5/3					
	201 ⁴⁸	6/2					
	50	6/2					
	I		OK	Cancel	Apply	Hel	
Opens the properties dialog box fo	or the current selection.	-					

Usted debe ahora confirmar varios valores de registro, que ayudarán a determinar las configuraciones de la extracción CRL en 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_DWORS = 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 minutosSi COINCIDENCIA > entonces COINCIDENCIA 720 = 720Si COINCIDENCIA < (1.5 * COINCIDENCIA de ClockSkewMinutes) entonces = (1.5 * ClockSkewMinutes)Si COINCIDENCIA > CRLPeriod, en la COINCIDENCIA de los minutos entonces = CRLPeriod en los minutosPeríodo de gracia = 720 minutos + 10 minutos = 730 minutosEjemplo: 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</li>
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 el CA publica el CRL siguiente y cuando expira el CRL actual. ISE necesita ser configurado para extraer los CRL por consiguiente.

 Ábrase una sesión al nodo primario Admin y elija la administración > el sistema > los Certificados. En el panel izquierdo, seleccione el almacén de certificados.

🔆 System 🛛 餐 Identity Management 👔	Nel	twork Resources	🛃 Web Port	al Management	La .		
Deployment Licensing Certificates Log	ging	Maintenance A	dmin Access	Settings			
Certificate Operations	1	Certificate Store					Selected 0 Total
🕵 Local Certificates		A Edit and Import	Chamart	Y Dalata	Show	AL	
Certificate Signing Requests	1	Friendle Marrie	- Coport	Autoria	ferring To	1.11	Issued By
Ocrtificate Store			F0_R41#rtna	20000242.cc	RTPAAA.DC1_MSC	"F0_R	rtnapa_CA
SCEP CA Profiles			-CA#00001	88-CH#00002	rtpaaa-CA	CEP These	rtpaaa-CA
•							

- 9. Controle la casilla de verificación del almacén de certificados al lado del certificado CA para el cual usted se prepone configurar los CRL. Haga clic en **Editar**.
- 10. Cerca de la parte inferior de la ventana, controle la casilla de verificación de la **transferencia directa CRL**.
- 11. En el campo URL de la distribución CRL, ingrese la trayectoria a la punta de la distribución CRL, que incluye el fichero .crl, creada en la sección 2. En este ejemplo, el URL es: http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
- 12. 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 establecidovalor establecido es más largo que el período de gracia, ISE controla la punta de la distribución CRL antes de que el 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 ISE no puede extraer el CRL en el intervalo configurado en el paso anterior, revisará en este intervalo más corto.
- 15. Controle la verificación de puente CRL si el CRL no es casilla de verificación recibida para permitir que proceda la autenticación certificado-basada normalmente (y sin un control CRL) si ISE no podía extraer el CRL para este CA en su tentativa pasada de la transferencia directa. Si esta casilla de verificación no se controla, toda la autenticación certificado-basada con los Certificados publicados por este CA fallará si el CRL no puede ser extraído.
- 16. Controle la negligencia que el CRL no es casilla de verificación todavía válida o expirada permitir que ISE utilice (o no todavía válido) los ficheros expirados CRL como si eran válidos. Si esta casilla de verificación no se controla, ISE considera un CRL ser inválido antes de su fecha de entrada en vigor y después de sus horas de actualización próximas. Salvaguardia del tecleo para completar la configuración.

Issued By	paaa-CA			
Valid From S	at, 11 Feb 2012 19:32:02 EST	•		
Valid To (Expiration)	Ved, 11 Feb 2037 19:42:01 ES	IT .		
Serial Number	D 85 1D 58 36 8C EC 93 4E F6	5 5B 28 9B 26 E7 89		
Jsage				
All Trust Certificates are availand administrative authent	lable for selection as the Root cation below:	CA for secure LDAP connection	ns. In addition, they may be en	abled for EAP-TLS
Trust for client authent	ication			
Enable Validation of	Certificate Extensions (accept o	only valid certificate)		
OCSP Configuration Validate against OCSP 5 Reject the request	ervice	*		
OCSP Configuration Ualidate against OCSP 5 Reject the reques Certificate Revocation I	ervice t if certificate status could not ist Configuration	+ be determined by OCSP		
OCSP Configuration Validate against OCSP Reject the reques Certificate Revocation I OWNload CRL	ervice t if certificate status could not ist Configuration	• be determined by OCSP		
OCSP Configuration Validate against OCSP Reject the reques Certificate Revocation I OVD Download CRL CRL Distribution U	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD	the determined by OCSP /rtpaaa-CA.crl		
OCSP Configuration Validate against OCSP S Reject the reques Certificate Revocation I Ocruiticate Revocation I CRL Distribution U Retrieve CRL	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD Automatically 10	be determined by OCSP /rtpaaa-CA.crl Ho	ours *	before expiration
DCSP Configuration Validate against OCSP S Reject the reques Certificate Revocation I Overlificate Revocation I CRL Distribution U Retrieve CRL	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD O Automatically 0 Every 0		ours 💌	before expirate
OCSP Configuration Ualidate against OCSP S Reject the reques Certificate Revocation I U Download CRL CRL Distribution U Retrieve CRL If download failed	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD O Automatically 0 Every 0		ours v /eeks before retry.	before expirate
OCSP Configuration Validate against OCSP S Reject the reques Certificate Revocation I ODWINID ORL CRL Distribution U Retrieve CRL If download failed Bypass CRL Vi	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD O Automatically 10 O Every 0 wait 1 rification if CRL is not Received		ours veeks veeks before retry.	before expirati
OCSP Configuration Validate against OCSP s Reject the reques Certificate Revocation I ✓ Download CRL CRL Distribution U Retrieve CRL If download failed ✓ Bypass CRL VA ☐ Ignore that C	ervice t if certificate status could not ist Configuration RL http://rtpaaa-dc1/CRLD O Automatically 0 Every wait 1 rification if CRL is not Received L is not yet valid or expired		ours Veeks Veeks before retry.	before expirati

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