Configurar Microsoft CA Server para publicar las listas de revocación de certificados para ISE

Contenido

Introducción
Requisito previo
Requirements
Componentes Utilizados
Configurar
Crear y configurar una carpeta en la CA para alojar los archivos CRL
Crear un sitio en IIS para exponer el nuevo punto de distribución CRL
Configurar Microsoft CA Server para publicar archivos CRL en el punto de distribución
Compruebe que el archivo CRL existe y que se puede obtener acceso a él mediante IIS
Configuración de ISE para utilizar el nuevo punto de distribución de CRL
Verificación
Troubleshoot

Introducción

Este documento describe la configuración de un servidor de la Autoridad de certificados (CA) de Microsoft que ejecuta Servicios de Internet Information Server (IIS) para publicar las actualizaciones de la Lista de revocación de certificados (CRL). También se explica cómo configurar Cisco Identity Services Engine (ISE) (versiones 3.0 y posteriores) para recuperar las actualizaciones para su uso en la validación de certificados. ISE se puede configurar para recuperar CRL para los distintos certificados raíz de CA que utiliza en la validación de certificados.

Requisito previo

Requirements

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.

- Cisco Identity Services Engine versión 3.0
- Microsoft Windows Server 2008 R2

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

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

Crear y configurar una carpeta en la CA para alojar los archivos CRL

La primera tarea consiste en configurar una ubicación en el servidor de la CA para almacenar los archivos CRL. De forma predeterminada, el servidor de Microsoft CA publica los archivos en C:\Windows\system32\CertSrv\CertEnroll\

En lugar de utilizar esta carpeta del sistema, cree 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 C:\CRLDistribution crea la carpeta.



2. Para que la CA escriba los archivos CRL en la nueva carpeta, debe estar habilitado el uso compartido. Haga clic con el botón secundario en la nueva carpeta, elija Properties, haga clic

en la Sharing ficha y, a continuación, haga clic en Advanced Sharing.

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 Apply	

3. Para compartir la carpeta, active la share this folder casilla de verificación y, a continuación, agregue un símbolo de dólar (\$) al final del nombre del recurso compartido en el campo Nombre del recurso compartido para ocultar el recurso compartido.

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

4. Haga clic en Permissions (1), haga clic en Add (2), haga clic en Object Types (3) y active la Computers casilla de verificación (4).

Advanced Sharing	Permissions for CRLDistribution	on\$	Sele	ect Users, Computers, Service Accounts, or Gr	oups ?X
Share this folder Settings CRLDistribution\$ Add Remove	Share Permissions for CRLD/schlode Share Permissions Group or user names:		See U: Frc It: En	eccosers, computers, service Accounts, or or elect this object type: sers, Groups, or Built-in security principals om this location: paaa.local iter the object names to select (<u>examples</u>):	3 Object Types
Limit the number of simultaneous usi Comments: 1 Permissions Caching OK C	2 Permissions for Everyone Full Control Change Read	Add		Object Types Select the types of objects you want to find. A Object types: Image: Service Accounts Image:	2 X
	Learn about access control and pe	rmissions	8		
	OK	Cancel	Apply		OK Cancel

5. Para volver a la ventana Seleccionar usuarios, equipos, cuentas de servicio o grupos, haga clic en ox. En el campo Escriba los nombres de objeto que desea seleccionar, escriba el nombre de equipo del servidor de la CA en este ejemplo: WIN0231PNBS4IPH y haga clic en Check Names. Si el nombre introducido es válido, se actualiza y aparece subrayado. Haga clic en ox.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type: Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
abtomar.local	Locations
Enter the object names to select (examples):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

6. En el campo Nombres de grupos o usuarios, elija el equipo de la CA. Compruebe Allow el Control total para conceder acceso completo a la CA.

Haga clic en ок. Vuelva ок a hacer clic para cerrar la ventana Uso compartido avanzado y volver a la ventana Propiedades.

Permissions for CRLDistribut	tionS	×
Share Permissions		
Group or user names:		
Everyone WIN-231PNBS4IPH (ABTO	MAR\WIN-231PNE	S4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read		
ОК	Cancel	Apply

7. Para permitir que la CA escriba los archivos CRL en la nueva carpeta, configure los permisos de seguridad adecuados. Haga clic en lassecurity fichas (1), haga clic en Edit (2), haga clic en Add (3), haga clic en Object Types (4) y active la Computers casilla de verificación (5).

🖡 CRLDistribution Properties 🛛 🔀	Permissions for CRLDistribution
General Sharii 1 Security Previous Versions Customize	Security
Object name: C:\CRLDistribution	Object name: C:\CRLDistribution
Group or user names:	Group or user names:
CREATOR OWNER	CREATOR OWNER
SYSTEM SYSTEM State (BTPAAA\Administrators)	SYSTEM System State (BTP000)
& Users (RTPAAA\Users)	Series (RTPAAA\Users)
To change permissions, click Edit.	
Permissions for CREATOR	3 Add Bernive
Eull control	Permissions for CREATOR
Modify	UWNER Allow Deny
Read & execute	Modify
Read	Read & exec Object Types
Write	List tolder co Select the types of objects you want to find.
Select Users, Computers, Service Accounts, or Groups	T X
Select this object type:	
Users, droups, or Built-In security principals 4	Ubject Types
From this location:	
Enter the object names to select (examples):	Cherk Names
Advanced	Cancel

8. En el campo Escriba los nombres de objeto que desea seleccionar, escriba el nombre de equipo del servidor de la CA y haga clic en Check Names. Si el nombre introducido es válido, se actualiza y aparece subrayado. Haga clic en ok.

Select Users, Computers, Service Accounts, or Groups	×
Select this object type:	
Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	
abtomar.local	Locations
Enter the object names to select (<u>examples</u>):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

9. Elija el equipo de la CA en el campo Nombres de grupos o usuarios y, a continuación, compruebe si hay Control total Allow para conceder acceso completo a la CA. Haga clic οκ y, a continuación, haga clic close para completar la tarea.

Permissions for CRLDistribu	ution	
Security		
Object name: C:\CRLDistribut	tion	
Group or user names:		
SCREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR)	Administrators)	
Users (ABTOMAR\Users)		0.4101145
WIN-231PNBS4IPH (ABTC	DMAR\WIN-231PNE	(S4IPH\$)
	Add	Remove
Permissions for		_
WIN-231PNBS4IPH	Allow	Deny
Full control		□ ^
Modify	\checkmark	
Read & execute	\checkmark	
List folder contents	\checkmark	
Read	\sim	
Read		
Read		

Crear un sitio en IIS para exponer el nuevo punto de distribución CRL

Para que ISE tenga acceso a los archivos CRL, haga que el directorio que contiene los archivos CRL sea accesible a través de IIS.

1. En la barra de tareas del servidor IIS, haga clic en Start. Seleccione Administrative Tools > Internet Information Services (IIS) Manager. 2. En el panel izquierdo (denominado árbol de la consola), expanda el nombre del servidor IIS y, a continuación, expanda sites.



3. Haga clic con el botón derecho del ratón Default Web Site y seleccione Add Virtual Directory, como se muestra en esta imagen.

💐 Internet Information Services (IIS) Manager



4. En el campo Alias, introduzca un nombre de dirección para el punto de distribución de CRL. En este ejemplo, se ingresa CRLD.

Add Virtual Dire	ectory		?	×
Site name: Path:	Default Web Site /			
Alias: CRLD Example: ima	ges			
Physical path C:\CRLDistrib	ution			
Pass-through Connect as.	authentication Test Settings]		
		ОК	Cance	el

5. Haga clic en los puntos suspensivos (. . .) a la derecha del campo Ruta física y busque la carpeta creada en la sección 1. Seleccione la carpeta y haga clic en οκ. Haga clic οκ para cerrar la ventana Agregar directorio virtual.

Add Virtual Directory		?	\times
Site name: Default Web Site			
Path: /			
Alias:			
CRLD			
Example: images			
Physical path:			
C:\CRLDistribution			
Pass-through authentication			
Connect as Test Settings			
ОК	(Cancel	

6. El nombre del sitio introducido en el paso 4 debe estar resaltado en el panel izquierdo. Si no es así, selecciónela ahora. En el panel central, haga doble clic en Directory Browsing.

Sinternet Information Services (IIS)	Manager					
← → E → WIN-231PNBS4II	PH 🕨 Sites 🕨	Default Web	Site + CRLD	•		
File View Help						
Connections	CR	LD Home	•			
Start Page WIN-231PNBS4IPH (ABTOMA Application Pools	Filter:		• 🐨 Go - 🕻	Show All	Group by:	
 ✓ Image: Application Pools ✓ Image: Sites ✓ Image: Default Web Site > Image: Defau	ASP	Authentic	2 Compression	Default Document	Directory Browsing	Error Pages
> 🔂 CRLD	Failed Request Tra	Handler Mappings	HTTP Redirect	HTTP Respon	Logging	MIME Types
	Modules	Output	Request	SSL Settings		
	Managemen	Caching	Filtering			^

7. En el panel derecho, haga clic Enable para habilitar la exploración de directorios.



8. En el panel izquierdo, elija de nuevo el nombre del sitio. En el panel central, haga doble clic en Configuration Editor.



9. En la lista desplegable Sección, seleccione system.webServer/security/requestFiltering. En la lista allowDoubleEscaping desplegable, seleccione True. En el panel derecho, haga clic en Apply, como se muestra en esta imagen.

Internet Information Services (IIS) 1	lanager	- 🗆 X
← → ₩IN-231PNBS4IF	H > Sites > Default Web Site > CRLD >	📴 🖂 🔂 I 😧 •
File View Help		
Connections	Configuration Editor Section: system.webServer/security/requestFiltering From: Default Web Site/CRLD Web.config	Actions Apply Bx Cancel Cancel Cancel
Application Pools Sites Sites Offault Web Site	allowDoubleEscaping True International Inter	Configuration Search Configuration
> CertEnroll > CertSrv > CRLD	alwaysAllowedQueryStrings False alwaysAllowedUrls (Count=0) denvQueryStringSequences (Count=0)	Section Cock Section
	denyUrlSequences (Count=0)	'allowDoubleEscaping'

Ahora se debe poder tener acceso a la carpeta mediante IIS.

Configurar Microsoft CA Server para publicar archivos CRL en el punto de distribución

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

- 1. En la barra de tareas del servidor de la CA, haga clic en Start. Seleccione Administrative Tools > Certificate Authority.
- 2. En el panel izquierdo, haga clic con el botón secundario en el nombre de la CA. Elija Properties y haga clic en la Extensions ficha. Para agregar un nuevo punto de distribución CRL, haga clic en Add.

Enrollment Agents	Auditing	Recovery	y Agents	Secu	irîty
General	Policy Mod	Policy Module Exit			
Extensions	Storage		Certificate I	Managers	
Select extension:					
CRL Distribution Point	(CDP)				~
Specify locations from	which users can	obtain a ce	rtificate rev	ocation lis	t
(CRL).					
C:\Windows\system3	2\CertStv\CertF	nroll\cCaNa	mescCRLN	VameSuffi	2
Idap:///CN= <catrun< td=""><td>catedName><cf< td=""><td>LNameSuff</td><td>ix>,CN=<s< td=""><td>erverShort</td><td>Na</td></s<></td></cf<></td></catrun<>	catedName> <cf< td=""><td>LNameSuff</td><td>ix>,CN=<s< td=""><td>erverShort</td><td>Na</td></s<></td></cf<>	LNameSuff	ix>,CN= <s< td=""><td>erverShort</td><td>Na</td></s<>	erverShort	Na
http:// <serverdnsna< td=""><td>ame>/CertEnroll/</td><td><caname></caname></td><td>CRLName</td><td>Suffix><d< td=""><td>elti</td></d<></td></serverdnsna<>	ame>/CertEnroll/	<caname></caname>	CRLName	Suffix> <d< td=""><td>elti</td></d<>	elti
ITIE://CherverUN.hNar	me >/Len Enroll/c				
		Canaliezo	CREIVames	ounite/ <de< td=""><td>lta</td></de<>	lta
<		Cananezo	CRENames	Junix	ita >
<		Carvanie	CRENames		ita
<		Add	d	Remove	sita >
 Publish CRLs to this 	s location	Add	d	Remove	sita >
 Publish CRLs to this Include in all CRLs, when publishing matrix 	s location . Specifies where anually.	Add to publish in	d	Remove e Directory	/ta
 Publish CRLs to this Include in all CRLs, when publishing ma Include in CRLs. Cl 	s location . Specifies where anually. ients use this to f	to publish ii	d	Remove e Directory	/
 Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP 	s location . Specifies where anually. ients use this to f extension of issu	to publish ir ind Delta Cl	n the Active	Remove e Directory s.	/
 Publish CRLs to this Include in all CRLs, when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs 	s location . Specifies where anually. ients use this to f extension of issues to this location	to publish in ind Delta Clared certifical	d	Remove e Directory s.	ita >
 Publish CRLs to this Include in all CRLs, when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs 	s location . Specifies where anually. ients use this to f extension of issu to this location	Add to publish in ind Delta Cl red certificat	n the Active	Remove e Directory s.	ita >
 Publish CRLs to this Include in all CRLs. when publishing mails Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP elita 	s location . Specifies where anually. ients use this to f extension of issue to this location extension of issue	Add to publish in ind Delta Cl red certificat	n the Active	Remove e Directory s.	/
 Publish CRLs to this Include in all CRLs, when publishing mains Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP eta 	s location . Specifies where anually. ients use this to f extension of issue to this location extension of issue	Add to publish in ind Delta Cl red certificat	d	Remove e Directory s.	/

3. En el campo Ubicación, introduzca la ruta de la carpeta creada y compartida en la sección 1. En el ejemplo de la sección 1, la ruta de acceso es:

\\WIN-231PNBS4IPH\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, sele the variable below and click Insert.	ss, ct
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable: <caname> Variable</caname>	
Description of selected variable:	_
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crl1< td=""><td>Na</td></crl1<></caname></serverdnsname>	Na
<	>
OK Cancel	

4. Con el campo Ubicación rellenado, selecciónelo en la lista desplegable Variable y haga clic en Insert.

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:

\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname></caname>	
--	--

Variable:

<CaName>

✓ Insert

Description of selected variable:

Used in URLs and paths Inserts the DNS name of the server Example location: http://<ServerDNSName>/CertEnroll/<CaName><CRLNa

5. En la lista desplegable Variable, elija y haga clic en Insert.

Add Location	\times
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, set the variable below and click Insert.	ect
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	
Variable:	_
<crlnamesuffix> V Insert</crlnamesuffix>	
Description of selected variable:	
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><crlname< td=""><td>eSi</td></crlname<></caname></servername>	eSi
	*
OK Cancel	

6. En el campo Ubicación, anexe .crl al final de la ruta. En este ejemplo, Location es:

\\WIN-231PNBS4IPH\CRLDistribution\$\

.crl

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:

\\WIN-231PNBS4IPH\CRLDistribution\$\<CaName><CRLNameSuffix>.crl

Variable:

<CRLNameSuffix> V Insert

Description of selected variable:

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><CRLNameSt

7. Haga clic ox para volver a la ficha Extensiones. Marque la Publish CRLs to this location casilla de verificación y haga clic ox para cerrar la ventana Propiedades.

Aparece una solicitud de permiso para reiniciar Servicios de certificados de Active Directory. Haga clic en yes.

 \times

chroiment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule Ex	t Module	
Extensions	Storage	Certificate	Managers	
Select extension:				
CRL Distribution Point	(CDP)		~	
Specify locations from (CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna< th=""><th>2\C Certificat ame ne></th><th>ion Authority</th><th>rocation list</th><th>rtificate Censicer for the changer to</th></serverdnsna<></catrun 	2\C Certificat ame ne>	ion Authority	rocation list	rtificate Censicer for the changer to
file:// <serverdnsnar \\WIN-231PNBS4IP1 <</serverdnsnar 	<u> </u>	You must restart A take effect. Do you	ctive Directory Ce want to restart th	te service now?

8. En el panel izquierdo, haga clic con el botón derecho del ratón Revoked Certificates. Seleccione All Tasks > Publish. Asegúrese de que está seleccionada la opción Nueva CRL y, a continuación, haga clic en ok.

🙀 certsrv - [Certification Autho	rity (Local)\abtoma	r-Wil	N-231PNBS4IPH-	CA\Revoked Certificates]
File Action View Help				
🗢 🔿 🖄 🔛 🖉				
Certification Authority (Local)) Request ID	Re	vocation Date	Effective Revocation Date
Bevoked Certificat			The	e are no items to show in this vi
Ssued Certificates	All Tasks	>	Publish	
Pending Requests Failed Requests	View	>		
📔 Certificate Templa	Refresh			
	Export List			
	Properties			
	Help			

El servidor de la CA de Microsoft debe crear un nuevo archivo .crl en la carpeta creada en la sección 1. Si el nuevo archivo CRL se crea correctamente, no habrá ningún cuadro de diálogo después de hacer clic en Aceptar. Si se devuelve un error con respecto a la nueva carpeta de puntos de distribución, repita cuidadosamente cada paso de esta sección.

Compruebe que el archivo CRL existe y que se puede obtener acceso a él mediante IIS

Compruebe que los nuevos archivos CRL existen y que se puede obtener acceso a ellos a través de IIS desde otra estación de trabajo antes de iniciar esta sección.

1. En el servidor IIS, abra la carpeta creada en la sección 1. Debe haber un único archivo .crl con el formulario

.crl donde

es el nombre del servidor de la CA. En este ejemplo, el nombre de archivo es:

abtomar-WIN-231PNBS4IPH-CA.crl



2. Desde una estación de trabajo de la red (idealmente en la misma red que el nodo de administración principal de ISE), abra un navegador web y navegue hasta http://

```
donde
sea el nombre del servidor de IIS configurado en la sección 2 y
sea el nombre del sitio elegido para el punto de distribución en la sección 2. En este
ejemplo, la dirección URL es:
```

```
http://win-231pnbs4iph/CRLD
```

Aparece el índice de directorio, que incluye el archivo observado en el paso 1.



Configuración de ISE para utilizar el nuevo punto de distribución de CRL

Antes de configurar ISE para recuperar la CRL, defina el intervalo para publicar la CRL. La estrategia para determinar este intervalo está fuera del alcance de este documento. Los valores potenciales (en Microsoft CA) oscilan entre 1 hora y 41 años, ambos incluidos. El valor predeterminado es 1 semana. Una vez determinado el intervalo adecuado para su entorno, configúrelo con estas instrucciones:

- 1. En la barra de tareas del servidor de la CA, haga clic en Start. Seleccione Administrative Tools > Certificate Authority.
- 2. En el panel izquierdo, expanda la CA. Haga clic con el botón secundario en la Revoked Certificates Carpeta y seleccione Properties.
- 3. En los campos Intervalo de publicación de CRL, escriba el número necesario y elija el período de tiempo. Haga clic ox para cerrar la ventana y aplicar el cambio. En este ejemplo, se configura un intervalo de publicación de siete días.



4. Ingrese el certutil -getreg CA\Clock* comando para confirmar el valor ClockSkew. El valor predeterminado es 10 minutos.

Ejemplo de salida:

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

5. Ingrese el certutil-getreg CA\CRLov* comando para verificar si CRLOverlapPeriod se ha configurado manualmente. De forma predeterminada, el valor de CRLOverlapUnit es 0, lo

que indica que no se ha establecido ningún valor manual. Si el valor es un valor distinto de 0, registre el valor y las unidades.

Ejemplo de salida:

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

6. Ingrese el certutil -getreg CA\CRLpe* comando para verificar el CRLPeriod, que se estableció en el paso 3.

Ejemplo de salida:

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

7. Calcule el período de gracia de CRL de la siguiente manera:

a. Si CRLOverlapPeriod se estableció en el paso 5: OVERLAP = CRLOverlapPeriod, en minutos;

Else: OVERLAP = (CRLPeriod / 10), en minutos

b. Si SUPERPOSICIÓN > 720, entonces SUPERPOSICIÓN = 720

c. Si SUPERPOSICIÓN < (1,5 * ClockSkewMinutes), entonces SUPERPOSICIÓN = (1,5 * ClockSkewMinutes)

d. Si SOLAPAMIENTO > CRLPeriod, en minutos entonces SOLAPAMIENTO = CRLPeriod en minutos

e. Período de gracia = SUPERPOSICIÓN + MinutosSesgadoReloj

Example:

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 el momento en que la CA publica la siguiente CRL y el momento en que caduca la CRL actual. ISE debe configurarse para recuperar las CRL en consecuencia.

8. Inicie sesión en el nodo ISE Primary Admin y elija Administration > System > Certificates. En el panel izquierdo, elija Trusted Certificate.

■ Cisco ISE	Administration - System									
Deployment Licensing	Certificate	s Logging Ma	aintenance Upgrade	Health Checks	Backup & Restor	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifica	tes							
Trusted Certificates	Ø Edit	+ Import 🏠 Export	Delete Q View							
OCSP Client Profile		P.1						11-11-1 P	P	-
Certificate Signing Requests	0	Friendly Name	∧ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Periodic Check Se	0	Baltimore CyberTrust Root	2 Enable	d Cisco Services	02 00 00 B9	Baltimore CyberTrust	Baltimore CyberTrust	Sat, 13 May 2000	Tue, 13 May 2025	H
Certificate Authority >		CA_Root	Enable	d Endpoints AdminAuth	4D 9B EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN_	Wed, 20 Feb 2019	Sun, 20 Feb 2039	
	0	Cisco ECC Root CA 2099	Enable	d Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
	0	Cisco Licensing Root CA	🖸 Enable	d Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

- 9. Active la casilla de verificación situada junto al certificado de CA para el que desea configurar CRL. Haga clic en Edit.
- 10. Cerca de la parte inferior de la ventana, marque la Download CRL casilla de verificación.
- En el campo URL de distribución CRL, escriba la ruta de acceso al punto de distribución CRL, que incluye el archivo .crl, creado en la sección 2. En este ejemplo, la dirección URL es:

http://win-231pnbs4iph/crld/abtomar-WIN-231PNBS4IPH-CA.crl

- 12. ISE se puede configurar para recuperar la CRL a intervalos regulares o en función del vencimiento (que, en general, también es un intervalo regular). Cuando el intervalo de publicación de CRL es estático, se obtienen actualizaciones de CRL más oportunas cuando se utiliza esta última opción. Haga clic en el botón de Automatically opción.
- 13. Establezca el valor de recuperación en un valor inferior al período de gracia calculado en el paso 7. Si el valor establecido es superior al período de gracia, ISE comprueba el punto de distribución de CRL antes de que la CA haya publicado la siguiente CRL. En este ejemplo, el período de gracia se calcula en 730 minutos, o 12 horas y 10 minutos. Se utilizará un valor de 10 horas para la recuperación.
- 14. Defina el intervalo de reintento como corresponda a su entorno. Si ISE no puede recuperar la CRL en el intervalo configurado en el paso anterior, volverá a intentarlo en este intervalo más corto.
- 15. Marque la Bypass CRL Verification if CRL is not Received Casilla de verificación para permitir que la autenticación basada en certificados continúe normalmente (y sin una comprobación de CRL) si ISE no pudo recuperar la CRL para esta CA en su último intento de descarga. Si esta casilla de verificación no está activada, se producirá un error en toda la autenticación basada en certificados con certificados emitidos por esta CA si no se puede recuperar la CRL.
- 16. Marque la Ignore that CRL is not yet valid or expired casilla de verificación para permitir que ISE utilice

archivos CRL caducados (o que aún no sean válidos) como si fueran válidos. Si esta casilla de verificación no está activada, ISE considera que una CRL no es válida antes de la fecha en vigor y después de la siguiente actualización. Haga clic save para completar la configuración.

To verify certificates, enable the methods below OCSP Configuration Validate against OCSP Service Reject the request if OCSP returns U Reject the request if OCSP Respond Certificate Revocation List Configuration Certificate Revocation List Configuration Certificate Revocation List Configuration CRL Distribution URL http://wind Certificate Revocation List Configuration Certificate Revocation List Configuration Certificate Revocation List Configuration CRL Distribution URL http://wind Certificate Revocation List Configuration Certificate Revocation List Configuration Certificate Revocation URL http://wind Certificate Revocation List Configuration Certificate Revocation URL http://wind Certificate Revocation List Configuration Certificate Revocation URL http://wind Certificate Revocation List Configuration Certificate Revocation URL http://wind http://wind http://wind http://wind http://wind	Certificate Status Validatio	n						
OCSP Configuration Validate against OCSP Service Reject the request If OCSP returns U Reject the request If OCSP Respond Certificate Revocation List Configuration Ocertificate Revocation List Configuration CRL Distribution URL CRL Distribution URL CRL CRL Distribution URL CRL CRL CRL CRL CRL CRL CRL CRL CRL C		To verify certificates, enable the m	nethods below. If bo	oth are enabled, OC	SP will always be	tried first.		
Validate against OCSP Service Reject the request if OCSP returns U Reject the request if OCSP Respond Certificate Revocation List Configuration Certificate Revocation List Configuration Certificate Revocation URL CRL Distribution URL http://win Retrieve CRL Function of Reliable Server Identity Check (Revocation ICBL Retrieve CRL Retrieve Identity Check (Revocation ICBL Retrieve Identity Check (Revocation ICBL Retrieve CRL Retrieve Identity Check (Revocation ICBL Retrieve Identity Check (Revocation ICBL Retrieve CRL Retrieve CRL Retrieve CRL Retrieve Identity Check (Revocation ICBL Retrieve CRL Retrieve CRL Retrieve CRL Retrieve Identity Check (Revocation ICBL Retrieve CRL Retrieve CR		OCSP Configuration						
Reject the request if OCSP returns U Reject the request if OCSP Respond Certificate Revocation List Configuration Download CRL CRL Distribution URL http://win Retrieve CRL Kutoma Retrieve CRL		Validate against OCSP Service	ce	~				
Reject the request if OCSP Respond Certificate Revocation List Configuration CRL Distribution URL CRL Distribution URL Retrieve CRL Extreme CRL If download failed, wait CRL Distribution URL Extreme CRL CRL Distribution URL CRL Dis		Reject the request if OC	SP returns UNKNO	OWN status				
Certificate Revocation List Configuration CRL Distribution URL http://win Retrieve CRL If download failed, wait D Enable Server Identity Check (Retrieves CRL Verification if CRI		Reject the request if OC	SP Responder is u	inreachable				
		Certificate Revocation List Configur	ation					
CRL Distribution URL http://win Retrieve CRL Automa Retrieve CRL If download failed, wait 10 Enable Server Identity Check (Runass CRI Verification if CRI		Download CRL						
Retrieve CRL Automa Automa ti download failed, wait Evable Server Identity Check (Bunass CPL Verification if CPL		CRL Distribution URL	http://win-231	pnbs4iph/crld/abt	comar-WIN-231	1PNBS4IPH-CA.crl		
Retrieve CRL Every If download failed, wait D Enable Server Identity Check (Burpass CRI Verification if CRI			 Automatically 	10		Hours	~	before expiration.
If download failed, wait 10 Enable Server Identity Check (20 Bunass CPI Verification if CPI		Retrieve CRL	O Every	1		Hours	~	
Enable Server Identity Check		If download failed, wait	10		Minutes	~	before retry.	
Runass CRI Verification if CRI		Enable Server Iden	tity Check 🕕					
		Bypass CRL Verific	ation if CRL is not	Received				
Ignore that CRL is not yet valid		Ignore that CRL is	not yet valid or exp	pired				

Verificación

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

Troubleshoot

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).