Publiceer de lijsten van de intrekking van het certificaat voor ISE in een Configuratievoorbeeld van de Microsoft CA-server

Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Configureren Configuraties Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepunt te onthullen Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepunt te publiceren Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via IS Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepunt te gebruiken Verifiëren Problemen oplossen Gerelateerde informatie

Inleiding

Dit document beschrijft de configuratie van een Microsoft certificaatserver (CA) van de Autoriteit die Internet Information Services (IS) beheert om updates van de Revocatielijst van het Certificaat (CRL) te publiceren. Het legt ook uit hoe u Cisco Identity Services Engine (ISE) (versies 1.1 en later) kunt configureren om de updates voor gebruik in certificatie op te halen. ISE kan worden ingesteld om CRL's te herstellen voor de verschillende CA root certificaten die het gebruikt bij certificatie.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine release 1.1.2.15
- Microsoft Windows[®] Server[®] 2008 R2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het <u>Opname Gereedschap</u> (<u>alleen geregistreerde</u> klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

- Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten
- Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepunt te onthullen
- Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepunt te publiceren
- Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via IS
- Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepunt te gebruiken

Sectie 1. Maak en vorm een map op de CA om de CRL-bestanden te huisvesten

De eerste taak is het configureren van een locatie op de CA server om de CRL bestanden op te slaan. Standaard publiceert de Microsoft CA-server de bestanden naar C:\Windows\system32\CertSrv\CertEnroll\. Maak geen nieuwe map voor de bestanden in plaats van deze systeemmap te gebruiken.

1. Kies een locatie op het bestandssysteem op de IIS-server en maak een nieuwe map. In dit voorbeeld, de map C:\CRLDistribution is



2. Om CA te kunnen de CRL bestanden naar de nieuwe map schrijven, moet het delen zijn ingeschakeld. Klik met de rechtermuisknop op de nieuwe map, kies **Eigenschappen**, klik op het **tabblad** Delen en klik vervolgens op **Geavanceerd**

I	CRLDistribution Properties	1
	General Sharing Security Previous Versions Customize	
	Network File and Folder Sharing CRLDistribution Not Shared Network Path: Not Shared	
	Share	
	Set custom permissions, create multiple shares, and set other advanced sharing options.	
delen -	Close Cancel Apply	

3. Als u de map wilt delen, controleert u het vakje **Deze map delen** en voegt u vervolgens een dollarteken (\$) toe aan het einde van de naam van het aandeel in het veld Naam delen om

Advanced Sharing	×
Share this folder	
Settings	12
Share name:	
CRLDistribution\$	
Add Remove	
Limit the number of simultaneous users to .	
Comments:	
Permissions Caching	
OK Cancel Apply	

het aandeel te verbergen.

4. Klik op toegangsrechten (1), klik op Add (2), klik op Objecttypen (3) en controleer het vakje
 Computers

 (4)

Advanced Sharing	🔋 Permissions for CRLDistribution	\$	Sele	ct Users, Computers, Service Accounts, or Groups	? X
Share this folder	Share Permissions		Sel	lest this object type:	
Settings	Group or user names		Us	sers, Groups, or Built in security principals	3 Object Types
Share name:	& Everyone		Fio	m this location	
CRUDistribution\$			11p	esalocal	Locations
Add Remove			En	ter the object names to select (examples):	
Linit the number of similations up				-	Charle Marray
child the hamper of sinatal boos de			_	Object Types	? ×
Comments:	2_	Add	iemo I	Select the types of objects you want to find.	
	Permissions for Everyone	Allow	Jeny	A Object types:	
	Full Control			🗹 🍇 Duilt-in security principals	
1 Certina	Change			Gervice Accounts	
	neau			. Marcomputers 4	
04 1				🗹 👗 Uters	
	Learn about access control and perm	esions			
	OK	Cancel	Apply		OK. Cancel

5. Klik op OK om terug te keren naar het venster Gebruikers, computers, servicerekeningen of groepen. Typ in het veld Voer de objectnamen in om het veld te selecteren, de computernaam van de CA-server in en klik op Namen controleren. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op

Select Users, Computers, Service Accounts, or Gro	oups	? ×
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 (examples):		
RTPAAA-DC1		Check Names
	-	
Advanced	OK	Cancel
	100	1

6. Kies de CA-computer in het veld Groep of gebruikersnamen. Controleer **toestaan** dat volledige controle volledige toegang tot de CA verleent. Klik op **OK**. Klik nogmaals op **OK** om het venster Geavanceerd delen te sluiten en naar het venster Eigenschappen terug te

Permissions for CRLDistribution	on\$	
Share Permissions		
Group or user names:		
	'AAA-DC1\$J	
	[
	Add	Hemove
Permissions for RTPAAA-DC1	Allow	Deny
Full Control		
Change		
Head		
Learn about access control and pe	ermissions	
 ПК	Cancel	1 Applu
n.		

7. Om CA toe te staan om de CRL bestanden naar de nieuwe map te schrijven, moet u de

juiste beveiligingsrechten configureren. Klik op het tabblad **Beveiliging** (1), klik op **Bewerken** (2), klik op **Add** (3), klik op **Objecttypen** (4) en controleer **het vakje Computers**

<i>(</i> 0).	
CRLDistribution Properties	🗴 🎼 Permissions for CRLDistribution 🛛 🗶
General Shari 1 Security Previous Versions Customize	Security
Object name: C:\CRLDistribution	Object name: C: VCRLD is tribution
Group or user names:	Group or user names:
CREATOR OWNER	CREATOR OWNER
SYSTEM	SYSTEM
& Administrators (RTPAAA\Administrators)	Administrators (RTPIAAAVAdministrators)
Coers (HTPAAA\Users)	M Users (RTPAAA VUsers)
To change permissions, click Edit. 2 Edit	
Permissions for CREATUR DW/NER Allow Deput	3 Add Bemove
Ful control	Permissions for CREATOR
Modify	UWNER Alow Deny
Read & execute	Ful control
List folder contents	Modify 🔲 🔲
Read	Read & exec Object Types ?
Write	List folder co
Select Users, Computers, Service Accounts, or Groups	2 Select the types of objects you want to Ind.
Select this object type:	ac Object types:
Users, Groups, or Built-in security principals 4	Object Types
From this location	
rtpasallocal	Laboritors
	🖉 🖉 🐍 Users
Enter the object names to select (examples):	
	Check Names
Advanced OK	Lancel UK Lancel

8. Typ in het veld Voer de objectnamen in om het veld te selecteren, de computernaam van de CA-server in en klik op **Namen controleren**. Als de ingevoerde naam geldig is, wordt de naam vernieuwd en onderstreept. Klik op

Select Users, Computers, Service Accounts, or Gr	oups	?
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

9. Kies de CA-computer in het veld Groep of gebruikersnamen en controleer vervolgens Laat volledige controle vrij om volledige toegang tot de CA te verlenen. Klik op **OK** en vervolgens op **Sluiten** om de taak te

Permissions for CRLDistribution	×
Security	
Object name: C:\CRLDistribution	
Group or user names:	
CREATOR OWNER	
SYSTEM	
Sers (RTPAAA\Users)	
Add Remove	
Permissions for RTPAAA-DC1 Allow Deny	
Full control	
Modify 🗹 🗖	
List folder contents	
Read	
Learn about access control and permissions	

Sectie 2. Maak een site in IS om het nieuwe CRL-distributiepunt te onthullen

Maak de map waarin de CRL-bestanden zich bevinden toegankelijk via ISE zodat ISE toegang kan krijgen tot de CRL-bestanden.

- 1. Klik in de taakbalk van de lis-server op **Start**. Kies **Administratieve tools > Internet Information Services (IS) Manager**.
- 2. In het linker deelvenster (bekend als de Console Tree) vouwt u de naam van de IIS-server uit en vouwt u vervolgens **locaties**



3. Klik met de rechtermuisknop op Standaardwebsite en kies Virtuele map

Internet Inform	ation S	ervices (IIS) Manager	
GO 6	RTPA	AA-DC1 🕨 Sites 🕨 Default V	Veb Si
File View Help)		
Connections			20
🔍 - 🔚 1 📶 🕵			
RTPAAA-DC1	(RTPAA n Pools It Web 1	A\Administrator)	1
	لغ	Explore	
		Edit Permissions	
	1	Add Application	
	2	Add Virtual Directory	
		Edit Bindings	
		Manage Web Site 🔹 🕨	
	-	Refresh	
	×	Remove	
		Rename	
	GA.	Switch to Content View	

4. Voer in het veld Alias een achternaam in voor het CRL Distribution Point. In dit voorbeeld wordt CRLD

ld Virtual Di	rectory			?
Site name: Path:	Default Web Site /			
Alias:				
CRLD				
Example: ima	ges			
Physical path				
, Pass-through	authentication			
Connect as.	Test Settings			
		ОК	Cano	el

ingevoerd.

5. Klik op de ellips (. . .) rechts van het veld Fysiek pad en blader naar de map die in sectie 1 is gemaakt. Selecteer de map en klik op **OK**. Klik op **OK** om het venster Add Virtual Directory te

Site name:	Default Web Site	
Path:	1	
Alias:		
CRLD		
Example: ima	ges	
Physical path	:	
C:\CRLDistrib	oution	
Pass-through	authentication	
Connect as.	Test Settings	
Connect as.	Test Settings	

 De in stap 4 ingevoerde gebiedsnaam moet in het linker deelvenster worden gemarkeerd. Zo niet, kies dan nu. Dubbelklik in het midden op **Directory** Browsing.



7. Klik in het rechter venster op **Schakel** de directory in om het bladeren in te schakelen.

Directory Browsing	Directory bro
Use this feature to specify the information that displays in a directory listing.	Actions
🗹 Time	Ev Apply
Size	🖳 🖾 Cancel
K Extension	Enable
₩ D <u>a</u> te	🕜 Help
Long date	Online Help

 Kies in het linker deelvenster de naam van de site opnieuw. Dubbelklik in het midden op de Configuration Editor.



9. Kies in de vervolgkeuzelijst Sectie **systeem.webServer/security/requestFiltering**. Kies **True** in de vervolgkeuzelijst allowDubbelscherm. Klik in het rechtervenster op **Toepassen**.

► CRLD ►		
Section: system.webServer/security/reque	stFikering - From: Default Web Site/CRLD Web.config -	Actions
E Deenest Path: MACHINE /WERDOOT	ADDHOST	Generate Script
allowDoubleEscaping	True	Configuration
alowHighBitCharacters	True	Search Configuration
alwaysAllowedQueryStrings	False	Search Conngurat
alwaysAllowedUrls	(count=0)	Section
denyQueryStringSequences	(Count=0)	Lock Section
denyUrlSequences	(Count=0)	LOCK SECONT
fileExtensions		allowDoubleEscapi
filteringRules	(Count=0)	Attribute
hidden5egments		Lock Attribute
requestLimits		O Hab
unescapeQueryString	True	and help
🕀 verbs		Online Help

De map moet nu toegankelijk zijn via IS.

Sectie 3. Configuratie van Microsoft CA-server om CRL-bestanden naar het distributiepunt te publiceren

Nu een nieuwe map is geconfigureerd voor het huisvesten van de CRL-bestanden en de map is blootgesteld in IS, moet u Microsoft CA-server configureren om de CRL-bestanden naar de nieuwe locatie te publiceren.

- 1. Klik in de taakbalk van de CA-server op **Start**. Kies **administratieve hulpmiddelen > certificaatinstantie**.
- 2. Klik in het linker deelvenster met de rechtermuisknop op de CA-naam. Kies **Eigenschappen** en klik vervolgens op het tabblad **Uitbreidingen**. Als u een nieuw CRL-distributiepunt wilt toevoegen, klikt u op

aaa-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).
C:\Windows\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix>< Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<servershortna http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta< th=""></delta<></crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortna </crlnamesuffix></catruncatedname></crlnamesuffix></caname>
Add Remove
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.
Include in CRLs. Clients use this to find Delta CRL locations.
Include in the CDP extension of issued certificates
Publish Delta CRLs to this location
Include in the IDP extension of issued CRLs
OK Cancel Apply Help

- Toevoegen.
- 3. Voer in het veld Locatie het pad naar de map in die is gemaakt en gedeeld in sectie 1. In het voorbeeld in sectie 1 is het pad:

\\RTPAAA-DC1\CRLDistribution\$\

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\$\
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. Kies <CaName> in het veld Locatie in de vervolgkeuzelijst Variabele en klik vervolgens op

ld Location		D
A location can be any valid URI or enter a UNC or local path. To the variable below and click Ins	L or path. Enter an HTTP, LD pinsert a variable into the URI sert.	AP, file address, L or path, select
Location:		
VRTPAAA-DC1\CRLDistributio	on\$\ <caname></caname>	
Variable:		
<caname></caname>	-	Insert
Description of selected variable.	t.	
Used in URLs and paths Inserts the DNS name of the se Example location: http:// <serve< td=""><td>erver erDNSName>/CertEnroll/<ca< td=""><td>Name><crlna< td=""></crlna<></td></ca<></td></serve<>	erver erDNSName>/CertEnroll/ <ca< td=""><td>Name><crlna< td=""></crlna<></td></ca<>	Name> <crlna< td=""></crlna<>
•		Þ

Invoegen.

5. Selecteer in de vervolgkeuzelijst Variabele de optie **<CRNameSuffix>** en klik vervolgens op

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:	200
\\RTPAAA-DC1\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	
Variable:	
<crlnamesuffix> 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><crlnames< td=""><td>1</td></crlnames<></caname></servername>	1
	1
OK Cancel	1
n.	

6. Voeg in het veld Locatie .crl toe aan het einde van het pad. In dit voorbeeld is de Locatie: \\RTPAAA-DC1\CRLDistribution\$\<CaName><CRLNameSuffix>.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:	
\\RTPAAA-DC1\CRLDistribution\$\ <caname><crlnamesuffix>.crl</crlnamesuffix></caname>	
Variable:	
<crlnamesuffix> 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><crlnames< td=""><td></td></crlnames<></caname></servername>	
	1
OK Cancel	

7. Klik op OK om naar het tabblad Uitbreidingen terug te keren. Controleer de openbare CRLs op deze locatie en klik vervolgens op OK (2) om het venster Properties te sluiten. Er verschijnt een melding voor toestemming om de Active Directory certificaatservices opnieuw in te voeren. Klik op Ja

(3).	
rtpaaa-CA Properties 🛛 🔋 🗙	
Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers	
CBL Distribution Point (CDP)	
Specify locations from which users can obtain a certificate revocation list (CRL).	
C:\Windows\system32\CertSrv\CertEnroll\ <caname><crlnamesuffix><i Idap:///CN=<catruncatedname><crlnamesuffix>,CN=<servershortnar http://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><delta file://<serverdnsname>/CertEnroll/<caname><crlnamesuffix><deltac \\RTPAAA-DC1\CRLDistribution\$\<caname><crlnamesuffix>.crl</crlnamesuffix></caname></deltac </crlnamesuffix></caname></serverdnsname></delta </crlnamesuffix></caname></serverdnsname></servershortnar </crlnamesuffix></catruncatedname></i </crlnamesuffix></caname>	
Add Remove	
Include in all U Certification Authority when publishin	×
 Include in CRL Include in the I Include in the I Publish Delta (
Include in the I	
2 OK Cancel Apply Help	

8. Klik in het linker venster met de rechtermuisknop op Ingetrokken certificaten. Kies Alle taken
 > Publiceren. Zorg ervoor dat Nieuw CRL is geselecteerd en klik vervolgens op OK.



De Microsoft CA-server moet een nieuw .crl-bestand maken in de map die in sectie 1 is gemaakt. Als het nieuwe CRL-bestand met succes is gemaakt, wordt er geen dialoogvenster geopend nadat op OK is gedrukt. Als er een fout wordt teruggegeven in de map van het nieuwe distributiepunt, herhaalt u elke stap in dit gedeelte zorgvuldig.

Sectie 4. Controleer of het CRL-bestand bestaat en is toegankelijk via IS

Controleer dat de nieuwe CRL-bestanden bestaan en dat ze vanaf een ander werkstation toegankelijk zijn voordat u deze sectie start.

 Open de map die is gemaakt in sectie 1 op de lis-server. Er moet één .crl-bestand zijn dat aanwezig is bij het formulier <CANAME>.crl waar <CANAME> de naam van de CA-server is. In dit voorbeeld is filename: rtpaaa-CA.crl

📕 CRLDistribution\$				_ 🗆 ×
Network -	rtpaaa-dc1 + CRLDistribution\$	- 🖾 🛛	Search CRLDistribution\$	2
Organize 🔻 📆 Open 👻	New folder		8==	• 🔟 🔞
☆ Favorites	Name *	Date modified	Туре	Size
🧮 Desktop	🛃 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				
Music Pictures				
Videos				
🜉 Computer				
🕌 Local Disk (C:)				

2. Van een werkstation op het netwerk (idealiter op hetzelfde netwerk als het ISE-primaire Admin-knooppunt) opent u een webbrowser en bladert naar http://<SERVER>/<CRLSITE> waarin <SERVER> de servernaam is van de IIS-server die in sectie 2 is geconfigureerd en <CRLSITE> de achternaam is die voor het distributiepunt in sectie 2 is gekozen. In dit voorbeeld is de URL:

http://RTPAAA-DC1/CRLD

De directory index wordt weergegeven, met inbegrip van het bestand dat in stap 1 is waargenomen.

🗢 🔶 🤁 🛃 rtpa	a-dc1/CRLD/	
rtpaaa-dc1 - /CRLD/	+	
rtpaaa-dc1	- /CRLD/	
[To Parent Director	1	
12/18/2012 12:56 PM 12/17/2012 5:04 PM	4437 rtpaaa-CA.crl 270 web.config	

Sectie 5. Configureer de ISE om het nieuwe CRL-distributiepunt te gebruiken

Voordat ISE wordt geconfigureerd om het CRL terug te halen, moet u het interval definiëren om het CRL te publiceren. De strategie om deze tussenpozen vast te stellen valt buiten het toepassingsgebied van dit document. De potentiële waarden (in Microsoft CA) zijn 1 uur tot 411 jaar, inclusief. De standaardwaarde is 1 week. Zodra een geschikte interval voor uw omgeving is vastgesteld, dient u het interval met deze instructies in te stellen:

1. Klik in de taakbalk van de CA-server op Start. Kies administratieve hulpmiddelen >

certificaatinstantie.

- 2. Vouw in het linker deelvenster de CA uit. Klik met de rechtermuisknop op de map **Ingetrokken certificaten** en kies **Eigenschappen**.
- Voer in de velden met CRL-publicatieinterval het gewenste nummer in en kies de tijdsperiode. Klik op OK om het venster te sluiten en de wijziging toe te passen. In dit voorbeeld wordt een publicatieinterval van 7 dagen ingesteld

🌆 certsry - [Certification Autho	ority (Local)\rtpaa	a-CA\	Revoked Certificates]			
File Action View Help						
🗢 🧼 🖄 🔚 🖻 💩 📑	1					
Certification Authority (Local)	Request ID	Re	Revoked Certificates Prope	rties		?×
🗄 🧃 rtpaaa-CA	8 6	5/8	CRL Publishing Parameters	View CRLs		
Issued Certific All Ta	sks 🕨	5/8				
Pending Reque	•	5/8	A Centrificate Revocation List consider invalid.	(URL) desc	nbes certificates t	hat clients should
Failed Request	-	5/8	CBL publication interval:	7	Davis	
	t List	5/8		11	Days	
		5/8	Next update:	12/20	/2012 8:45 AM	
Prope	roes	5/8				
Help		5/8	Publish Delta CRLs			
	20	5/8	Publication interval:	1	Hours	¥
	33	5/8	Next update:			
	34	5/8				
	a	5/8				
	36	5/8				
	39	5/8				
	40	5/9				
	41	5/3				
	26 48	5/3				
	49	6/2				
	50	6/2		c	1	
Conservation states that a first		_		Cancel	Apply	
opens the properties dialog box for t	ne current selection.					

U dient nu meerdere registratiewaarden te bevestigen, die helpen de instellingen voor CRLherkenning in ISE te bepalen.

4. Voer de opdracht **certutil -getreg CA\Clock*** in om de waarde van ClockSkew te bevestigen. De standaardwaarde is 10 minuten.Uitvoer van voorbeeld:

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

5. Voer de certutil-getreg CA\CRLov* opdracht in om te controleren of de CRLOverlapPeriod handmatig is ingesteld. Standaard is de waarde voor CRLOverlapUnit 0, wat aangeeft dat er geen handmatige waarde is ingesteld. Indien de waarde een andere waarde is dan 0, registreert u de waarde en de eenheden.Uitvoer van voorbeeld:

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

6. Voer de opdracht certutil -getreg CA\CRLpe* in om de CRLPsperiode te controleren, die in stap 3 was ingesteld.Uitvoer van voorbeeld:

Values:

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

7. Bereken de CRL-Grace-periode als volgt:Indien CRLOverlapPeriod in stap 5 was ingesteld: OVERLAP = CRLOverlapPeriod, in minuten;Elders: OVERLAP = (CRLP-periode / 10), in minutenBij OVERLAP > 720 dan overLAP = 720Als overLAP < (1,5 * KloktijdSkewMinutes) is het mogelijk dat u overLAP maakt = (1,5 * ClockSkewMinutes)Indien overLAP > CRLPeriod, in minuten, dan overLAP = CRLPd in minutenGrace Periode = 720 minuten + 10 minuten = 730 minutenVoorbeeld:

```
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

De berekende aflossingsvrije periode is de tijd tussen het tijdstip waarop de CA het volgende CRL publiceert en het tijdstip waarop het huidige CRL afloopt. ISE moet worden geconfigureerd om de CRL's dienovereenkomstig te herstellen.

8. Meld u aan bij het primaire Admin-knooppunt en kies **Beheer > Systeem > Certificaten**. Selecteer in het linker venster de optie

certifi	caato	pslaan.

A Home Operations • Policy • Ad	imin istr	ation 🔻					🔫 Task Navi
🔆 System 🏾 👰 Identity Management Deployment Licensing Certificates Li	ne Ne	etwork Reso Mainter	nance A	dmin Access	al Management Settings	<u>, Lata I</u> E	
Certificate Operations		Certificat	e Store				Selected 0 Total
😨 Local Certificates		/ Edit		C Export	XDelete	Show AI	Conclusion (rotan
Certificate Signing Requests	-18	Enend	ly Name	Greek		 Issued To 	Issued By
SCEP CA Profiles	-8	C RTPA	AA-DC1-MSC	EP-RA1#rtpa	aa-CA#00002	RTPAAA-DC1-MSCEP-R	rtpaaa-CA
OCSP Services		🗆 rtpaaa	-CA#rtpaaa	-CA#00001		rtpaaa-CA	rtpaaa-CA

- 9. Controleer het aanvinkvakje in de certificaatwinkel naast het CA-certificaat waarvoor u CRL's wilt configureren. Klik op **Bewerken**.
- 10. Controleer bij de onderkant van het venster het vakje CRL downloaden.
- 11. In het veld CRL Distribution URL specificeert u het pad naar het CRL Distribution Point, dat het .crl-bestand bevat, dat in sectie 2 is gemaakt. In dit voorbeeld is de URL: http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
- 12. ISE kan worden ingesteld om het CRL met regelmatige tussenpozen terug te halen of op basis van de verloopdatum (die in het algemeen ook een regelmatig interval is). Wanneer

het CRL publicatieinterval statisch is, worden tijdigere CRL-updates verkregen wanneer de laatste optie wordt gebruikt. Klik op de knop **Automatisch** selecteren.

- 13. Stel de waarde voor herwinning in op een waarde die lager is dan de aflossingsvrije periode die in stap 7 is berekend. Als de waarde is ingesteld langer is dan de aflossingsvrije periode, controleert ISE het CRL-distributiepunt voordat de CA het volgende CRL heeft gepubliceerd. In dit voorbeeld wordt de aflossingsvrije periode berekend op 730 minuten, ofwel 12 uur en 10 minuten. Voor het ophalen wordt een waarde van 10 uur gebruikt.
- 14. Stel de interval voor het opnieuw proberen in, afhankelijk van uw omgeving. Als ISE het CRL niet kan herstellen met het ingestelde interval in de vorige stap, zal het opnieuw proberen met dit kortere interval.
- 15. Controleer de **CRL-verificatie omzeilen indien CRL niet is ontvangen**, aanvinkvakje om op certificaat gebaseerde verificatie normaal te laten doorgaan (en zonder een CRL-controle) indien ISE in zijn laatste downloadpoging de CRL voor deze CA niet heeft kunnen ophalen. Als dit aankruisvakje niet is ingeschakeld, zal alle op certificaten gebaseerde echtheidscontrole met door deze CA afgegeven certificaten mislukken als het CRL niet kan worden opgehaald.
- 16. Controleer het **negeren dat CRL nog niet geldig is of verlopen** aanvinkvakje om ISE toe te staan verlopen (of nog niet geldige) CRL bestanden te gebruiken alsof ze geldig zijn. Als dit aanvinkvakje niet is ingeschakeld, beschouwt ISE een CRL als ongeldig vóór hun effectieve datum en na hun volgende update. Klik op **Opslaan** om de configuratie te voltooien.

Issued By	rtpaaa-CA					
Valid From	Sat, 11 Feb 2012 1	9:32:02 EST				
Valid To (Expiration)	Wed, 11 Feb 2037	19:42:01 EST				
Serial Number	1D 85 1D 58 36 8C	EC 93 4E F6 5B 2	8 9B 26 E7 89			
Usage						
All Trust Certificates are av and administrative authent	vailable for selection tication below:	as the Root CA fo	or secure LDAP con	nections. In additic	on, they may be ena	bled for EAP-TL
Trust for client authen	tication					
Enable Validation of	Certificate Extensio	ons (accept only va	alid certificate)			
OCSP Configuration Validate against OCSP Reject the reque	Service	us could not be de	*			
OCSP Configuration Validate against OCSP Reject the reque Certificate Revocation	Service st if certificate stati List Configuration	us could not be de n	etermined by OCSP			
OCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Ownload CRL	Service st if certificate stati List Configuration	us could not be de n	stermined by OCSP	5		_
OCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Ocentificate Revocation CRL Distribution I	Service st if certificate state List Configuration JRL http://rtpa	us could not be de n aa-dc1/CRLD/rtpaa	etermined by OCSP			
OCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Ownload CRL CRL Distribution I	Service st if certificate state List Configuration JRL http://rtpa ©	us could not be de n aa-dc1/CRLD/rtpaa	etermined by OCSP	Hours	_	before expirate
OCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Ocru Download CRL CRL Distribution I Retrieve CRL	Service est if certificate stati List Configuration URL http://rtpai O	us could not be de n aa-dc1/CRLD/rtpaa aly	etermined by OCSP	Hours	¥	before expirati
DCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Overview CRL CRL Distribution I Retrieve CRL	Service est if certificate state List Configuration URL http://rtpa O Automatica O Every	us could not be de n aa-dc1/CRLD/rtpaa ally 10 0	etermined by OCSP	Hours Weeks	¥	before expirati
DCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Overlificate Revocation CRL Distribution I Retrieve CRL If download failed	Service est if certificate stati List Configuration URL http://rtpai O Automatica Every d, wait 1	us could not be de n aa-dc1/CRLD/rtpaa ally 10	etermined by OCSP	Hours	before retry.	before expirati
DCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Ownload CRL CRL Distribution I Retrieve CRL If download failed Revocation	Service est if certificate state List Configuration URL http://rtpai O Automatica O Every d, wait 1	us could not be de n aa-dc1/CRLD/rtpaa ally 10 0	etermined by OCSP	Hours Weeks	before retry.	before expirat
DCSP Configuration Validate against OCSP Reject the reque Certificate Revocation Over Download CRL CRL Distribution I Retrieve CRL If download failed Bypass CRL V Ignore that C	Service est if certificate state List Configuration URL http://rtpa O Automatica O Every d, wait 1 'erification if CRL is n CRL is not yet valid of	us could not be de n aa-dc1/CRLD/rtpaa ally 10 0 not Received or expired	etermined by OCSP	Hours Weeks	before retry.	before expirat

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

• Technische ondersteuning en documentatie – Cisco Systems