Configurer Microsoft CA Server pour publier les listes de révocation de certificats pour ISE

Contenu

Introduction Prérequis Conditions requises Components Used Configuration Créer et configurer un dossier sur l'autorité de certification pour héberger les fichiers CRL Créer un site dans IIS pour exposer le nouveau point de distribution CRL Configurer Microsoft CA Server pour publier les fichiers CRL sur le point de distribution Vérifier que le fichier CRL existe et est accessible via IIS Configurer ISE pour utiliser le nouveau point de distribution CRL

Introduction

Ce document décrit la configuration d'un serveur d'autorité de certification Microsoft qui exécute les services IIS (Internet Information Services) pour publier les mises à jour de la liste de révocation de certificats (CRL). Il explique également comment configurer Cisco Identity Services Engine (ISE) (versions 3.0 et ultérieures) pour récupérer les mises à jour à utiliser dans la validation de certificat. ISE peut être configuré pour récupérer des LCR pour les différents certificats racine de l'autorité de certification qu'il utilise dans la validation des certificats.

Prérequis

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Identity Services Engine version 3.0
- Microsoft Windows[®] Server[®] 2008 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Créer et configurer un dossier sur l'autorité de certification pour héberger les fichiers CRL

La première tâche consiste à configurer un emplacement sur le serveur AC pour stocker les fichiers CRL. Par défaut, le serveur Microsoft CA publie les fichiers sur C:\Windows\system32\CertSrv\CertEnroll\

Plutôt que d'utiliser ce dossier système, créez un nouveau dossier pour les fichiers.

1. Sur le serveur IIS, choisissez un emplacement sur le système de fichiers et créez un nouveau dossier. Dans cet exemple, le dossier C:\CRLDistribution est créé.



2. Pour que l'autorité de certification puisse écrire les fichiers CRL dans le nouveau dossier, le partage doit être activé. Cliquez avec le bouton droit sur le nouveau dossier, choisissez **Propriétés**, cliquez sur l'onglet **Partage**, puis cliquez sur **Partage** avancé.

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	
Not Shared	
Network Path: Not Shared	
Share	
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	10. A
Advanced Sharing	10
Close Cancel Apply	

3. Pour partager le dossier, cochez la case **Partager ce dossier**, puis ajoutez un signe dollar (\$) à la fin du nom du partage dans le champ Nom du partage pour masquer le partage.

va	nced Sharing
~	Share this folder
Se	ettings
	Share name:
	CRLDistribution\$
1	Add Remove
	Comments:
	Permissions Caching

4. Cliquez sur **Autorisations** (1), sur **Ajouter** (2), sur **Types d'objets** (3) et activez la case à cocher **Ordinateurs** (4).

Advanced Sharing	🔋 Permissions for CRLDistributio	in\$	Select Us	ers, Computers, Service Accounts, or Grou	ps ?X
I✓ Share this folder	Share Permissions		Select thi	is object type:	
Settings	Group or user names:		- JUsers, G From this	roups, or Built-in security principals	J Ubject Types
CRLDistribution\$			rtpaaa.lo	ical	Locations
Add Remove			Enter the	object names to select (<u>examples</u>):	
Limit the number of simultaneous us			Ob	ject Types	? 🗙
Comments:	2	Add Re		elect the types of objects you want to find.	
	Permissions for Everyone Full Control	Allow De		Diject types:	
1 Permissions Caching	Change			Service Accounts	
				Image: Comparison of the compar	
С					
	Learn about access control and pe	missions			
	OK	Cancel	Apply		OK Cancel
		Lancel	Apply		

5. Pour revenir à la fenêtre Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes, cliquez sur **OK**. Dans le champ Entrez les noms d'objet à sélectionner, entrez le nom d'ordinateur du serveur AC dans cet exemple : WIN0231PNBS4IPH et cliquez sur **Vérifier les noms**. Si le nom saisi est valide, il est actualisé et apparaît souligné. Click 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 (examples):	
WIN-231PNBS4IPH	Check Names
Advanced OK	Cancel

6. Dans le champ Group or user names, sélectionnez l'ordinateur AC. Cochez **Allow** for Full Control pour accorder un accès complet à l'AC.

Click OK. Cliquez de nouveau sur **OK** pour fermer la fenêtre Partage avancé et revenir à la fenêtre Propriétés.

Permissions for CRLDistribution	onS	×
Share Permissions		
Group or user names: Everyone WIN-231PNBS4IPH (ABTOM)	AR\WIN-231PNE	8S4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control Change Read	\Box \Box	
ОК		

7. Afin de permettre à l'autorité de certification d'écrire les fichiers CRL dans le nouveau dossier, configurez les autorisations de sécurité appropriées. Cliquez sur l'onglet Sécurité (1), cliquez sur **Modifier** (2), sur **Ajouter** (3), sur **Types d'objets** (4) et activez la case à cocher **Ordinateurs** (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 Sectors (BTPAAA\Administrators)	SYSTEM SAdministrators (BTPAAA\Administrators)
Sers (RTPAAA\Users)	Users (RTPAAA\Users)
To change permissions, click Edit.	
Permissions for CREATOR Allow Deny	3 Add Remove
Full control	Permissions for CREATOR Allow Denv
Modify	Full control
Head & execute	Modify 🗖 🗖
Read	Read & exec List folder on Object Types
Write 🔽	Select the types of objects you want to find.
Select Users, Computers, Service Accounts, or Groups	
Select this object type:	
Users, Groups, or Built-in security principals 4	. Object Types
From this location:	📃 🔤 🔛 Computers 5
rtpaaa.local	Locations
Enter the object names to select (<u>examples</u>):	Users
	Check Names
Advanced	Cancel OK Cancel

8. Dans le champ Entrez les noms d'objet à sélectionner, entrez le nom d'ordinateur du serveur AC, puis cliquez sur **Vérifier les noms**. Si le nom saisi est valide, il est actualisé et apparaît souligné. Click 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. Choisissez l'ordinateur de l'Autorité de certification dans le champ Groupe ou noms d'utilisateurs, puis cochez la case **Autoriser** le contrôle complet pour accorder un accès complet à l'Autorité de certification. Cliquez sur **OK** puis sur **Fermer** pour terminer la tâche.

Permissions for CRLDistributi	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
CREATOR OWNER		
Administrators (ABTOMAR\A	dministrators)	
Sers (ABTOMAR\Users)	,	
WIN-231PNBS4IPH (ABTOM	IAR\WIN-231PNB	S4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full control		^
Modify	\checkmark	
Read & execute		
List folder contents	\leq	
Read		
OK	Canaal	Acaly
UK	Cancer	нрру

Créer un site dans IIS pour exposer le nouveau point de distribution CRL

Pour que ISE puisse accéder aux fichiers CRL, rendez le répertoire qui héberge les fichiers CRL accessible via IIS.

- 1. Dans la barre des tâches du serveur IIS, cliquez sur **Démarrer**. Choisissez **Outils** d'administration > Gestionnaire des services Internet (IIS).
- 2. Dans le volet gauche (appelé arborescence de la console), développez le nom du serveur IIS, puis développez **Sites.**



3. Cliquez avec le bouton droit sur **Site Web par défaut** et choisissez **Ajouter un répertoire virtuel**, comme illustré dans cette image.

💐 Internet Information Services (IIS) Manager



4. Dans le champ Alias, saisissez un nom de site pour le point de distribution CRL. Dans cet exemple, CRLD est saisi.

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

5. Cliquez sur l'ellipse (. . .) à droite du champ Physical path et accédez au dossier créé dans la section 1. Sélectionnez le dossier et cliquez sur **OK**. Cliquez sur **OK** pour fermer la fenêtre Ajouter un répertoire virtuel.

Add Virtual Directory			?	×
Site name: Default Web Path: /	Site			
Alias:				
CRLD				
Example: images				
Physical path:				
C:\CRLDistribution]	
Pass-through authenticatio	n			
Connect as Test S	ettings]		
		ОК	Cancel	

6. Le nom de site saisi à l'étape 4 doit être mis en surbrillance dans le volet gauche. Sinon, choisissez-le maintenant. Dans le volet central, double-cliquez sur **Navigation dans les répertoires**.



7. Dans le volet droit, cliquez sur Activer pour activer la navigation dans les répertoires.

Internet Information Services (IIS)	Manager	– 🗆 ×
← → 21 + WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +	🖬 🖂 🏠 🔞 •
File View Help		
Connections Connections Start Page WIN-231PNBS4IPH (ABTOMA Application Pools CertEnroll CertEnroll CertEnv CertEnv CERLD	Directory Browsing Use this feature to specify the information that displays in a directory listing. Time Size Extension Date Long date	Alerts Directory browsing has been disabled. Actions Actions Cancel Enable Help

8. Dans le volet gauche, sélectionnez à nouveau le nom du site. Dans le volet central, doublecliquez sur **Éditeur de configuration**.



9. Dans la liste déroulante Section, sélectionnez **system.webServer/security/requestFiltering**. Dans la liste déroulante **allowDoubleEscaping**, sélectionnez **True**. Dans le volet droit, cliquez sur **Appliquer**, comme illustré dans cette image.



Le dossier doit maintenant être accessible via IIS.

Configurer Microsoft CA Server pour publier les fichiers CRL sur le point de distribution

Maintenant qu'un nouveau dossier a été configuré pour héberger les fichiers CRL et que le dossier a été exposé dans IIS, configurez le serveur AC Microsoft pour publier les fichiers CRL dans le nouvel emplacement.

- 1. Dans la barre des tâches du serveur AC, cliquez sur **Démarrer**. Choisissez **Outils** d'administration > Autorité de certification.
- 2. Dans le volet gauche, cliquez avec le bouton droit sur le nom de l'autorité de certification. Choisissez **Propriétés**, puis cliquez sur l'onglet **Extensions**. Pour ajouter un nouveau point de distribution CRL, cliquez sur **Ajouter**.

	SHIPH-CA PIO	perties		?	\sim
Enrollment Agents	Auditing	Recover	y Agents	Sec	urity
General	Policy Mo	odule	Ex	it Module	
Extensions	Storage		Certificate	Managers	3
Select extension:					
Select extension.	(000)				
CRL Distribution Point	(CDP)				~
C:\Windows\system3 Idap:///CN= <catrund http://<serverdnsna file://<serverdnsna< th=""><th>2\CertSrv\Cert catedName><c me>/CertEnroll ne>/CertEnroll/</c </th><th>Enroll\<cana RLNameSuf /<caname> /<caname><</caname></caname></cana </th><th>ame><crl fix>,CN=<s <crlname CRLName</crlname </s </crl </th><th>NameSuff erverSho Suffix><[Suffix><d< th=""><th>tNar Delta eltaC</th></d<></th></serverdnsna<></serverdnsna </catrund 	2\CertSrv\Cert catedName> <c me>/CertEnroll ne>/CertEnroll/</c 	Enroll\ <cana RLNameSuf /<caname> /<caname><</caname></caname></cana 	ame> <crl fix>,CN=<s <crlname CRLName</crlname </s </crl 	NameSuff erverSho Suffix><[Suffix> <d< th=""><th>tNar Delta eltaC</th></d<>	tNar Delta eltaC
<					>
<		Ad	d	Remov	> e
Publish CRLs to this	s location	Ad	d	Remov	> e
 Publish CRLs to this Include in all CRLs. when publishing ma 	s location Specifies when mually.	Ad re to publish i	d in the Activ	Remov e Director	» е
 Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli 	s location Specifies when anually.	Ad re to publish i find Delta C	d in the Activ	Remov e Director	> e
 Publish CRLs to this Include in all CRLs. when publishing main and the comparison of the compa	s location Specifies when anually. ients use this to extension of iss	Ad re to publish i find Delta C sued certifica	d in the Active RL location ites	Remov e Director ns.	> e
 Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli Include in the CDP Publish Delta CRLs 	s location Specifies when anually. ients use this to extension of iss to this location	Ad re to publish i find Delta C sued certifica	d in the Active RL location ites	Remov e Director ns.	> e
Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cli Include in the CDP Publish Delta CRLs Include in the IDP #	s location Specifies when anually. ients use this to extension of iss to this location	Ad re to publish i find Delta C sued certifica	d in the Active RL location ites	Remov e Director ns.	> y
 Publish CRLs to this Include in all CRLs. when publishing mails in the CDP Include in the CDP Publish Delta CRLs Include in the IDP etails 	s location Specifies when anually. ients use this to extension of iss to this location extension of issu	Ad re to publish i find Delta C sued certifica	d in the Active RL location ites	Remove e Director	> y
 Publish CRLs to this Include in all CRLs. when publishing main of the comparison of the compar	s location Specifies when anually. ients use this to extension of iss to this location extension of issu	Ad te to publish i find Delta C sued certifica	d in the Active RL location ites	Remove e Director	> e

3. Dans le champ Emplacement, saisissez le chemin d'accès au dossier créé et partagé dans la section 1. Dans l'exemple de la section 1, le chemin est :

\\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, select the variable below and click Insert.	
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable:	
<caname> Validable:</caname>	1
Description of selected variable:	_
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""><td>1</td></crlna<></caname></serverdnsname>	1
< >	
OK Cancel]

4. Lorsque le champ Emplacement est renseigné, sélectionnez **<CaName>** dans la liste déroulante Variable, puis cliquez sur **Insérer.**

Add Location		×
A location can be any valid URL or path. E or enter a UNC or local path. To insert a va the variable below and click Insert.	inter an HTTP, LD ariable into the UR)AP, file address, L or path, select
Location:		
\\WIN-231PNBS4IPH\CRLDistribution\$\	<caname></caname>	
Variable: <caname> Description of selected variable:</caname>	~	Insert
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsnam< td=""><td>e>/CertEnroll/<ca< td=""><td>aName><crlna< td=""></crlna<></td></ca<></td></serverdnsnam<>	e>/CertEnroll/ <ca< td=""><td>aName><crlna< td=""></crlna<></td></ca<>	aName> <crlna< td=""></crlna<>
•		2
	ОК	Cancel

5. Dans la liste déroulante Variable, sélectionnez **<CRLNameSuffix>**, puis cliquez sur **Insérer**.

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.	: i
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	7
Variable: <crlnamesuffix> Variable:</crlnamesuffix>] i
Used in URLs and paths for the CRL Distribution Points extension	1
Appends a suffix to distinguish the CRL file name	
Example location: http:// <servername>/CertEnroll/<caname><crlnames< td=""><td>t r</td></crlnames<></caname></servername>	t r
< >	
	_
OK Cancel]

6. Dans le champ Emplacement, ajoutez **.crl** à la fin du chemin. Dans cet exemple, l'emplacement est le suivant :

\\WIN-231PNBS4IPH\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, selec the variable below and click Insert.	s. ti
Location: \\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix>.crl</crlnamesuffix></caname>	
Variable: <crlnamesuffix> VInsert Description of selected variable:</crlnamesuffix>	
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>Si ,</td></crlnames<></caname></servername>	Si ,
OK Cancel	

7. Cliquez sur **OK** pour revenir à l'onglet Extensions. Cochez la case **Publier les LCR à cet emplacement**, puis cliquez sur **OK** pour fermer la fenêtre Propriétés.

Une invite s'affiche pour demander l'autorisation de redémarrer les services de certificats Active Directory. **Cliquez sur Yes.**

Enroliment 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).	which users can	obtain a certificate rev	ocation list	
Idap:///CN= <catrun< th=""><th>cate</th><th></th><th></th><th></th></catrun<>	cate			
nttp:// <serverdnsna file://<serverdnsna WWIN-231PNBS4IP</serverdnsna </serverdnsna 		You must restart Ad take effect. Do you	tive Directory Co want to restart ti	ertificate Services for the changes to he service now?
rittp:// <serverunsna file://<serverdnsna WWIN-231PNBS4IP</serverdnsna </serverunsna 		You must restart Ao take effect. Do you	tive Directory Co want to restart t	ertificate Services for the changes to he service now? Yes No

8. Dans le volet gauche, cliquez avec le bouton droit sur **Certificats révoqués**. Choisissez **Toutes les tâches > Publier**. Assurez-vous que la nouvelle liste de révocation de certificats est sélectionnée, puis cliquez sur **OK**.





Le serveur AC Microsoft doit créer un nouveau fichier .crl dans le dossier créé dans la section 1. Si le nouveau fichier CRL est créé avec succès, aucune boîte de dialogue ne s'affiche après avoir cliqué sur OK. Si une erreur est renvoyée en ce qui concerne le nouveau dossier du point de distribution, répétez soigneusement chaque étape de cette section.

Vérifier que le fichier CRL existe et est accessible via IIS

Vérifiez que les nouveaux fichiers CRL existent et qu'ils sont accessibles via IIS à partir d'une autre station de travail avant de démarrer cette section.

 Sur le serveur IIS, ouvrez le dossier créé dans la section 1. Un fichier .crl unique doit être présent avec le formulaire <CANAME>.crl où <CANAME> est le nom du serveur AC. Dans cet exemple, le nom de fichier est :

abtomar-WIN-231PNBS4IPH-CA.crl

📙 🛃 📕 🖛 CRL	Distrib	ution			-		×
File Home	Share	View					~ 🕐
← → • ↑ 📙	> Thi	s PC > Local Disk (C:) > CRLDistribution	~	ල් Search CF	RLDistribution		P
 Quick access Desktop Downloads Documents Pictures System32 	* * * *	Name abtomar-WIN-231PNBS4IPH-CA web.config	Date modified 11/28/2020 10:39 11/28/2020 10:22	Type Certificate Re CONFIG File	Size	1 KB 1 KB	

2. À partir d'une station de travail sur le réseau (idéalement sur le même réseau que le noeud principal d'administration ISE), ouvrez un navigateur Web et accédez à http://<SERVER>/<CRLSITE> où <SERVER> est le nom du serveur IIS configuré dans la section 2 et <CRLSITE> le nom du site choisi pour le point de distribution dans la section 2. Dans cet exemple, l'URL est :

L'index du répertoire s'affiche, qui inclut le fichier observé à l'étape 1.



Configurer ISE pour utiliser le nouveau point de distribution CRL

Avant que ISE ne soit configuré pour récupérer la liste de révocation de certificats, définissez l'intervalle de publication de la liste de révocation de certificats. La stratégie de détermination de cet intervalle dépasse le cadre de ce document. Les valeurs potentielles (dans Microsoft CA) sont comprises entre 1 heure et 411 ans, inclusivement. La valeur par défaut est 1 semaine. Une fois qu'un intervalle approprié pour votre environnement a été déterminé, définissez l'intervalle avec les instructions suivantes :

- 1. Dans la barre des tâches du serveur AC, cliquez sur **Démarrer**. Choisissez **Outils** d'administration > Autorité de certification.
- 2. Dans le volet gauche, développez l'autorité de certification. Cliquez avec le bouton droit sur le dossier **Certificats révoqués** et sélectionnez **Propriétés.**
- 3. Dans les champs intervalle de publication CRL, saisissez le numéro requis et choisissez la période. Cliquez sur **OK** pour fermer la fenêtre et appliquer la modification. Dans cet exemple, un intervalle de publication de 7 jours est configuré.

 Certification Authority abtomar-WIN-231 	y (Local) PNBS4IPH-I	Request ID	Revocation D
Revoked Cert	All Tasks	>	
Pending Re	View	>	
Certificate	Refresh		
	Export Lis	t	
	Properties	;	
	Help		
Revoked Certificates Propertie	5	?	×
Revoked Certificates Propertie CRL Publishing Parameters Vi A Certificate Revocation List (Consider invalid.	ew CRLs CRL) describes ce	? rtificates that clien	ts should
Revoked Certificates Propertie CRL Publishing Parameters We A Certificate Revocation List (C consider invalid. CRL publication interval:	ew CRLs cRL) describes ce 7 Day	rtificates that clien s ~	ts should
Revoked Certificates Propertie CRL Publishing Parameters W A Certificate Revocation List (Consider invalid. CRL publication interval: Next update: Publish Detta CRLs Publication interval: Next update:	sw CRLs cw CRLs CRL) describes ce 7 Day 12/5/2020 10	rtificates that client s v :39 AM	ts should

4. Entrez la commande **certutil -getreg CA\Clock*** pour confirmer la valeur ClockSkew. La valeur par défaut est 10 minutes.

Exemple de rapport :

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

5. Entrez la commande **certutil -getreg CA\CRLov*** pour vérifier si CRLOverlapPeriod a été défini manuellement. Par défaut, la valeur CRLOverlapUnit est 0, ce qui indique qu'aucune valeur manuelle n'a été définie. Si la valeur est différente de 0, enregistrez la valeur et les unités.

Exemple de rapport :

```
Values:
    CRLOverlapPeriod REG_SZ = Hours
    CRLOverlapUnits REG_DWORD = 0
CertUtil: -getreg command completed successfully.
6. Entrez la commande certutil -getreg CA\CRLpe* pour vérifier la période CRLP, définie à l'étape
```

3.

Exemple de rapport :

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

7. Calculez la période de grâce de la LCR comme suit :

a. Si CRLOverlapPeriod a été défini à l'étape 5 : OVERLAP = CRLOverlapPeriod, en minutes ;

Autre : OVERLAP = (période CRLP/10), en minutes

b. Si SURLAP > 720, alors SURLAP = 720

c. Si SURLAP < (1,5 * ClockSkewMinutes), alors SURLAP = (1,5 * ClockSkewMinutes)

d. Si OVERLAP > CRLPeriod, en minutes, OVERLAP = CRLPperiode en minutes

e. Période de grâce = SUPERLAP + minutes de décalage d'horloge

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 d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes e. Grace Period = 720 minutes + 10 minutes = 730 minutes Le délai de grâce calculé est le délai entre le moment où l'autorité de certification publie la prochaine liste de révocation de certificats et l'expiration de la liste de révocation de certificats actuelle. ISE doit être configuré pour récupérer les LCR en conséquence.

8. Connectez-vous au noeud d'administration principal ISE et choisissez Administration > System > Certificates. Dans le volet gauche, sélectionnez Certificat approuvé

E Cisco ISE					Admini	stration · System					
Deployment Licensing	Certificates	Logging M	aintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifica	ites								
Trusted Certificates	Ø Edit	+ Import 🗈 Export	Delete	Q View							
OCSP Client Profile		Friendly Name		∧ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Signing Requests	-	,									
Certificate Periodic Check Se		Baltimore CyberTrust Root		Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust	Baltimore CyberTrust	Sat, 13 May 2000	Tue, 13 May 2025	2
Certificate Authority >		CA_Root		Enabled	Infrastructure 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		Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
		Cisco Licensing Root CA		Enabled	Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

9. Cochez la case en regard du certificat CA pour lequel vous avez l'intention de configurer des LCR. Cliquez sur **Edit**.

10. En bas de la fenêtre, cochez la case Télécharger la liste de révocation de certificats.

11. Dans le champ URL de distribution CRL, saisissez le chemin d'accès au point de distribution CRL, qui inclut le fichier .crl, créé à la section 2. Dans cet exemple, l'URL est :

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

12. ISE peut être configuré pour récupérer la liste de révocation de certificats à intervalles réguliers ou en fonction de l'expiration (qui, en général, est également un intervalle régulier). Lorsque l'intervalle de publication CRL est statique, des mises à jour CRL plus opportunes sont obtenues lorsque cette dernière option est utilisée. Cliquez sur la case d'option **Automatically**.

13. Définissez la valeur de récupération sur une valeur inférieure à la période de grâce calculée à l'étape 7. Si le jeu de valeurs est plus long que la période de grâce, ISE vérifie le point de distribution de la liste de révocation de certificats avant que l'autorité de certification ait publié la liste de révocation de certificats suivante. Dans cet exemple, la période de grâce est calculée sur 730 minutes, soit 12 heures et 10 minutes. Une valeur de 10 heures sera utilisée pour la récupération

14. Définissez l'intervalle des nouvelles tentatives en fonction de votre environnement. Si ISE ne parvient pas à récupérer la liste de révocation de certificats à l'intervalle configuré à l'étape précédente, il réessaiera à cet intervalle plus court.

15. Cochez la case **Ignorer la vérification CRL si la liste de révocation de certificats n'est pas reçue** pour autoriser l'authentification basée sur le certificat à continuer normalement (et sans vérification CRL) si ISE n'a pas pu récupérer la liste de révocation de certificats pour cette autorité de certification lors de sa dernière tentative de téléchargement. Si cette case n'est pas cochée, toute authentification basée sur un certificat avec des certificats émis par cette autorité de certification échouera si la liste de révocation de certificats ne peut pas être récupérée.

16. Cochez la case **Ignorer que la liste de révocation de certificats n'est pas encore valide ou a expiré** pour permettre à ISE d'utiliser des fichiers de liste de révocation de certificats expirés (ou non encore valides) comme s'ils étaient valides. Si cette case n'est pas cochée, ISE considère qu'une liste de révocation de certificats n'est pas valide avant sa date d'entrée en vigueur et après sa prochaine mise à jour. Cliquez sur **Enregistrer** pour terminer la configuration.

Certificate	Status	Validation
-------------	--------	------------

validate against 000P Service	ce .	~					
Reject the request if OC	SP returns UNKNO	WN status					
Reject the request if OC	SP Responder is u	nreachable					
Certificate Revocation List Configur	ation						
Download CRL							
CRL Distribution URL	http://win-221						
	11((p./)wiii-231	pnbs4iph/crld/abtor	mar-WIN-231	IPNBS4IPH-C/	A.Crl		
0.11-0.00	Automatically	nbs4iph/crid/abto	mar-WIN-231	Hours	v.cri	before expiration.	
Retrieve CRL	Automatically Every	10 1	mar-WIN-231	Hours Hours		before expiration.	
Retrieve CRL If download failed, wait	Automatically Every	nbs4iph/crid/abtor	Minutes	Hours Hours	before retry.	before expiration.	
Retrieve CRL If download failed, wait	Automatically Every 10	10 1	Minutes	Hours Hours Hours	↓ cri	before expiration.	

Save

Informations internes Cisco

1. Microsoft. « Configurer un point de distribution CRL pour les certificats. » <u>http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx</u>, 7 octobre 2009 [18 décembre 2012]

2. Microsoft. « Publier manuellement la liste de révocation de certificats. » <u>http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx</u>, 21 janvier 2005 [18 décembre 2012]

3. Microsoft. « Configurez les périodes de chevauchement CRL et Delta CRL. » <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>, 11 avril 2011 [18 décembre 2012]

4. MS2065 [MSFT]. « Comment EffectiveDate (cette mise à jour), NextUpdate et NextCRLPublish sont calculés. » <u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>, 4 juin 2008 [18 décembre 2012]