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

Table des matières

Introduction
Prérequis
Exigences
Composants utilisés
Configurer
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 des fichiers CRL sur le point de distribution
Vérifiez que le fichier CRL existe et qu'il est accessible via IIS
Configurer ISE pour utiliser le nouveau point de distribution CRL
Vérifier
<u>Dépannage</u>

Introduction

Ce document décrit la configuration d'un serveur d'autorité de certification Microsoft qui exécute les services Internet (IIS) 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 des certificats. ISE peut être configuré pour récupérer les listes de révocation de certificats pour les divers certificats racines CA qu'il utilise dans la validation de certificat.

Prérequis

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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.

Configurer

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 AC Microsoft 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 Properties , cliquez sur l'SharingOnglet, puis cliquez sur Advanced Sharing.

CRLDistribution Properties	X
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	10 10 10

3. Afin de partager le dossier, cochez la case, Share this folder puis ajoutez un symbole dollar (\$) à la fin du nom du partage dans le champ Nom du partage pour masquer le partage.

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

4. Cliquez sur Permissions (1), cliquez sur Add (2), cliquez sur Object Types (3), puis cochez la case Computers (4).

Advanced Sharing	🔋 Permissions for CRLDistributio	in\$	Se	elect Users, Computers, Service Accounts, or Gro	ups ?X
Share this folder Settings Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous us-	aring Permissions for CRUDistribution\$ is folder ame: tribution\$ Remove rnumber of simultaneous usi		9 	Select this object type: Users, Groups, or Built-in security principals From this location: Itpaaa.local Enter the object names to select (<u>examples</u>)	3 Object Types Locations
Comments: 1 Permissions Caching OK C	Permissions for Everyone Full Control Change Read	Add	Remo	Select the types of objects you want to find. A Object types: Built-in security principals Service Accounts Computers Computers USGroups USers USers	
	Learn about access control and per	missions			
	ОК	Cancel	Apply		OK Cancel

5. Pour revenir à la fenêtre Sélectionner des utilisateurs, des ordinateurs, des comptes de service ou des groupes, cliquez sur ок. Dans le champ Entrez les noms d'objets à sélectionner, entrez le nom d'ordinateur du serveur AC dans cet exemple : WIN0231PNBS4IPH et cliquez sur Check Names. Si le nom saisi est valide, il est actualisé et est souligné. Cliquez sur ок.

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

6. Dans le champ Nom du groupe ou de l'utilisateur, sélectionnez l'ordinateur AC. Cochez Allow Contrôle total pour accorder un accès complet à l'autorité de certification.

Cliquez sur ok. Cliquez ok à nouveau pour fermer la fenêtre Partage avancé et revenir à la fenêtre Propriétés.

Permissions for CRLDistribu	Permissions for CRLDistribution\$					
Share Permissions						
Group or user names:						
Everyone WIN-231PNBS4IPH (ABTO)MAR\WIN-231PNB	S4IPH\$)				
	Add	Remove				
Permissions for WIN-231PNBS4IPH	Allow	Deny				
Full Control						
Change						
Change Read	\leq					
Change Read						
Change Read						
Change Read						

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 sursecurity l'onglet (1), cliquez sur Edit (2), cliquez sur Add (3), cliquez sur Object Types (4), puis cochez la case (5)Computers.

🚺 CRLDistribution Properties	Permissions for CRLDistribution
General Sharii 1 Security Previous Versions Customize	Security
Object name: C:\CRLDistribution	Object name: C:\CRLDistribution
Group or user pamer:	Group of user names
CREATOR OWNER	
SYSTEM	SYSTEM
Administrators (RTPAAA\Administrators)	Administrators (RTPAAA\Administrators)
To change permissions, click Edit. 2 Edit	
Permissions for CREATOR OWNER Allow Denv	3 Add Remove
Full control	Permissions for CREATOR
Modify	
Read & execute	
Bead	Read & exec Object Types
Write	List folder co
Select Users, Computers, Service Accounts, or Groups	
Select this object type:	ac Object types:
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>):	Cosets
	Check Names
Advanced	UK Lancel

8. Dans le champ Entrez les noms des objets à sélectionner, entrez le nom d'ordinateur du serveur AC, puis cliquez sur Check Names. Si le nom saisi est valide, il est actualisé et est souligné. Cliquez sur 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

9. Choisissez l'ordinateur AC dans le champ Nom du groupe ou de l'utilisateur, puis vérifiez que l'option Contrôle total est activée Allow pour accorder un accès complet à l'AC. Cliquez sur OK, puis sur Close pour terminer la tâche.

	ion	
Security		
Object name: C:\CRLDistributio	n	
Group or user names:		
SCREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\A	dministrators)	
Sers (ABTOMAR\Users)		
WIN-231PNBS4IPH (ABTOM	AR\WIN-231PNB	S4IPH\$)
	Add	Remove
Permissions for	Add	Remove
Permissions for WIN-231PNBS4IPH	Add	Remove Deny
Permissions for WIN-231PNBS4IPH Full control	Allow	Deny
Permissions for WIN-231PNBS4IPH Full control Modify	Allow	Remove Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute	Add	Remove Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute	Add	Remove Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Allow	Remove
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove Deny
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove
Permissions for WIN-231PNBS4IPH Full control Modify Read & execute List folder contents Read	Add	Remove

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

Afin qu'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 Start. Sélectionnez Administrative Tools > Internet Information Services (IIS) Manager.

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 de la souris Default Web Site et choisissez Add Virtual Directory, 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 entré.

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

5. Cliquez sur les points de suspension (. . .) à droite du champ Chemin d'accès physique et accédez au dossier créé dans la section 1. Sélectionnez le dossier et cliquez sur οκ. Cliquez oκ pour fermer la fenêtre Ajouter un répertoire virtuel.

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	C	ancel	

6. Le nom de site entré à l'étape 4 doit être mis en surbrillance dans le volet gauche. Si ce n'est pas le cas, choisissez-le maintenant. Dans le volet central, double-cliquez sur Directory Browsing.

Internet Information Services (IIS) N	Manager					
↔ WIN-231PNBS4IP	PH + Sites +	Default Web	Site + CRLD	•		
File View Help						
Connections	CRI	LD Home	•			
Start Page	Filter:		• 🦻 Go - 🕻	Show All	Group by:	
Application Pools Sites Oefault Web Site Site CertEnroll CertSpy	ASP	Authentic	2 Compression	Default	Directory Browsing	Error Pages
> CRLD	Failed Request Tra	Handler Mappings	HTTP	HTTP	Logging	MIME Types
	Modules	Output	Request	SSI Settings		
	Managemen	Caching	Filtering	our occurrys		^

7. Dans le volet droit, cliquez sur Enable afin d'activer la navigation dans le répertoire.



8. Dans le volet gauche, sélectionnez à nouveau le nom du site. Dans le volet central, doublecliquez sur Configuration Editor.



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

Internet Information Services (IIS) 1	Manager			- 🗆 X
↔ WIN-231PNBS4IF	PH + Sites + Default Web Site + CRLD +			📅 🖂 🔂 🔞
File View Help				
Connections Connec	Configuration Editor Section: system.webServer/security/requestF	iltering • From: Default Web Site/CRLD Web.config		Actions Apply Ex Cancel Ex Generate Script
GetEnroll GetEnroll GetEnroll GetEnroll GetEnroll	allowDoubleEscaping allowHighBitCharacters alwaysAllowedQueryStrings alwaysAllowedUrIs demcOupsOstingSequencer	True False (Count=0)	~	Configuration Search Configuration Section (*) Lock Section
5 3 Crico	denyUrlSequences	(Count=0)		'allowDoubleEscaping'

Le dossier doit maintenant être accessible via IIS.

Configurer Microsoft CA Server pour publier des 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 au nouvel emplacement.

- 1. Dans la barre des tâches du serveur AC, cliquez sur Start. Sélectionnez Administrative Tools > Certificate Authority.
- 2. Dans le volet gauche, cliquez avec le bouton droit sur le nom de l'autorité de certification. ChoisissezProperties, puis cliquez sur l'Extensionsonglet. Afin d'ajouter un nouveau point de distribution CRL, cliquez sur Add.

Enrollment Agents	Auditing	Recove	ery Agents	Securit			
General	Policy Mo	Policy Module Exit					
Extensions	Storage Certificate Managers						
Select extension:							
CPI Distribution Paint	(CDD)						
CRL Distribution Foint	(CDF)						
Specify locations from	which users can	obtain a c	ertificate rev	ocation list			
(CRL).							
0.101-1-0.00	2\CertSrv\CertE	nroll\ <cal\< td=""><td>lame><crl< td=""><td>NameSuffix></td></crl<></td></cal\<>	lame> <crl< td=""><td>NameSuffix></td></crl<>	NameSuffix>			
C:\Windows\system3							
Idap:///CN= <catrune< td=""><td>catedName><cf< td=""><td>RLNameSu</td><td>ffix>,CN=<s< td=""><td>erverShortN</td></s<></td></cf<></td></catrune<>	catedName> <cf< td=""><td>RLNameSu</td><td>ffix>,CN=<s< td=""><td>erverShortN</td></s<></td></cf<>	RLNameSu	ffix>,CN= <s< td=""><td>erverShortN</td></s<>	erverShortN			
Idap:///CN= <catrune http://<serverdnsna file://<serverdnsnar< td=""><td>catedName><cf ame>/CertEnroll/ me>/CertEnroll/<</cf </td><td>RLNameSu <caname CaName></caname </td><td>ffix>,CN=<s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s </td></serverdnsnar<></serverdnsna </catrune 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu <caname CaName></caname 	ffix>,CN= <s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta< td=""></delta<></del 			
Idap:///CN= <catrunc http://<serverdnsna file://<serverdnsnar< th=""><th>catedName><cf ame>/CertEnroll/ me>/CertEnroll/<</cf </th><th>RLNameSu CaName CaName></th><th>ffix>,CN=<s ><crlname <crlname< th=""><th>erverShortN Suffix><del Suffix><delta< th=""></delta<></del </th></crlname<></crlname </s </th></serverdnsnar<></serverdnsna </catrunc 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu CaName CaName>	ffix>,CN= <s ><crlname <crlname< th=""><th>erverShortN Suffix><del Suffix><delta< th=""></delta<></del </th></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta< th=""></delta<></del 			
Idap:///CN= <catrune http://<serverdnsna file://<serverdnsnar< td=""><td>catedName><cf ame>/CertEnroll/ me>/CertEnroll/<</cf </td><td>RLNameSu CaName CaName></td><td>ffix>,CN=<s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s </td></serverdnsnar<></serverdnsna </catrune 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu CaName CaName>	ffix>,CN= <s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta< td=""></delta<></del 			
Idap:///CN= <catrunc http://<serverdnsna file://<serverdnsnar< td=""><td>catedName><cf ame>/CertEnroll/ me>/CertEnroll/<</cf </td><td>RLNameSu CaName CaName></td><td>ffix>,CN=<s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta ; ;</delta </del </td></crlname<></crlname </s </td></serverdnsnar<></serverdnsna </catrunc 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu CaName CaName>	ffix>,CN= <s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta ; ;</delta </del </td></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta ; ;</delta </del 			
Idap:///CN= <catrunc http://<serverdnsna file://<serverdnsnar< td=""><td>catedName><cf ame>/CertEnroll/ me>/CertEnroll/<</cf </td><td>RLNameSu <caname CaName></caname </td><td>ffix>,CN=<s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s </td></serverdnsnar<></serverdnsna </catrunc 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu <caname CaName></caname 	ffix>,CN= <s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta< td=""></delta<></del 			
Idap:///CN= <catrund http://<serverdnsnar file://<serverdnsnar <</serverdnsnar </serverdnsnar </catrund 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/<</cf 	RLNameSu CaName CaName>	ffix>,CN= <s ><crlname <crlname< td=""><td>erverShortN Suffix><del Suffix><delta< td=""></delta<></del </td></crlname<></crlname </s 	erverShortN Suffix> <del Suffix><delta< td=""></delta<></del 			
Idap:///CN= <catrunk http://<serverdnsnar file://<serverdnsnar < Publish CRLs to this Include in all CRLs. when publishing ma</serverdnsnar </serverdnsnar </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location . Specifies where anually.</cf 	RLNameSu (CaName) CaName>	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			
Idap:///CN= <catrunk http://<serverdnsnar ile://<serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma</serverdnsnar </serverdnsnar </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location Specifies where anually.</cf 	CaNameSu CaName>	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			
Idap:///CN= <catrunk http://<serverdnsnar ile://<serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP</serverdnsnar </serverdnsnar </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location Specifies where anually. ients use this to f extension of issu</cf 	RLNameSu (CaName) CaName>	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			
Idap:///CN= <catrunk http://<serverdnsnar ile://<serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP</serverdnsnar </serverdnsnar </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location Specifies where anually. ients use this to f extension of issues to this location</cf 	RLNameSu (CaName) CaName> (CaName> (CaName> (CaName) (CaN	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			
Idap:///CN= <catrunk http://<serverdnsnar ile://<serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs</serverdnsnar </serverdnsnar </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location Specifies where anually. ients use this to t extension of issuential to this location</cf 	RLNameSu (CaName) CaName>	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			
Idap:///CN= <catrunk http://<serverdnsna file://<serverdnsnar Publish CRLs to this Include in all CRLs. when publishing ma Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP e</serverdnsnar </serverdnsna </catrunk 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/ s location . Specifies where anually. ients use this to f extension of issu to this location extension of issu</cf 	RLNameSu (CaName) CaName> (CaName> (CaName> (CaName) (CaN	ffix>,CN= <s ><crlname <crlname dd</crlname </crlname </s 	e Directory			

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

\\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.	as, ⊂t
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable:	
<caname> V Insert</caname>	
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crln< td=""><td>la</td></crln<></caname></serverdnsname>	la
<	>
OK Cancel	

4. Lorsque le champ Emplacement est renseigné, choisissez une variable dans la liste déroulante Variable, puis cliquez sur 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. Dans la liste déroulante Variable, sélectionnez, puis cliquez sur 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.	s. t
Location:	
\\WIN-231PNBS4IPH\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>à</td></crlnames<></caname></servername>	à
< 2	*
OK Cancel	

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

\\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><CRLNameSı <</td>

OK

7. Cliquez sur OK pour revenir à l'onglet Extensions. Cochez cette Publish CRLs to this location case, 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.

×

Inroliment Agents	Auditing	Recovery Agen	ts Security		
General	Policy Mo	dule	Exit Module		
Extensions	Storage	Storage Certificate Managers			
elect extension:					
CRL Distribution Point	(CDP)		~		
specity locations from (CRL). C:\Windows\system3	which users car	n obtain a certificate	e revocation list		
Idap:///CN= <catrun http://<serverdnsna file://<serverdnsnar XWIN-231PNBS4IP</serverdnsnar </serverdnsna </catrun 	Certificat me me>	You must restat take effect. Do	rt Active Directory C you want to restart	ertificate Services for the changes to the service now?	

8. Dans le volet gauche, cliquez avec le bouton droit sur Revoked Certificates. Sélectionnez All Tasks > Publish. Assurez-vous que l'option Nouvelle liste de révocation de certificats est sélectionnée, puis cliquez sur ok.

🙀 certsrv - [Certification Autho	rity (Local)\abtoma	r-Wli	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			

Le serveur d'autorité de certification Microsoft doit créer un nouveau fichier .crl dans le dossier créé à la section 1. Si le nouveau fichier CRL est créé avec succès, aucune boîte de dialogue ne s'affiche une fois que vous avez cliqué sur OK. Si une erreur est renvoyée concernant le nouveau dossier de point de distribution, répétez soigneusement chaque étape de cette section.

Vérifiez que le fichier CRL existe et qu'il est accessible via IIS

Avant de commencer cette section, vérifiez que les nouveaux fichiers CRL existent et qu'ils sont accessibles via IIS à partir d'une autre station de travail.

1. Sur le serveur IIS, ouvrez le dossier créé à la section 1. Un seul fichier .crl doit être présent sous la forme

```
.crl
OÙ
```

est le nom du serveur AC. Dans cet exemple, le nom du fichier est :

abtomar-WIN-231PNBS4IPH-CA.crl



2. À partir d'une station de travail sur le réseau (idéalement sur le même réseau que le noeud Administrateur principal ISE), ouvrez un navigateur Web et accédez à http://

```
où
est le nom du serveur IIS configuré dans la section 2 et
est le nom du site choisi pour le point de distribution dans la section 2. Dans cet exemple,
l'URL est :
```

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

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



Configurer ISE pour utiliser le nouveau point de distribution CRL

Avant de configurer ISE pour récupérer la liste de révocation de certificats, définissez l'intervalle de publication de la liste. 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 inclus. 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 Start. Sélectionnez Administrative Tools > Certificate Authority.
- 2. Dans le volet gauche, développez l'autorité de certification. Cliquez avec le bouton droit sur le Revoked Certificates dossier et sélectionnez Properties.
- 3. Dans les champs d'intervalle de publication de la liste CRL, saisissez le nombre requis et choisissez la période. Cliquez sur ox pour fermer la fenêtre et appliquer la modification. Dans cet exemple, un intervalle de publication de sept jours est configuré.



4. Entrez la certutil -getreg CA\Clock* commande permettant de 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 certutil -getreg CA\CRLov* commande permettant de 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, notez 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 certutil -getreg CA\CRLpe* commande permettant de 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 le délai de grâce CRL comme suit :

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

Sinon : OVERLAP = (CRLPériod / 10), en minutes

b. Si CHEVAUCHEMENT > 720, CHEVAUCHEMENT = 720

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

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

e. Délai de grâce = CHEVAUCHEMENT + minutesDésalignementHorloge

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 laps de temps entre le moment où l'autorité de certification

publie la liste de révocation de certificats suivante et le moment où la liste de révocation de certificats actuelle expire. ISE doit être configuré pour récupérer les LCR en conséquence.

8. Connectez-vous au noeud Administrateur principal ISE et sélectionnez Administration > System > Certificates. Dans le volet gauche, sélectionnez Trusted Certificate.

E Cisco ISE					Adminis	stration · System					
Deployment Licensing	Certificate	s Logging	Maintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certifi	cates								
Trusted Certificates	/ Edit	+ Import 🐽 Ex	port 🔋 Delete	Q View							
OCSP Client Profile Certificate Signing Requests		Friendly Name		∧ Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio
Certificate Periodic Check Se	0	Baltimore CyberTrust	Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust	Baltimore CyberTrust	Sat, 13 May 2000	Tue, 13 May 2025	
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 2	099	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 souhaitez configurer les listes de révocation de certificats. Cliquez sur Edit.
- 10. Près du bas de la fenêtre, cochez la Download CRL case.
- 11. Dans le champ CRL Distribution URL, 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 CRL à intervalles réguliers ou en fonction de l'expiration (qui, en général, est également un intervalle régulier). Lorsque l'intervalle de publication des LCR est statique, des mises à jour plus opportunes des LCR 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 au délai de grâce calculé à l'étape 7. Si le jeu de valeurs est plus long que le délai de grâce, ISE vérifie le point de distribution de la liste de révocation de certificats avant que l'autorité de certification n'ait publié la liste suivante. Dans cet exemple, le délai de grâce est calculé sur 730 minutes, soit 12 heures et 10 minutes. Une valeur de 10 heures sera utilisée pour la récupération.
- 14. Définissez l'intervalle de nouvelle tentative en fonction de votre environnement. Si ISE ne peut pas récupérer la liste de révocation de certificats à l'intervalle configuré à l'étape précédente, il réessaiera à cet intervalle plus court.
- 15. Cochez cette Bypass CRL Verification if CRL is not Received Case pour permettre à l'authentification basée sur certificat de continuer normalement (et sans vérification de la liste de révocation de certificats) 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 les certificats avec des certificats émis par cette autorité de certification échouera si la liste de révocation de certificats ne peut pas être récupérée.
- 16. Cochez cette Ignore that CRL is not yet valid or expired case pour permettre à ISE d'utiliser les 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'effet et après ses heures de mise à jour suivante.

Cliquez s_{ave} sur pour terminer la configuration.

Certificate Status Validation							
To verify certifica OCSP Configurati Validate aga Reject 1 Certificate Revoca Validate description descriptin description description description description description desc	ites, enable the me on ainst OCSP Service the request if OCS the request if OCS ation List Configurat RL	thods below. If bot p P returns UNKNOV P Responder is ur	h are enabled, OCSP ~ WN status wreachable	P will always be t	ried first.		
CRL Di	istribution URL	http://win-231p	nbs4iph/crld/abto				
Retriev	Ve CRL	 Automatically Every 	10		Hours	~	before expiration.
If down	nload failed, wait	10		Minutes	~	before retry.	
— En 19 19	nable Server Identi ypass CRL Verifica nore that CRL is n	ty Check () tion if CRL is not F ot yet valid or expl	teceived				

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.