Éditez les listes des révocations de certificat pour ISE sur un exemple de configuration du serveur de Microsoft CA

Contenu

Introduction Conditions préalables **Conditions requises** Composants utilisés **Conventions** Configurer Configurations La section 1. créent et configurent un répertoire sur le CA pour loger les fichiers CRL La section 2. créent un site dans IIS pour exposer le nouveau point de distribution CRL La section 3. configurent le serveur de Microsoft CA pour éditer des fichiers CRL au point de distribution La section 4. vérifient le fichier CRL existe et est accessible par l'intermédiaire d'IIS La section 5, configurent ISE pour utiliser le nouveau point de distribution CRL Vérifier Dépanner Informations connexes

Introduction

Ce document décrit la configuration d'un serveur de Microsoft Certificate Authority (CA) qui dirige l'Internet Information Services (IIS) pour éditer des mises à jour de Liste des révocations de certificat (CRL). Il explique également comment configurer le Logiciel Cisco Identity Services Engine (ISE) (versions 1.1 et ultérieures) récupérer les mises à jour pour l'usage dans la validation de certificat. ISE peut être configuré pour récupérer CRLs pour les divers certificats racine CA qu'il l'utilise dans la validation de certificat.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

logiciel suivantes :

- Version 1.1.2.145 de Logiciel Cisco Identity Services Engine
- [®] 2008 R2 de serveur de ^{® de} Microsoft Windows

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurezvous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco</u>.

Configurer

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

Remarque: Utilisez l'outil <u>Command Lookup Tool</u> (clients <u>enregistrés</u> seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Ce document utilise les configurations suivantes :

- La section 1. créent et configurent un répertoire sur le CA pour loger les fichiers CRL
- La section 2. créent un site dans IIS pour exposer le nouveau point de distribution CRL
- La section 3. configurent le serveur de Microsoft CA pour éditer des fichiers CRL au point de distribution
- La section 4. vérifient le fichier CRL existe et est accessible par l'intermédiaire d'IIS
- La section 5. configurent ISE pour utiliser le nouveau point de distribution CRL

La section 1. créent et configurent un répertoire sur le CA pour loger les fichiers CRL

La première tâche est de configurer un emplacement sur le serveur CA pour enregistrer les fichiers CRL. Par défaut, le serveur de Microsoft CA édite les fichiers à C:\Windows\system32\CertSrv\CertEnroll\. Plutôt qu'utilisent ce dossier système, créent un nouveau répertoire pour les fichiers.

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



2. Pour que le CA écrive les fichiers CRL au nouveau répertoire, partageant doit être activé. Cliquez avec le bouton droit le nouveau répertoire, choisissez Properties, cliquez sur l'**onglet Partage**, et puis cliquez sur **partager**

1	CRLDistribution Properties	×
	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. Advanced Sharing	
avancé -	Close Cancel Apply	

3. Afin de partager le répertoire, cochez le **partage cette** case de **répertoire** et puis ajoutez un symbole dollar (\$) à la fin du nom de partage dans le domaine de nom de partage de

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

masquer le partage.

4. Cliquez sur les **autorisations** (1), cliquez sur Add (2), cliquez sur les **types d'objet** (3), et cochez la case d'**ordinateurs**

		_		
Permissions for CRLDistribution	1\$	Selec	ct Users, Computers, Service Accounts, or Groups	? ×
Share Permissions		Sel	lect this object type:	
Group or user names		Us	ers, Groupe, or Built in security principals	Object Types
🍇 Everyone		Fior	m this location	
		itpe	esaloca	Locations
		Enb	ter the object names to select (examples)	
			Press water	Charle Marray
0			Object Types	MX
Z _	A01	iamo I	Select the types of objects you want to find	
Permissions for Everyone	Alox	Deny	A Object types:	
Full Control			🔽 🍇 Duit-in security principals	
Change Boart		음	Service Accounts	
11000		-		
			🗹 🔱 Users	
Learn about access control and per	nsaons			
OK.	Cancel	Apply	OK	Cancel
	Permissions for CRLDistribution Share Permissions Group or user names Everyone 2 Permissions for Everyone Full Control Change Read Learn about access control and per	Permissions for CRLDistribution; Share Permissions Group or user names: Everyone 2 Add Permissions for Everyone Alow Full Centrel	Permissions for CRLDistribution# Selection Share Permissions Selection Group or user names: Fin Permissions for Everyone Permissions for Everyone Permissions for Everyone Alow Dency Image Full Central Image Read Image Learn about access: control and permission: OK Cencel	Permissions for CRLDistribution# Select Users, Computers, Service Accounts, or Groups Share Permissions Select this abject type: Users, Groups, or Built in security principals Group or user names: Users, Groups, or Built in security principals Everyone Everyone 2 Add. Permissions for Everyone Alow Dependent type: Object Types Select the types: Select type: Full Central Image Read Image Dependent control and poemesions Image OK Cencel

5. Afin de retourner aux utilisateurs choisis, les ordinateurs, fenêtre de comptes des services, ou de groupes, cliquent sur OK. Dans l'entrer les noms d'objet pour sélectionner le champ, écrire le nom de l'ordinateur du serveur CA et du **contrôle de** clic **nomme**. Si le nom écrit est valide, le nom régénère et semble souligné. Cliquez sur

Select Users, Computers, Service Accounts, or G	roups	? ×
Select this object type:		
Users, Computers, Groups, or Built-in security principals	1	Object Types
From this location:		
rtpaaa.local		Locations
Enter the object names to select (<u>examples</u>):		
RTPAAA-DC1		Check Names
		8
Advanced	OK	Cancel

6. Dans le groupe ou les noms d'utilisateur mettez en place, choisissez l'ordinateur CA. Le contrôle **tiennent compte** pour que le plein contrôle accorde l'accès complet au CA cliquent sur OK. Cliquez sur OK de nouveau pour fermer la fenêtre partageante avancée et pour retourner à la fenêtre de

Permissions for CRLDistribu	tion\$						
Share Permissions							
Group or user names:							
Serveryone							
RTPAAA-DC1 (RTPAAA\R	RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$)						
530							
	Add	Remove					
Permissions for RTPAAA-DC1	Allow	Deny					
Full Control							
Change							
Read							
Learn about access control and	permissions						
	Sector contraction						

Properties.

 Afin de permettre au CA pour écrire les fichiers CRL au nouveau répertoire, configurez les autorisations appropriées de Sécurité. Cliquez sur l'onglet Sécurité (1), cliquez sur Edit (2), cliquez sur Add (3), cliquez sur les types d'objet (4), et cochez la case d'ordinateurs



8. Dans l'entrer les noms d'objet pour sélectionner le champ, écrire le nom de l'ordinateur du serveur CA et du **contrôle de** clic **nomme**. Si le nom écrit est valide, le nom régénère et semble souligné. Cliquez sur

Select Users, Computers, Service Accounts, or Gro	ups	? ×
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. Choisissez l'ordinateur CA dans le groupe ou les noms d'utilisateur mettent en place et puis vérifient **tiennent compte** pour que le plein contrôle accorde l'accès complet au CA cliquent sur OK et puis cliquent sur **près de** complet la

Security Object name: C:\CRLDistribution Group or user names: CREATOR OWNER SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\ATPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Permissions for CRLDistribut	ion	
Object name: C:\CRLDistribution Group or user names: CREATOR OWNER SYSTEM SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Security		
Group or user names: CREATOR OWNER SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Object name: C:\CRLDistributio	on	
REATOR OWNER Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	Group or user names:		
SYSTEM Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read	& CREATOR OWNER		
Administrators (RTPAAA\Administrators) RTPAAA-DC1 (RTPAAA\RTPAAA-DC1\$) Users (RTPAAA\Users) Add Remove Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Modify Read & execute List folder contents Read U	SYSTEM		
Add Add Remove Add Remove Add Remove Add Remove Add Add Remove Add Remove Add Remove Add Remove Add Remove Add Remove Add Add Remove Add Add Remove Add Add Remove Add Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control <td>Administrators (RTPAAA\Adr</td> <td>ninistrators)</td> <td></td>	Administrators (RTPAAA\Adr	ninistrators)	
Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control image: Cont		PAAA-DUT\$j	
Add Remove Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control image: Cont			
Permissions for RTPAAA-DC1 Allow Deny Full control Image: Second	1	Add	Persous
Permissions for RTPAAA-DC1 Allow Deny Full control Image: Control delta delt		Add	nemove
Full control Image: Control Modify Image: Control Read & execute Image: Control List folder contents Image: Control Read Image: Control	Permissions for RTPAAA-DC1	Allow	Deny
Modify Image: Constant sector Read & execute Image: Constant sector List folder contents Image: Constant sector Read Image: Constant sector	Full control		
Read & execute List folder contents Read	Modify		
List folder contents Read	Read & execute		
Read 🗹 🗖	1. Second and a first state of the second state		
	List folder contents	1000 C	
	List folder contents Read Learn about access control and p	ermissions	

La section 2. créent un site dans IIS pour exposer le nouveau point de distribution CRL

Pour qu'ISE accède aux fichiers CRL, faites le répertoire qui loge les fichiers CRL accessibles par l'intermédiaire d'IIS.

- 1. Sur la barre des tâches de serveur IIS, **début de** clic. Choisissez le **gestionnaire d'outils d'administration > d'Internet Information Services (IIS)**.
- 2. Dans le volet gauche (connu sous le nom d'arborescence de la console), développez le nom du serveur IIS et puis développez les sites.



3. Cliquez avec le bouton droit le site Web par défaut et choisissez ajoutent le répertoire

Internet Informat	ion S	ervices	(11	5) Ma	nag	ger	
	RTPA	AA-DC1	ŀ	Sites)	Default	Web Si
File View Help							
Connections							20
😪 - 🔚 🖄 🐼							
Start Page RTPAAA-DC1 (F Application I Sites	(TPAA Pools	A\Admini	stra	ator)			
		Explore	;				
		Edit Pe	rmis	sions	4		
	2	Add Ap	plic	ation			
	2	Add Vir	tua	l Direct	ory		
		Edit Bir	ding	gs			
		Manag	e W	eb Site		•	
	127	Refres	h				
	×	Remov	е				2
		Renam	е				
		Switch	to (Ionten	t Vie	ew	

virtuel.

4. Dans le domaine de pseudonyme, écrivez un nom du site pour le point de distribution CRL. Dans cet exemple, CRLD est

dd ¥irtual Dire	ectory		
Site name:	Default Web Site		
Path:			
Alias:			
CRLD			
Example: imag	es		
Physical path:			
Pass-through a	authentication		
Connect as	Test Settings		
		ОК	Cancel

5. Cliquez sur les points de suspension (...) à la droite du gisement physique de chemin et parcourez au répertoire créé dans la section 1. choisie le répertoire et cliquez sur OK. Cliquez sur OK pour fermer la fenêtre de répertoire virtuel

ju virtual Diret	cory			
Site name: De Path: /	afault Web Site			
Alias:				
CRLD				
Example: images				
Physical path:				
C:\CRLDistributio	n			
Pass-through au	thentication			
Connect as	Test Settings			
		OK	Can	cel

d'ajouter.

6. Le nom du site écrit dans l'étape 4 devrait être mis en valeur dans le volet gauche. Sinon, choisissez-le maintenant. Dans le volet central, **répertoire de** double clic **parcourant**.



7. Dans le volet de droite, **enable de** clic pour activer le répertoire parcourant.

Directory Browsing	Alerts
	Directory bro disabled.
Use this feature to specify the information that displays in a directory listing.	Actions
Ime Time	Apply
🔽 Size	Cancel
Kension	Enable
₩ D <u>a</u> te	🕜 Help
Long date	Online Help

8. Dans le volet gauche, choisissez le nom du site de nouveau. Dans le volet central, **éditeur de configuration de** double clic.



 Dans la liste déroulante de section, choisissez system.webServer/Sécurité/requestFiltering. Dans la liste déroulante allowDoubleEscaping, choisissez vrai. Dans le volet de droite, cliquez sur Apply.

► CRLD ►					
Configuration Editor Section: system.webServer/security/reque	stFikering - From: Default Web Site/CRLD Web.config	Actions Apply Actions Cancel			
Despect Bath MACHINE AVERDOOT	ADDUGET	Generate Script			
alowDoubleEscaping	True	Configuration			
alowHighBitCharacters	True	Configuration			
alwaysAllowedQueryStrings	False	Search Conngurat			
alwaysAllowedUrls	(count=o)	Section			
denyQueryStringSequences	(Count=0)	Lock Section			
denyUrlSequences	(Count=0)	LOCK DECOURT			
fileExtensions		'allowDoubleEscapii			
filteringRules	(Count=0)	Attribute			
hiddenSegments		Lock Attribute			
requestLimits		D Hab			
unescapeQueryString	True	a nep			
🕀 verbs		Online Help			

Le répertoire devrait maintenant être accessible par l'intermédiaire d'IIS.

La section 3. configurent le serveur de Microsoft CA pour éditer des fichiers CRL au point de distribution

Maintenant qu'un nouveau répertoire a été configuré pour loger les fichiers CRL et le répertoire a été exposé dans IIS, configurez le serveur de Microsoft CA pour éditer les fichiers CRL au nouveau emplacement.

- 1. Sur la barre des tâches de serveur CA, **début de** clic. Choisissez les **outils d'administration >** l'autorité de certification.
- 2. Dans le volet gauche, cliquez avec le bouton droit le nom CA. Choisissez Properties et alors cliquez sur les **extensions** tableau afin d'ajouter un nouveau point de distribution CRL,

rtp	aaa-CA Properties			? ×
	Enrollment Agents General Extensions	Auditing Re Policy Module Storage	covery Agents Exit Certificate N	Security Module fanagers
	Select extension:			
	CRL Distribution Point	(CDP)		•
	Specify locations from v (CRL).	which users can obtai	n a certificate revo	ocation list
	C:\Windows\system32 Idap:///CN= <catrund http://<serverdnsnar file://<serverdnsnar< td=""><td>2\CertSrv\CertEnroll\ atedName><crlnar me>/CertEnroll/<can he>/CertEnroll/<can< td=""><td>(CaName><crln meSuffix>,CN=<sa lame><crlnames ame><crlnames< td=""><td>ameSuffix>≺l erverShortNai Suffix>≺Delta uffix>≺DeltaC</td></crlnames<></crlnames </sa </crln </td></can<></can </crlnar </td></serverdnsnar<></serverdnsnar </catrund 	2\CertSrv\CertEnroll\ atedName> <crlnar me>/CertEnroll/<can he>/CertEnroll/<can< td=""><td>(CaName><crln meSuffix>,CN=<sa lame><crlnames ame><crlnames< td=""><td>ameSuffix>≺l erverShortNai Suffix>≺Delta uffix>≺DeltaC</td></crlnames<></crlnames </sa </crln </td></can<></can </crlnar 	(CaName> <crln meSuffix>,CN=<sa lame><crlnames ame><crlnames< td=""><td>ameSuffix>≺l erverShortNai Suffix>≺Delta uffix>≺DeltaC</td></crlnames<></crlnames </sa </crln 	ameSuffix>≺l erverShortNai Suffix>≺Delta uffix>≺DeltaC
	•			Þ
			Add	Remove
	Publish CRLs to this	s location		
	Include in all CRLs. when publishing ma	Specifies where to p mually.	ublish in the Active	e Directory
	🔲 Include in CRLs. Cli	ients use this to find D	elta CRL location	s.
	Include in the CDP	extension of issued c	ertificates	
	Publish Delta CRLs	to this location		
	Include in the IDP e	extension of issued CF	9Ls	
cliquez sur Add.	ОК	Cancel	Apply	Help

3. Dans le champ Location, entrez dans le chemin au répertoire créé et partagé dans la section 1. Dans l'exemple dans la section 1, le chemin est :

\\RTPAAA-DC1\CRLDistribution\$\

Add Location
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.
Location:
\\RTPAAA-DC1\CRLDistribution\$\
Mariable.
Variable:
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. Le champ Location étant rempli, choisissez le **<CaName> de la** liste déroulante variable et puis cliquez sur

Add Location	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file addres or enter a UNC or local path. To insert a variable into the URL or path, selec the variable below and click Insert.	s, :t
Location:	
\\RTPAAA-DC1\CRLDistribution\$\ <caname></caname>	
Variable:	
<caname></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	

l'insertion.

5. De la liste déroulante variable, choisissez le **<CRLNameSuffix>** et puis cliquez sur

Add Location	×
A location can be any valid URL or path. Enter an HTTP, LDAP, file add or enter a UNC or local path. To insert a variable into the URL or path, se the variable below and click Insert.	lress, elect
Location:	
\\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><crlna< td=""><td>meSi</td></crlna<></caname></servername>	meSi
	Þ
OK Cance	
on.	

6. Dans le champ Location, ajoutez .crl à l'extrémité du chemin. Dans cet exemple, l'emplacement est :

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

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.
\\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><crlnamesi< td=""></crlnamesi<></caname></servername>
Appends a suffix to distinguish the CRL file name Example location: http:// <servername>/CertEnroll/<caname><crlnamesi< td=""></crlnamesi<></caname></servername>

7. Cliquez sur OK pour retourner à l'onglet d'extensions. Cochez l'édition CRLs dans cette case d'emplacement (1) et puis cliquez sur OK (2) pour fermer la fenêtre de Properties. Une demande apparaît pour que l'autorisation redémarre des services de certificat de Répertoire actif. Clic oui

(3).

rtpaaa-CA Properties	
Enrollment Agents Auditing Recovery Agents Security General Policy Module Exit Module Extensions Storage Certificate Managers	
Select extension:	
CRL Distribution Point (CDP)	
Specify locations from which users can obtain a certificate revocation list (CRL).	
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	
1 I Publish CRLs to this location	
Include in all C Certification Authority when publishin	×
 Include in CRL Include in the I You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now? 	
Publish Delta (
Include in the I	
2 OK Cancel Apply Help	

 Dans le volet gauche, le clic droit a retiré des Certificats. Choisissez toutes les tâches > éditent. Assurez-vous que nouveau CRL est sélectionné et puis cliquez sur OK.



Le serveur de Microsoft CA devrait créer un nouveau fichier dans le dossier .crl créé dans la section 1. Si le nouveau fichier CRL est créé avec succès il n'y aura aucun dialogue après que CORRECT est cliqué sur. Si une erreur est retournée en vue de le nouveau répertoire de point de distribution, répétez soigneusement chaque étape dans cette section.

La section 4. vérifient le fichier CRL existe et est accessible par l'intermédiaire d'IIS

Vérifiez les nouveaux fichiers CRL existent et cela ils sont accessibles par l'intermédiaire d'IIS d'un autre poste de travail avant que vous commenciez cette section.

 Sur le serveur IIS, ouvrez le répertoire créé dans la section 1. Il devrait y a un fichier simple .crl actuel avec la forme <CANAME>.crl où <CANAME> est le nom du serveur CA. Dans cet exemple, le nom du fichier est : rtpaaa-CA.crl

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

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

http://RTPAAA-DC1/CRLD

Les affichages d'index de répertoire, qui inclut le fichier ont observé dans l'étape

	G republication			
🗌 rtpaaa-dc1 - /C	RLD/	+		
	1 4 1	CDI	D/	
rtpaaa-	-dc1 - /(D/	
rtpaaa-	-dcl - /		D/	
rtpaaa-	-dcl - /		D/	

La section 5. configurent ISE pour utiliser le nouveau point de distribution CRL

Avant qu'ISE soit configuré pour récupérer le CRL, définissez l'intervalle pour éditer le CRL. La stratégie pour déterminer cet intervalle est hors de portée de ce document. Les valeurs potentielles (à Microsoft CA) sont de 1 heure à de 411 ans, d'incluses. La valeur par défaut est de 1 semaine. Une fois qu'un intervalle approprié pour votre environnement a été déterminé, placez l'intervalle avec ces instructions :

1. Sur la barre des tâches de serveur CA, début de clic. Choisissez les outils d'administration >

l'autorité de certification.

- 2. Dans le volet gauche, développez le clic droit CA le répertoire **retiré de Certificats** et choisissez Properties.
- Dans les domaines d'intervalle de publication CRL, introduisez le nombre requis et choisissez le délai prévu. Cliquez sur OK pour fermer la fenêtre et pour appliquer la modification. Dans cet exemple, un intervalle de publication de 7 jours est configuré.

🧱 certsrv - [Certification	n Authority	(Local)\rtpaa	a-CA\	Revoked Certificates]		
File Action View Hel	lp .					
(+ - +) 🖄 🔄 🖸	- ?					
Certification Authority (I	Local)	Request ID	Rev	Revoked Certificates Prope	rties	2 🛛 🛓
rtpaaa-CA	All Tasks	6	5/8 5/8 5/8	CRL Publishing Parameters	/iew CRLs ICRL) describes certificates t	hat clients should
Pending Reque	View	•	5/8	consider invalid.		
Certificate Ter	Refresh	þ	5/8 5/8	CRL publication interval:	7 Days	•
	Export List	··· 2	5/8 5/8	Next update:	12/20/2012 8:45 AM	
	Help		5/8 5/8	Publish Delta CRLs		
		20 29 29	5/8 5/8	Publication interval:	1 Hours	
		33	5/8 5/8	Next update:		
		35	5/8			
		37	5/8			
		00-139 00-140	5/8 5/9			
		41	5/3			
		48	5/3			
		49	6/2			
		50	6/2	ОК	Cancel Apply	Help
Opens the properties dialog b	box for the cu	urrent selection.			1	

Vous devriez maintenant confirmer plusieurs valeurs de registre, qui aideront à déterminer les configurations de récupération CRL dans ISE.

4. Écrivez le **certutil - le getreg CA** \ commande de **Clock*** de confirmer la valeur de ClockSkew. La valeur par défaut est de 10 minutes.Exemple de sortie :

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

5. Écrivez le certutil - le getreg CA \ commande de CRLov* de vérifier si le CRLOverlapPeriod a été manuellement placé. Par défaut la valeur de CRLOverlapUnit est 0, qui indique qu'aucune valeur manuelle n'a été placée. Si la valeur est une valeur autre que 0, enregistrez la valeur et les unités.Exemple de sortie :

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

6. Écrivez le certutil - le getreg CA \ commande de CRLpe* de vérifier le CRLPeriod, qui a été placé dans l'étape 3.Exemple de sortie : Values: CRLPeriod REG_SZ = Days CRLUnits REG_DWORD = 7 CertUtil: -getreg command completed successfully.

7. Calculez le délai de grâce CRL comme suit :Si CRLOverlapPeriod était placé dans l'étape 5 : SUPERPOSITION = CRLOverlapPeriod, en quelques minutes ;Autrement : SUPERPOSITION = (CRLPeriod/10), en quelques minutesSi SUPERPOSITION > puis SUPERPOSITION 720 = 720Si SUPERPOSITION < (1.5 * SUPERPOSITION de ClockSkewMinutes) puis = (1.5 * ClockSkewMinutes)Si SUPERPOSITION > CRLPeriod, dans la SUPERPOSITION de minutes puis = le CRLPeriod en quelques minutesDélai de grâce = 720 minutes + 10 minutes = 730 minutesExemple :

```
As stated above, CRLPeriod was set to 7 days, or 10248 minutes and CRLOverlapPeriod was not set.
```

```
a. OVERLAP = (10248 / 10) = 1024.8 minutes
b. 1024.8 minutes is > 720 minutes : OVERLAP = 720 minutes
c. 720 minutes is NOT < 15 minutes : OVERLAP = 720 minutes</li>
d. 720 minutes is NOT > 10248 minutes : OVERLAP = 720 minutes
e. Grace Period = 720 minutes + 10 minutes = 730 minutes
```

Le délai de grâce calculé est la durée entre quand le CA édite le prochain CRL et quand le courant CRL expire. ISE doit être configuré pour récupérer le CRLs en conséquence.

 Ouvrez une session au noeud primaire d'admin et choisissez la gestion > le système > les Certificats. Dans le volet gauche, mémoire choisie de certificat.

🏟 Home Operations 🔻 Policy 🔻 Admin	istrați	on 🔻					00 Task Nave
🔆 System 🛛 💐 Identity Management 🛛 🖩	Netv	vork Re	sources	👪 Web Porta	al Management		
Deployment Licensing Certificates Logg	ng	Mainte	anance A	dmin Access	Settings		
Certificate Operations	Ce	ertifica	te Store				Selected 0 Total ?
Certificate Signing Requests		/ Edt		Export	XDelete	Show	AI
O Certificate Store	C	Frien	dly Name			▲ Issued To	Issued By
SCEP CA Profiles	C	RTP/	AAA-DC1-MSC	EP-RA1#rtpa	aa-CA#00002	RTPAAA-DC1-MS	CEP-R rtpaaa-CA
S OCSP Services		l rtpaa	a-CA#rtpaaa	-CA#00001		rtpaaa-CA	rtpaaa-CA

- 9. Cochez la case de mémoire de certificat à côté du certificat de CA pour lequel vous avez l'intention de configurer CRLs. Cliquez sur **Edit**.
- 10. Près du bas de la fenêtre, cochez la case du téléchargement CRL.
- 11. Dans le champ URL de distribution CRL, entrez dans le chemin au point de distribution CRL, qui inclut le fichier .crl, créé dans la section 2. Dans cet exemple, l'URL est : http://RTPAAA-DC1/CRLD/rtpaaa-ca.crl
- 12. ISE peut être configuré pour récupérer le CRL à intervalles réguliers ou être basé sur l'expiration (qui, est généralement également un intervalle régulier). Quand les CRL éditent

l'intervalle est charge statique, des mises à jour plus opportunes CRL sont obtenus quand la dernière option est utilisée. Cliquez sur **automatiquement la** case d'option.

- 13. Placez la valeur pour la récupération à une valeur moins que le délai de grâce calculé dans l'étape 7. Si le positionnement de valeur est plus long que le délai de grâce, ISE vérifie le point de distribution CRL avant que le CA ait édité le prochain CRL. Dans cet exemple, le délai de grâce est calculé pour être de 730 minutes, ou de 12 heures et de 10 minutes. Une valeur de 10 heures sera utilisée pour la récupération.
- 14. Placez le retry interval comme approprié pour votre environnement. S'ISE ne peut pas récupérer le CRL à l'intervalle configuré dans l'étape précédente, il relancera à cet intervalle plus court.
- 15. Cochez la vérification du contournement CRL si CRL n'est pas case reçue pour permettre à l'authentification basée sur certificat pour poursuivre normalement (et sans contrôle CRL) s'ISE ne pouvait pas récupérer le CRL pour ce CA dans sa dernière tentative de téléchargement. Si cette case n'est pas cochée, toute l'authentification basée sur certificat avec des Certificats délivrés par ce CA échouera si le CRL ne peut pas être récupéré.
- 16. Cochez l'ignorer que CRL n'est pas case encore valide ou expirée pour permettre à ISE pour utiliser (ou pas encore valide) les fichiers expirés CRL comme s'ils étaient valides. Si cette case n'est pas cochée, ISE considère comme étant un CRL non valide avant leur date effective et après leurs minuteurs de mise à jour suivants. Sauvegarde de clic pour se terminer la configuration

configuration.

Issued By						
	rtpaaa-CA					
Valid From	Sat, 11 Feb 2012 19	9:32:02 EST				
Valid To (Expiration)	Wed, 11 Feb 2037 1	19:42:01 EST				
Serial Number	1D 85 1D 58 36 8C 8	EC 93 4E F6 5B 28 9	9B 26 E7 89			
Usage						
All Trust Certificates are av and administrative authent	alable for selection a lication below:	as the Root CA for s	ecure LDAP conne	ctions. In addition,	they may be enal	bled for EAP-TLS
Trust for client authen	tication					
Enable Validation of	Certificate Extension	ns (accept only valid	certificate)			
Reject the reque	st if certificate statu.		marca by o'cor			
Certificate Revocation	st if certificate statu List Configuration	1		_		
Certificate Revocation	st if certificate statu					
Certificate Revocation Certificate Revocation CRL Distribution U	Ist Configuration	ı ıa-dc1/CRLD/rtpaaa-C	A.crl]
Certificate Revocation Certificate Revocation CRL Distribution U	List Configuration	a-dc1/CRLD/rtpaaa-C	A.crl	Hours] before expiratio
Certificate Revocation Control Download CRL CRL Distribution U Retrieve CRL	Ist Configuration JRL http://rtpaaa O	a-dc1/CRLD/rtpaaa-C	CA.crl	Hours	_] before expiratio
Certificate Revocation Certificate Revocation CRL Distribution U Retrieve CRL	Ist if certificate statu List Configuration JRL http://rtpaa Automatical Every	a-dc1/CRLD/rtpaaa-C	CA.crl	Hours Weeks		before expiratio
Certificate Revocation Certificate Revocation CRL Distribution U Retrieve CRL If download failed	st if certificate statu List Configuration JRL http://rtpaa: O Automatical O Every 1, wait 1	a-dc1/CRLD/rtpaaa- lly 10	CA.crl	Hours Weeks	▼ ■ ■ ■ ■	before expiratio
Certificate Revocation Download CRL CRL Distribution L Retrieve CRL If download failed Revocation CRL If with the reque	st if certificate statu List Configuration JRL http://rtpaa: O Automatical C Every 1, wait 1 erification if CRL is po	a-dc1/CRLD/rtpaaa-(CA.crl	Hours Weeks	↓ ↓ ↓ before retry.) before expiratio
Certificate Revocation Certificate Revocation CRL Distribution U Retrieve CRL If download failed Bypass CRL V G Ignore that C	st if certificate statu List Configuration JRL http://rtpaa: O Automatical O Every 1, wait 1 erification if CRL is no RL is not yet valid or	a-dc1/CRLD/rtpaaa-(ily 10 0 ot Received r expired	CA.crl	Hours Weeks	v before retry.	before expiratio

Vérifier

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

Dépanner

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

Informations connexes

Support et documentation techniques - Cisco Systems