Configurazione di Microsoft CA Server per la pubblicazione degli elenchi di revoche di certificati per ISE

Sommario

Introduzione Prerequisito Requisiti Componenti usati Configurazione Creare e configurare una cartella nella CA per contenere i file CRL Creare un sito in IIS per esporre il nuovo punto di distribuzione CRL Configurare Microsoft CA Server per la pubblicazione dei file CRL nel punto di distribuzione Verificare che il file CRL esista e sia accessibile tramite IIS Configurare ISE per l'utilizzo del nuovo punto di distribuzione CRL

Introduzione

In questo documento viene descritta la configurazione di un server Microsoft Certificate Authority (CA) che esegue Internet Information Services (IIS) per pubblicare gli aggiornamenti CRL (Certificate Revocation List). Viene inoltre illustrato come configurare Cisco Identity Services Engine (ISE) (versioni 3.0 e successive) per recuperare gli aggiornamenti da utilizzare per la convalida del certificato. È possibile configurare ISE in modo da recuperare i CRL per i vari certificati radice CA utilizzati nella convalida dei certificati.

Prerequisito

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Creare e configurare una cartella nella CA per contenere i file CRL

La prima operazione consiste nel configurare un percorso nel server CA in cui archiviare i file CRL. Per impostazione predefinita, il server CA Microsoft pubblica i file in C:\Windows\system32\CertSrv\CertEnroll\

Anziché utilizzare questa cartella di sistema, creare una nuova cartella per i file.

1. Sul server IIS, scegliere un percorso nel file system e creare una nuova cartella. In questo esempio viene creata la cartella C:\CRLDistribution.



2. Affinché la CA possa scrivere i file CRL nella nuova cartella, è necessario abilitare la condivisione. Fare clic con il pulsante destro del mouse sulla nuova cartella, scegliere **Proprietà**, fare clic sulla scheda **Condivisione** e quindi su **Condivisione avanzata**.

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

3. Per condividere la cartella, selezionare la casella di controllo **Condividi la cartella** e quindi aggiungere un simbolo di dollaro (\$) alla fine del nome della condivisione nel campo Nome condivisione per nascondere la condivisione.

Adv	anced Sharing
Γ	Settings
	CRLDistribution\$
	Add Remove
	Limit the number of simultaneous users to: 77216
	Permissions Caching
1.1	OK Cancel Apply

4. Fare clic su **Autorizzazioni** (1), su **Aggiungi** (2), su **Tipi di oggetto** (3) e selezionare la casella di controllo **Computer** (4).

Advanced Sharing	📔 Permissions for CRLDistributio	n\$	Selec	ct Users, Computers, Service Accounts, or Grou	ps ?X
Share this folder	Share Permissions		Sele	ect this object type:	
Coltings	Group or user names:		Us	ers, Groups, or Built-in security principals	3 Object Types
Share name:	& Everyone		From	m this location:	
CRLDistribution\$			rtpa	aaa.local	Locations
Add Remove			Ent	er the object names to select (<u>examples</u>):	
Limit the number of simultaneous us					Check Mamor
Comments:	Permissions for Everyone Full Control Change Read	Add F		Object types Select the types of objects you want to find. Object types:	
	Learn about access control and per	missions			
	ОК	Cancel	Apply		OK Cancel

5. Per tornare alla finestra Seleziona utenti, computer, account di servizio o gruppi, fare clic su **OK**. Nel campo Immettere i nomi degli oggetti da selezionare immettere il nome del computer del server CA nell'esempio seguente: WIN0231PNBS4IPH e fare clic su **Controlla nomi**. Se il nome immesso è valido, viene aggiornato e sottolineato. Fare clic su **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. Nel campo Utenti e gruppi scegliere il computer CA. Selezionare **Consenti** controllo completo per concedere l'accesso completo alla CA.

Fare clic su **OK**. Fare di nuovo clic su **OK** per chiudere la finestra Condivisione avanzata e tornare alla finestra Proprietà.

Permissions for CRLDistribution\$ >							
Share Permissions							
Group or user names:							
WIN-231PNBS4IPH (ABTO	MAR\WIN-231PNE	BS4IPH\$)					
	Add	Remove					
Permissions for WIN-231PNBS4IPH	Allow	Deny					
Full Control	$\mathbf{\nabla}$						
Read	\mathbf{N}						

7. Per consentire alla CA di scrivere i file CRL nella nuova cartella, configurare le autorizzazioni di sicurezza appropriate. Fare clic sulla scheda Protezione (1), su **Modifica** (2), su **Aggiungi** (3), su **Tipi di oggetto** (4) e selezionare la **casella di controllo Computer** (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 co
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. Nel campo Immettere i nomi degli oggetti da selezionare, immettere il nome computer del server CA e fare clic su **Controlla nomi**. Se il nome immesso è valido, viene aggiornato e sottolineato. Fare clic su **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:	object typee		
abtomar.local	Locations		
Enter the object names to select (examples):			
WIN-231PNBS4IPH	Check Names		
Advanced OK	Cancel .:		

9. Scegliere il computer CA nel campo Utenti e gruppi, quindi selezionare **Consenti** controllo completo per concedere l'accesso completo alla CA. Fare clic su **OK** e quindi su **Chiudi** per completare l'operazione.

Permissions for CRLDistribution					
Security					
Object name: C:\CRLDistribution	n				
Group or user names:					
SCREATOR OWNER					
Administratore (ABTOMAR\A)	dminietratore)				
Users (ABTOMAR\Users)	aministrators/				
WIN-231PNBS4IPH (ABTOM	AR\WIN-231PNB	S4IPH\$)			
	Add	Remove			
Permissions for WIN-231PNBS4IPH	Allow	Deny			
Full control		□ ^			
Modify					
Read & execute	\checkmark				
List folder contents	\checkmark				
Read					
OK	Cancel	Apply			

Creare un sito in IIS per esporre il nuovo punto di distribuzione CRL

Per consentire ad ISE di accedere ai file CRL, rendere accessibile tramite IIS la directory che contiene i file CRL.

- 1. Sulla barra delle applicazioni del server IIS fare clic su **Start**. Scegliere **Strumenti di amministrazione > Gestione Internet Information Services (IIS)**.
- 2. Nel riquadro di sinistra, noto come struttura della console, espandere il nome del server IIS e quindi **Siti.**



3. Fare clic con il pulsante destro del mouse su **Default Web Site** (Sito Web predefinito) e scegliere **Add Virtual Directory** (Aggiungi directory virtuale), come mostrato nell'immagine.

💐 Internet Information Services (IIS) Manager



4. Nel campo Alias, inserire un nome di sede per il punto di distribuzione CRL. Nell'esempio, viene immesso CRLD.

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	Can	cel

5. Fare clic sui puntini di sospensione (. . .) a destra del campo Percorso fisico e individuare la cartella creata nella sezione 1. Selezionare la cartella e fare clic su **OK**. Fare clic su **OK** per chiudere la finestra Aggiungi directory virtuale.

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

6. Il nome del sito immesso al passaggio 4 deve essere evidenziato nel riquadro di sinistra. In caso contrario, sceglietela ora. Nel riquadro centrale fare doppio clic su **Esplorazione directory**.



7. Nel riquadro destro, fare clic su Abilita per abilitare l'esplorazione delle directory.

Internet Information Services (IIS)	Manager	-		\times
← → 21 + WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +	1	a 🖂 🔂	0-
File View Help				
Connections	Ciractony Browsing	Alerts		
Internet Information Services (IIS) Internet Information Services (IIS) Internet Information Services (IIS) File View Help Connections Start Page Start Page Start Page Start Page Start Page Default Web Site Start Service Service CentSrv CentD CentSrv CentD	Directory browsing	Directory br directory br	owsing has h	been
VIN-231PNBS4IPH (ABTOMA	 Internet Information Services (IIS) Manager WIN-231PNBS4IPH → Sites → Default Web Site → CRLD → WIN-231PNBS4IPH → Sites → Default Web Site → CRLD → Directory Browsing Start Page WIN-231PNBS4IPH (ABTOMA	disabled.		
- 2 Application Pools				
V 🙆 Sites				
> 🐖 CertEnroll	C Extension	Enable		
> 💮 CetSrv	✓ Date	🕑 Help		
	Long date			

8. Nel riquadro sinistro, scegliere nuovamente il nome del sito. Nel riquadro centrale fare doppio clic su **Editor di configurazione**.



9. Nell'elenco a discesa Sezione, scegliere **system.webServer/security/requestFiltering**. Nell'elenco a discesa **allowDoubleEscaping** scegliere **True**. Nel riquadro di destra, fare clic su **Apply** (Applica), come mostrato nell'immagine.



La cartella deve essere accessibile tramite IIS.

Configurare Microsoft CA Server per la pubblicazione dei file CRL nel punto di distribuzione

Ora che è stata configurata una nuova cartella per ospitare i file CRL e che la cartella è stata esposta in IIS, configurare il server CA Microsoft per pubblicare i file CRL nel nuovo percorso.

- 1. Sulla barra delle applicazioni del server CA fare clic su **Start**. Scegliere **Strumenti di amministrazione > Autorità di certificazione**.
- Nel riquadro sinistro fare clic con il pulsante destro del mouse sul nome della CA. Scegliere Proprietà, quindi fare clic sulla scheda Estensioni. Per aggiungere un nuovo punto di distribuzione CRL, fare clic su Aggiungi.

abtomar-WIN-231PNB	S4IPH-CA Pro	perties		?	×	
Enrollment Agents	Auditing	Recov	ery Agents	Sec	unity	
General	Policy M	odule	Exi	t Module		
Extensions	Storage		Certificate I	Manager	s	
Select extension:						
CRL Distribution Point	t (CDP)				\sim	
Specify locations from (CRL).	which users ca	n obtain a (certificate rev	ocation I	ist	
C:\Windows\system3	2\CertSrv\Cert	Enroll\ <ca< td=""><td>Name><crln< td=""><td>Name Suf</td><td>fix><l< td=""></l<></td></crln<></td></ca<>	Name> <crln< td=""><td>Name Suf</td><td>fix><l< td=""></l<></td></crln<>	Name Suf	fix> <l< td=""></l<>	
Idap:///CN= <catrun< td=""><th>catedName><c< th=""><td>RLNameS</td><td>uffix>,CN=<s< td=""><td>erverSho</td><td>ntNar Delta</td></s<></td></c<></th></catrun<>	catedName> <c< th=""><td>RLNameS</td><td>uffix>,CN=<s< td=""><td>erverSho</td><td>ntNar Delta</td></s<></td></c<>	RLNameS	uffix>,CN= <s< td=""><td>erverSho</td><td>ntNar Delta</td></s<>	erverSho	ntNar Delta	
file:// <serverdnsna< td=""><th>me>/CertEnroll/</th><td><caname:< td=""><td><crlnames< td=""><td>Suffix><d< td=""><td>)eltaC</td></d<></td></crlnames<></td></caname:<></td></serverdnsna<>	me>/CertEnroll/	<caname:< td=""><td><crlnames< td=""><td>Suffix><d< td=""><td>)eltaC</td></d<></td></crlnames<></td></caname:<>	<crlnames< td=""><td>Suffix><d< td=""><td>)eltaC</td></d<></td></crlnames<>	Suffix> <d< td=""><td>)eltaC</td></d<>)eltaC	
<		_			>	
_		- 4	dd	Remov	/e	
Publish CRLs to this	s location					
Include in all CRLs when publishing ma	. Specifies wher anually.	re to publis	n in the Active	e Directo	ny	
Include in CRLs. Cl	lients use this to	find Delta	CRL location	s.		
Include in the CDP	extension of iss	sued certific	cates			
Publish Delta CRLs	Publish Delta CRLs to this location					
Include in the IDP	Include in the IDP extension of issued CRLs					
OK	Cano	xel	Apply	н	elp	

3. Nel campo Posizione, inserire il percorso della cartella creata e condivisa nella sezione 1.

Nell'esempio della sezione 1, il percorso è:

\\WIN-231PNBS4IPH\CRLDistribuzione\$

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. 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>а</td></crln<></caname></serverdnsname>	а
< 2	F
OK Cancel	

4. Con il campo Posizione compilato, scegliere **<CaName>** dall'elenco a discesa Variabile e fare clic su **Inserisci.**

Ad	d	Lo	cat	ion

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\CRLDi	stribution\$\ <cana< td=""><th>ame></th><td></td></cana<>	ame>	
Variable:			
<caname></caname>		~	Insert
Description of selected variable Used in URLs and paths	9:		
Inserts the DNS name of the s Example location: http:// <serv< td=""><td>erver verDNSName>/Ce</td><th>ertEnroll/<ca< th=""><td>Name><crlna< td=""></crlna<></td></ca<></th></serv<>	erver verDNSName>/Ce	ertEnroll/ <ca< th=""><td>Name><crlna< td=""></crlna<></td></ca<>	Name> <crlna< td=""></crlna<>
<			>
		ОК	Cancel

5. Dall'elenco a discesa Variabile, scegliere **<CRLNameSuffix>** e fare clic su **Inserisci**.

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. t j
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix></crlnamesuffix></caname>	
Variable:	
<crlnamesuffix> V Insert</crlnamesuffix>	
Description of selected variable:	
Used in URLs and paths for the CRL Distribution Points extension Appends a suffix to distinguish the CRL file name Example location: http:// <servername>/CertEnroll/<caname><crlnames< td=""><td>à,</td></crlnames<></caname></servername>	à,
< >	
OK Cancel	

6. Nel campo Posizione, aggiungere **.crl** alla fine del percorso. In questo esempio, il valore di Location è:

\\WIN-231PNBS4IPH\CRLDistribuzione\$\<NomeCa><SuffissoNomeCRL>.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.	i
Location: \\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix>.crl</crlnamesuffix></caname>	וו
Variable: <crlnamesuffix> V Insert Description of selected variable:</crlnamesuffix>] 1
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><crlnamesu< td=""><td></td></crlnamesu<></caname></servername>	
OK Cancel]

7. Fare clic su **OK** per tornare alla scheda Estensioni. Selezionare la casella di controllo **Pubblica CRL in questa posizione** e quindi fare clic su **OK** per chiudere la finestra Proprietà.

Verrà visualizzata una richiesta di autorizzazione per il riavvio di Servizi certificati Active Directory. Fare clic su **Sì**.

Enroliment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule E	t Module	
Extensions	Storage	Certificate	Managers	
Select extension:				
CRL Distribution Point	t (CDP)		~	
Specify locations from [CRL].	which users car	n obtain a certificate re	vocation list	
C:\Windows\system3 Idap:///CN= <catrun http://cServerDNSN</catrun 	32\C cate ame	ion Authority		
file:// <serverdnsna \\WIN-231PNBS4IP <</serverdnsna 		You must restart A take effect. Do you	ctive Directory Co want to restart t	ertificate Services for the changes to he service now?
file:// <serverdnsna WWIN-231PNBS4IP <</serverdnsna 	me>	You must restart A take effect. Do you	ctive Directory Co want to restart t	ertificate Services for the changes to he service now? Yes No

8. Nel riquadro sinistro fare clic con il pulsante destro del mouse su **Certificati revocati**. Scegliere **Tutte le attività > Pubblica**. Verificare che sia selezionato Nuovo CRL, quindi fare clic su **OK**.

.

🙀 certsrv - [Certification Autho	rity (Local)\abtoma	r-WIN	I-231PNBS4IPH-	CA\Revoked Certificates]
File Action View Help				
🗢 🔿 🖄 🔚 🖾				
Certification Authority (Local) Request ID	Rev	vocation Date	Effective Revocation Date
Payokad Cartificator			The	e are no items to show in this vi
Issued Certificates	All Tasks	>	Publish	
Pending Requests Failed Requests	View	>		
Certificate Templa	Refresh Export List			
	Properties			
	Help			



Il server CA Microsoft deve creare un nuovo file CRL nella cartella creata nella sezione 1. Se il nuovo file CRL viene creato correttamente, non verrà visualizzata alcuna finestra di dialogo dopo aver scelto OK. Se viene restituito un errore relativo alla nuova cartella del punto di distribuzione, ripetere attentamente ogni passaggio in questa sezione.

Verificare che il file CRL esista e sia accessibile tramite IIS

Verificare che i nuovi file CRL esistano e che siano accessibili tramite IIS da un'altra workstation prima di iniziare questa sezione.

 Sul server IIS, aprire la cartella creata nella sezione 1. Deve essere presente un singolo file con estensione crl con il formato <CANAME>.crl dove <CANAME> è il nome del server CA. In questo esempio, il nome del file è:

abtomar-WIN-231PNBS4IPH-CA.crl



2. Da una workstation in rete (preferibilmente sulla stessa rete del nodo Amministrazione primaria ISE), aprire un browser Web e selezionare http://<SERVER>/<CRLSITE> dove <SERVER> è il nome del server IIS configurato nella sezione 2 e <CRLSITE> è il nome del sito scelto per il punto di distribuzione nella sezione 2. In questo esempio, l'URL è:

Viene visualizzato l'indice della directory, che include il file osservato nel passaggio 1.



Configurare ISE per l'utilizzo del nuovo punto di distribuzione CRL

Prima di configurare ISE per il recupero del CRL, definire l'intervallo di pubblicazione del CRL. La strategia per determinare questo intervallo esula dall'ambito del presente documento. I valori potenziali (in Microsoft CA) sono compresi tra 1 ora e 411 anni. Il valore predefinito è 1 settimana. Una volta determinato l'intervallo appropriato per l'ambiente, impostare l'intervallo con queste istruzioni:

- 1. Sulla barra delle applicazioni del server CA fare clic su **Start**. Scegliere **Strumenti di amministrazione > Autorità di certificazione**.
- 2. Nel riquadro sinistro espandere la CA. Fare clic con il pulsante destro del mouse sulla cartella **Certificati revocati** e scegliere **Proprietà**.
- 3. Nei campi Intervallo pubblicazione CRL immettere il numero richiesto e scegliere il periodo di tempo. Fare clic su **OK** per chiudere la finestra e applicare la modifica. Nell'esempio è configurato un intervallo di pubblicazione di 7 giorni.

abtomar-WIN-231PNBS4IPH-I Revoked C Issued Cert Pending Re Failed Requ Refresh Export List Properties Help Revoked Certificate View Revoked Certificate Properties Help CRL Publishing Parameters View CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. CRL publication interval: 7 Days Next update: 1 Days Next update:	nertification Authority	≝ ■ / (Local)	Request ID	Revocation (
Issued Cert Pending Re Failed Requ Certificate Properties Help Revoked Certificates Properties ? × CRL Publishing Parameters Wew CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. CRL publication interval: ? Days Next update: 1 Days Next update:	✓ abtomar-WIN-231 ■ Revoked Ce	PNBS4IPH-		
Pending Ke Failed Requ Certificate Properties Help Help Revoked Certificates Properties ? X CRL Publishing Parameters View CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invald. CRL publication interval: Publication interval: Publication interval: Publication interval: Next update:	Ssued Cert	All Tasks	>	
Certificate Refresh Export List Properties Help Revoked Certificates Properties ? × CRL Publishing Parameters Wew CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. CRL publication interval: 7 Days Next update: 12/5/2020 10:39 AM Publish Detta CRLs Publication interval: 1 Days Next update:	Pending Re Failed Requ	View	>	
Properties Help Revoked Certificates Properties ? × CRL Publishing Parameters Yew CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. ? CRL publication interval: ? Publication interval: ? Publication interval: ? Next update: 12/5/2020 10.39 AM Publish Deta CRLs Publication interval: Next update: 1 Days Next update:	📋 Certificate	Refresh Export List		
Revoked Certificates Properties ? × CRL Publishing Parameters View CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. ? • CRL publication interval: ? • Next update: 12/5/2020 10:39 AM Publish Deta CRLs Publication interval: Next update: 1 Days Next update: 1		Properties		
Revoked Certificates Properties ? X CRL Publishing Parameters View CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. CRL publication interval: 7 Days Next update: 12/5/2020 10:39 AM Publish Delta CRLs Publication interval: 1 Days Next update:		Help		
Revoked Certificates Properties ? X CRL Publishing Parameters View CRLs A Certificate Revocation List (CRL) describes certificates that clients should consider invalid. CRL publication interval: 7 Days V Next update: 12/5/2020 10:39 AM Publish Delta CRLs Publication interval: 1 Days V Next update:		1101		
CRL publication interval: 7 Days Next update: 12/5/2020 10:39 AM Publish Deta CRLs Publication interval: 1 Days Next update:	Revoked Certificates Propertie	s	?	×
Next update: 12/5/2020 10:39 AM	Revoked Certificates Propertie CRL Publishing Parameters Vie A Certificate Revocation List (C consider invalid.	s sw CRLs CRL) describes ce	? tificates that clien	ts should
Publication interval: Next update:	Revoked Certificates Propertie CRL Publishing Parameters Vie A Certificate Revocation List (C consider invalid. CRL publication interval:	s sw CRLs CRL) describes ce 7 Day	? trificates that clien s ~	ts should
Publication interval: 1 Days	Revoked Certificates Propertie CRL Publishing Parameters Ve A Certificate Revocation List (C consider invalid. CRL publication interval: Next update:	s rw CRLs :RL) describes ce 7 Day 12/5/2020 10	? tificates that clien s ~ 39 AM	ts should
Next update:	Revoked Certificates Propertie CRL Publishing Parameters We A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Delta CRLs	s ew CRLs :RL) describes ce 7 Day 12/5/2020 10	? ntificates that clien s ~ 39 AM	ts should
	Revoked Certificates Propertie CRL Publishing Parameters Ve A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Delta CRLs Publication interval:	s sw CRLs CRL) describes ce 7 Day 12/5/2020 10	rtficates that clien s v :39 AM	ts should
	Revoked Certificates Propertie CRL Publishing Parameters Ve A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Detta CRLs Publication interval: Next update:	s sw CRLs CRL) describes ce 7 Day 12/5/2020 10	rtficates that clien s v :39 AM	ts should
	Revoked Certificates Propertie CRL Publishing Parameters Ve A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Detta CRLs Publication interval: Next update:	s ew CRLs :RL) describes ce 7 Day 12/5/2020 10	? tificates that clien 8 ~ 39 AM	ts should
	Revoked Certificates Propertie CRL Publishing Parameters We A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Delta CRLs Publication interval: Next update:	s ew CRLs :RL) describes ce 7 Day 12/5/2020 10	rtficates that clien s v :39 AM	x should
	Revoked Certificates Propertie CRL Publishing Parameters We A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Delta CRLs Publication interval: Next update:	s sw CRLs CRL) describes ce 7 Day 12/5/2020 10	rtficates that clien s v :39 AM	ts should
	Revoked Certificates Propertie CRL Publishing Parameters Ve A Certificate Revocation List (C consider invalid. CRL publication interval: Next update: Publish Delta CRLs Publication interval: Next update:	s ew CRLs :RL) describes ce 7 Day 12/5/2020 10	? tificates that clien s v :39 AM	x should

4. Immettere il comando **certutil -getreg CA\Clock*** per confermare il valore di ClockSkew. Il valore predefinito è 10 minuti.

Output di esempio:

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

5. Immettere il comando **certutil -getreg CA\CRLov*** per verificare se CRLOverlapPeriod è stato impostato manualmente. Per impostazione predefinita, il valore di CRLOverlapUnit è 0, che indica che non è stato impostato alcun valore manuale. Se il valore è diverso da 0, registrare il valore e le unità.

Output di esempio:

```
Values:

CRLOverlapPeriod REG_SZ = Hours

CRLOverlapUnits REG_DWORD = 0

CertUtil: -getreg command completed successfully.
```

6. Immettere il comando **certutil -getreg CA\CRLpe*** per verificare il periodo CRLP impostato nel passaggio 3.

Output di esempio:

Values: CRLPeriod REG_SZ = Days CRLUnits REG_DWORD = 7 CertUtil: -getreg command completed successfully. 7. Calcolare il periodo di tolleranza CRL nel modo seguente:

r. Se CRLOverlapPeriod è stato impostato nel passaggio 5: OVERLAP = CRLOverlapPeriod, in minuti:

Altrimenti: OVERLAP = (CRLPeriod / 10), in minuti

b. Se SOVRAPPONI > 720, SOVRAPPONI = 720

c. Se OVERLAP < (1.5 * ClockSkewMinutes), OVERLAP = (1.5 * ClockSkewMinutes)

d. Se OVERLAP > CRLPeriod, in minuti quindi OVERLAP = CRLPeriod in minuti

e. Periodo di tolleranza = OVERLAP + ClockSkewMinutes

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 II periodo di prova calcolato è il periodo di tempo che intercorre tra la pubblicazione da parte della

CA del CRL successivo e la scadenza del CRL corrente. ISE deve essere configurato in modo da recuperare i CRL di conseguenza.

8. Accedere al nodo ISE Primary Admin e scegliere Amministrazione > Sistema > Certificati. Nel

riquadro sinistro selezionare Certificato attendibile

Deployment Licensing Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
	Click h
Certificate Management Y Trusted Certificates	
Trusted Certificates // Edit + Import ① Export 1 Delete Q View	
OCSP Client Profile	
Certificate Signing Requests	iratio
Certificate Periodic Check Se	
CA_Root CA_ROO	
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 2 Enabled Cisco Services 01 Cisco Licensing Root Fri, 31 May 2013 Mon, 31 May 2038 2	

9. Selezionare la casella di controllo accanto al certificato CA per il quale si desidera configurare i CRL. Fare clic su **Modifica**.

10. Accanto alla parte inferiore della finestra, selezionare la casella di controllo Download CRL.

11. Nel campo URL distribuzione CRL, immettere il percorso del punto di distribuzione CRL, che include il file con estensione crl, creato nella sezione 2. In questo esempio, l'URL è:

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

12. L'ISE può essere configurato in modo da recuperare il CRL a intervalli regolari o in base alla scadenza (che in generale è anche un intervallo regolare). Se l'intervallo di pubblicazione del CRL è statico, gli aggiornamenti del CRL più tempestivi vengono ottenuti quando si utilizza l'ultima opzione. Fare clic sul pulsante di opzione **Automaticamente**.

13. Impostare il valore per il recupero su un valore inferiore al periodo di tolleranza calcolato nel passaggio 7. Se il valore impostato è più lungo del periodo di tolleranza, ISE controlla il punto di distribuzione del CRL prima che la CA abbia pubblicato il successivo CRL. In questo esempio, il periodo di tolleranza viene calcolato in 730 minuti, ovvero 12 ore e 10 minuti. Per il recupero verrà utilizzato un valore di 10 ore

14. Impostare l'intervallo tra i tentativi in base all'ambiente. Se ISE non è in grado di recuperare il CRL in base all'intervallo configurato nel passaggio precedente, verrà eseguito un nuovo tentativo a questo intervallo più breve.

15. Selezionare la casella di controllo **Ignora verifica CRL se CRL non è ricevuto** per consentire la normale esecuzione dell'autenticazione basata sui certificati (e senza il controllo CRL) se ISE non è stata in grado di recuperare il CRL per questa CA nell'ultimo tentativo di download. Se questa casella di controllo non è selezionata, tutte le autenticazioni basate su certificati emesse da questa CA avranno esito negativo se non è possibile recuperare il CRL.

16. Selezionare la casella di controllo **Ignora CRL non ancora valido o scaduto** per consentire ad ISE di utilizzare file CRL scaduti (o non ancora validi) come se fossero validi. Se questa casella di controllo non è selezionata, ISE considera un CRL non valido prima della data effettiva e dopo l'ora del successivo aggiornamento. Fare clic su **Save** per completare la configurazione.

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

Validate against OCSP Service	:e		~			
Reject the request if OC	SP returns UNKNO	WN status				
Reject the request if OC	SP Responder is u	inreachable				
Certificate Revocation List Configur	ation					
Download CRL						
CRL Distribution URL	http://win-231	pnbs4iph/crld/at	otomar-WIN-23	1PNBS4IPH-CA	crl	
	 Automatically 	10		Hours	~	before expiration.
Retrieve CRL	 Every 	1		Hours	~	
If download failed, wait	10		Minutes		✓ before retry.	
Enable Server Iden	tity Check 🕕					

Informazioni interne Cisco

1. Microsoft "Configurare un punto di distribuzione CRL per i certificati." <u>http://technet.microsoft.com/en-us/library/ee649260%28v=ws.10%29.aspx</u>, 7 ottobre 2009 [18 dic 2012]

2. Microsoft "Pubblicare manualmente l'elenco di revoche di certificati." http://technet.microsoft.com/en-us/library/cc778151%28v=ws.10%29.aspx, 21 gen 2005 [18 dic 2012]

3. Microsoft "Configurare i periodi di sovrapposizione CRL e Delta CRL." <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>, 11 apr 2011 [18 dic 2012]

4. MS2065 [MSFT]. "Modalità di calcolo di EffectiveDate (thisupdate), NextUpdate e NextCRLPublish." <u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-</u> <u>thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>, 4 giugno 2008 [18 dic 2012]