配置Microsoft CA伺服器以發佈ISE的證書吊銷清 單

目錄

簡介 必備條件 需求 採用元件 設定 在CA上建立並配置資料夾以容納CRL檔案 在IIS中建立網站以公開新的CRL分發點 配置Microsoft CA伺服器以將CRL檔案發佈到分發點 驗證CRL檔案存在且可通過IIS訪問 配置ISE以使用新的CRL分發點

簡介

本文檔介紹運行Internet Information Services(IIS)以發佈證書吊銷清單(CRL)更新的Microsoft證書頒 發機構(CA)伺服器的配置。還說明了如何配置思科身份服務引擎(ISE)(3.0及更高版本)以檢索更 新以用於證書驗證。可以將ISE配置為檢索它在證書驗證中使用的各種CA根證書的CRL。

必備條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

•思科身分識別服務引擎版本3.0

Microsoft Windows[®] Server[®] 2008 R2

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

設定

本節提供用於設定本文件中所述功能的資訊。

在CA上建立並配置資料夾以容納CRL檔案

第一項任務是配置CA伺服器上的一個位置以儲存CRL檔案。預設情況下,Microsoft CA伺服器將檔

案發佈到C:\Windows\system32\CertSrv\CertEnroll\

不要使用此系統資料夾,而是為檔案建立一個新資料夾。

1. 在IIS伺服器上,選擇檔案系統上的位置並建立新資料夾。在本示例中,建立資料夾 C:\CRLDistribution。



2.為了使CA將CRL檔案寫入新資料夾,必須啟用共用。按一下右鍵新資料夾,選擇**屬性**,按一下**共 用**頁籤,然後按一下**高級共用**。

CRLDistribution Properties	×
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	

3.若要共用資料夾,請選中**共用此資料夾**覈取方塊,然後在「共用名稱」欄位中的共用名稱末尾新 增一個美元符號(\$)以隱藏共用。

Settings Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216	Settings Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216	anced s	5haring this folder	2		
Share name: CRLDistribution\$ Add Remove: Limit the number of simultaneous users to: 77216 🛫	Share name: CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 Comments: Permissions Caching	Settings		ý.		
CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216 📑 Comments:	CRLDistribution\$ Add Remove Limit the number of simultaneous users to: 77216	Share	name:			
Add Remove Limit the number of simultaneous users to: 77216 📑	Add Remove Limit the number of simultaneous users to: 77216 Comments: Permissions Caching	CRLD	istribution\$			
Limit the number of simultaneous users to: 77216	Limit the number of simultaneous users to: 77216	A	dd Rer	move		
	Permissions Caching	Comm	ents:		 	

4.按一下**Permissions**(1),按一下**Add**(2),按一下**Object Types**(3),然後選中**Computers**覈取方塊 (4)。

Advanced Sharing	Permissions for CRLDistribution	1\$	Sela	ect Users, Computers, Service Accounts, or Groups	?×
☑ Share this folder	Share Permissions		Se	elect this object type:	
⊂ Settings	Group or user names:		U	Isers, Groups, or Built-in security principals	Object Types
Share name:	& Everyone		Fro	om this location:	
CRLDistribution\$			Itt	paaa.local	Locations
Add Remove			Er	nter the object names to select (<u>examples)</u> :	
Limit the number of simultaneous us				Object Types	? X
Comments:	2	Add	Remo	Select the types of objects you want to find.	
	Permissions for Everyone	Allow	Deny _	A Object types:	
	Full Control			: 🗹 🍇 Built-in security principals	
1 Permissions Caching	Change Read	N N	H	Service Accounts	
		-	-	Groups	
ОК С				Users	
	Learn about access control and perm	nissions			
	OK	Cancel	Apply		OK Cancel

5. 要返回「選擇使用者」、「電腦」、「服務帳戶」或「組」視窗,請按一下**確定**。在輸入要選擇 的對象名稱欄位中,在此示例中輸入CA伺服器的電腦名稱:WIN0231PNBS4IPH並按一下**Check** Names。如果輸入的名稱有效,該名稱將刷新並帶有下劃線。按一下「**OK**」(確定)。

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. 在「組或使用者名稱」欄位中,選擇CA電腦。選中**Allow** for Full Control以授予對CA的完全訪問 許可權。

按一下「OK」(確定)。再次按一下OK以關閉「高級共用」視窗並返回到「屬性」視窗。

Permissions for CRLDistribution\$				
Share Permissions				
Group or user names:				
WIN-231PNBS4IPH (ABTOM	IAR\WIN-231PNE	3S4IPH\$)		
	Add	Remove		
Permissions for WIN-231PNBS4IPH	Allow	Deny		
Full Control				
Read	\square			
OK	Cancel	Apply		

7.為了允許CA將CRL檔案寫入新資料夾,請配置相應的安全許可權。按一下Security頁籖(1),按一下Edit(2),按一下Add(3),按一下Object Types(4),然後選中Computers覈取方塊(5)。

🚺 CRLDistribution Properties.	Permissions for CRLDistribution
General Sharii <mark>1</mark> 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
Administrators (RTPAAA VAdministrators)	Administrators (H I PAAA Vadministrators)
To change permissions, click Edit. 2 Edit	
OWNER Allow Deny	3 Add Remove
Full control	Permissions for CREATOR OWNER Allow Deny
Modify Read & exercise	Full control
List folder contents	Modify
Read	Head & exec List folder co
Select Users, Computers, Service Accounts, or Groups	Select the types of objects you want to find.
Select this chiect ture:	ac Object types:
Users, Groups, or Built-in security principals	Object Types
From this location:	Service Accounts
rtpaaa.local	Locations
Enter the object names to select (examples)	Users
	Check Names
Advanced	Cancel OK Cancel

8.在「輸入要選擇的對象名稱」欄位中,輸入CA伺服器的電腦名稱,然後按一下**檢查名稱**。如果輸 入的名稱有效,該名稱將刷新並帶有下劃線。按一下「**OK**」(確定)。

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.在「組或使用者名稱」欄位中選擇CA電腦,然後選中Allow for Full control以授予對CA的完全訪問許可權。按一下OK,然後按一下Close以完成任務。

Permissions for CRLDistributi	on	×
Security		
Object name: C:\CRLDistribution	n	
Group or user names:		
SECREATOR OWNER		
SYSTEM		
Administrators (ABTOMAR\Ad	dministrators)	
Sers (ABTOMAR\Users)		
WIN-231PNBS4IPH (ABTOM	IAR\WIN-231PNB	S4IPH\$)
	Add	Remove
Permissions for		
WIN-231PNBS4IPH	Allow	Deny
Full control		
Modify	\square	
Read & execute	\checkmark	
List folder contents	\checkmark	
Read	\checkmark	
L		
ОК	Cancel	Apply

在IIS中建立網站以公開新的CRL分發點

為了讓ISE訪問CRL檔案,請通過IIS訪問包含CRL檔案的目錄。

- 1. 在IIS伺服器工作列上,按一下**開始**。選擇**管理工具> Internet資訊服務(IIS)管理器**。
- 2. 在左側窗格(稱為控制檯樹)中,展開IIS伺服器名稱,然後展開**站點。**



3.按一下右鍵**預設網站**,然後選擇**新增虛擬目錄**,如下圖所示。

💐 Internet Information Services (IIS) Manager



4.在「別名」欄位中,輸入CRL分發點的站點名稱。在此示例中,輸入了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	Cancel	

5.按一下省略號(。..)在「物理路徑」(Physical path)欄位的右側,瀏覽到在第1部分中建立的資料夾 。選擇該資料夾,然後按一下**確定**。按一下**OK**以關閉Add Virtual Directory視窗。

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

6.在步驟4中輸入的站點名稱必須在左窗格中突出顯示。如果沒有,現在就選擇。在中心窗格中,按兩下Directory Browsing。



7.在右窗格中,按一下**啟用**以啟用目錄瀏覽。

💐 Internet Information Services (IIS) i	Manager	– 🗆 X
← → 21 + WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +	🖬 🖂 🔂 😣 •
File View Help		
Connections	Directory Browsing Use this feature to specify the information that displays in a directory listing. Time	Alerts Directory browsing has been disabled. Actions Actions Actions
Getter Getter	Sube Extension Date Long date	Enable Enable Help

8.在左窗格中,再次選擇站點名稱。在中心窗格中,按兩下Configuration Editor。



9.在「部分」下拉選單中,選擇system.webServer/security/requestFiltering。在 allowDoubleEscaping下拉選單中,選擇True。在右窗格中,按一下Apply,如下圖所示。

Internet Information Services (IIS) 1	Manager	– 🗆 X
← → ² → WIN-231PNBS4IF	PH + Sites + Default Web Site + CRLD +	📅 🖂 🔂 - 🚱 -
File View Help		
Connections	Configuration Editor Section: system.webServer/security/requestFiltering From: Default Web Site/CRLD Web.config Deepest Path: MACHINE/WEBROOT/APPHOST allowDoubleEscaping True allowEbitCharacter	Actions Apply Cancel Generate Script Configuration Sauch Configuration
> 💭 CertEnroll > 🖓 CertEnroll > 🖓 CertSrv > 🏸 CRLD	alwaysAllowedQueryStrings False alwaysAllowedUrls (Count=0) denyQueryStringSequences (Count=0) denvUrlSequences (Count=0)	Section Lock Section 'allowDoubleEscaping'

現在必須通過IIS訪問該資料夾。

配置Microsoft CA伺服器以將CRL檔案發佈到分發點

現在,已配置了一個新資料夾來容納CRL檔案,並且該資料夾已在IIS中公開,請配置Microsoft CA伺服器以將CRL檔案發佈到新位置。

- 1. 在CA伺服器工作列上,按一下**開始**。選擇Administrative Tools > Certificate Authority。
- 2. 在左窗格中,按一下右鍵CA名稱。選擇**Properties**,然後按一下**Extensions**頁籤。要新增新的 CRL分發點,請按一下**Add**。

abtomar-WIN-231PNE	S4IPH-CA Pro	perties		?	\times
Enrollment Agents	Auditing Recovery Agents		Sec	urity	
General	Policy Mo	dule	Ð	Exit Module	
Extensions	Storage		Certificate	Manager	s
Select extension:					
CRL Distribution Poin	t (CDP)				\sim
Specify locations from (CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsna< td=""><td>which users car 2/CertSn/Cert catedName><c ame>/CertEnroll/</c </td><td>n obtain Enroll\<c RLName /<canam <canam< td=""><td>a certificate rev aName><crl Suffix>,CN=<s me><crlname ae><crlname< td=""><td>vocation li NameSuff ServerSho eSuffix><i Suffix><d< td=""><td>it Nar Delta eltaC</td></d<></i </td></crlname<></crlname </s </crl </td></canam<></canam </c </td></serverdnsna<></serverdnsna </catrun 	which users car 2/CertSn/Cert catedName> <c ame>/CertEnroll/</c 	n obtain Enroll\ <c RLName /<canam <canam< td=""><td>a certificate rev aName><crl Suffix>,CN=<s me><crlname ae><crlname< td=""><td>vocation li NameSuff ServerSho eSuffix><i Suffix><d< td=""><td>it Nar Delta eltaC</td></d<></i </td></crlname<></crlname </s </crl </td></canam<></canam </c 	a certificate rev aName> <crl Suffix>,CN=<s me><crlname ae><crlname< td=""><td>vocation li NameSuff ServerSho eSuffix><i Suffix><d< td=""><td>it Nar Delta eltaC</td></d<></i </td></crlname<></crlname </s </crl 	vocation li NameSuff ServerSho eSuffix> <i Suffix><d< td=""><td>it Nar Delta eltaC</td></d<></i 	it Nar Delta eltaC
<			_		>
Publish CRLs to th	is location		Add	Remov	e
Include in all CRLs when publishing m	. Specifies wher anually.	e to pub	lish in the Activ	e Directo	ry
Include in CRLs. C	lients use this to	find Del	ta CRL location	ns.	
Include in the CDP	extension of iss	ued cert	ificates		
Publish Delta CRL	s to this location				
Include in the IDP	extension of issu	ed CRL	S		
OK	Canc	el	Apply	He	elp

3.在「位置」欄位中,輸入在第1部分中建立和共用的資料夾的路徑。在第1部分的示例中,路徑為

\\WIN-231PNBS4IPH\CRL分配\$

:

Add Location >	<
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.	
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\	
Variable:	
Containes and insert	
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""><td></td></crlna<></caname></serverdnsname>	
< >	
OK Cancel	

4.填寫「位置」欄位後,從**「變數」**下拉選單中選擇<CaName>,然後按一下「插**入」。**

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\CRL	Distribution\$\ <cana< td=""><td>ame></td><td></td></cana<>	ame>	
Variable:			
<caname></caname>		~	Insert
Description of selected variab Used in URLs and paths Inserts the DNS name of the Example location: http:// <se< td=""><td>le: server rverDNSName>/Ce</td><td>ertEnroll/<ca< td=""><td>Name><crlna< td=""></crlna<></td></ca<></td></se<>	le: server rverDNSName>/Ce	ertEnroll/ <ca< td=""><td>Name><crlna< td=""></crlna<></td></ca<>	Name> <crlna< td=""></crlna<>
<			>
		OK	Cancel

5.從「變數」下拉選單中,選擇**<CRLNameSuffix>,**然後按一下**插入**。

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> VInsert</crlnamesuffix>]
Used in URLs and paths for the CRL Distribution Points extension Appends a suffix to distinguish the CRL file name Example location: http:// <servername>/CertEnroll/<caname><crlnames< td=""><td>à.</td></crlnames<></caname></servername>	à.
OK Cancel	

6.在「位置」欄位中,將.crl附加到路徑的末尾。在此示例中,位置為:

\\WIN-231PNBS4IPH\CRL分配\$\<CaName><CRLNameSuffix>.crl

Add Location >	<
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.	i
Location:	
\\WIN-231PNBS4IPH\CRLDistribution\$\ <caname><crlnamesuffix>.crl</crlnamesuffix></caname>	
Variable:	
<crlnamesuffix> V Insert</crlnamesuffix>	1
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><crlnamest< td=""><td></td></crlnamest<></caname></servername>	
< >	
OK Cancel	

7. 按一下OK返回到「擴展」頁籤。選中Publish CRLs to this location覈取方塊,然後按一下OK以 關閉「屬性」視窗。

出現一個提示符,提示獲得重新啟動Active Directory證書服務的許可權。按一下「Yes」。

Enrollment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule E	xit Module	
Extensions	Storage	Certificate	Managers	
Select extension:				
CRL Distribution Point	t (CDP)		~	
Specify locations from (CRL). C:\Windows\system3 Idao:///CN= <catrun< td=""><td>which users car</td><td>obtain a certificate re</td><td>vocation list</td><th></th></catrun<>	which users car	obtain a certificate re	vocation list	
http:// <serverdnsna< th=""><th>ame</th><th></th><th></th><th></th></serverdnsna<>	ame			
http:// <serverdnsna file://<serverdnsna WWIN-2311PNBS41P</serverdnsna </serverdnsna 	ame me>	You must restart A take effect. Do you	active Directory Ce u want to restart th	ertificate Services for the changes to ne service now?
http:// <serverdnsna file://<serverdnsna WWIN-231PNBS4IP</serverdnsna </serverdnsna 	ame me> HVC	You must restart A take effect. Do you	active Directory Ce u want to restart th	ertificate Services for the changes to the service now? Yes No

8.在左窗格中,按一下右鍵**Revoked Certificates**。選擇**所有任務>發佈**。確保選中「New CRL(新 建CRL)」 ,然後按一下**「OK(確定)」。**

.

a certsrv - [Certification Autho	ority (Local)\abtoma	r-WIN	V-231PNBS4IPH-	CA\Revoked Certificates]
File Action View Help				
🗢 🔿 🙍 🔚 🔯				
Certification Authority (Local	I) Request ID	Re	vocation Date	Effective Revocation Date
Revoked Certificator			The	re 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			



Microsoft CA伺服器必須在第1節中建立的資料夾中建立新的.crl檔案。如果成功建立了新的CRL檔 案,則按一下「確定」後將不會出現對話方塊。如果返回有關新分發點資料夾的錯誤,請仔細重複 本節中的步驟。

驗證CRL檔案存在且可通過IIS訪問

開始本節之前,請確認新的CRL檔案是否存在,以及是否可以通過另一工作站的IIS訪問這些檔案。

 在IIS伺服器上,開啟在第1部分中建立的資料夾。必須存在一個.crl檔案,格式為 <CANAME>.crl,其中<CANAME>是CA伺服器的名稱。在此範例中,檔案名稱為: abtomar-WIN-231PNBS4IPH-CA.crl

File Home St	istribution nare View		-		× ~ ?
← → ~ ↑ □,	This PC > Local Disk (C:) > CRLDistribution	ٽ ~	Search CRLDistrib	ution	P
 Quick access Desktop Downloads Documents Pictures System32 	Name i abtomar-WIN-231PNBS4IPH-CA web.config i	Date modified 11/28/2020 10:39 11/28/2020 10:22	Type Certificate Revoca CONFIG File	Size 1 K 1 K	В

2.從網路上的工作站(最好與ISE主管理節點位於同一網路),開啟Web瀏覽器並瀏覽到 http://<SERVER>/<CRLSITE>,其中<SERVER>是在第2部分中配置的IIS伺服器的伺服器名稱 ,<CRLSITE>是在第2部分中為分發點選擇的站點名稱。在此示例中,URL為:

http://win-231pnbs4iph/CRLD

將顯示目錄索引,其中包括步驟1中觀察到的檔案。



(=) C http://win-231pnbs4iph/crld/ D - C C win-231pnbs4iph - /crld/

win-231pnbs4iph - /crld/

[To Parent Directory]

11/28/2020 10:39 AM 11/28/2020 10:22 AM

979 abtomar-WIN-231PNBS4IPH-CA.crl 270 web.config

配置ISE以使用新的CRL分發點

在將ISE配置為檢索CRL之前,定義發佈CRL的時間間隔。確定此間隔的策略不在本檔案的範圍之 內。潛在值(在Microsoft CA中)為1小時到411年(含)。預設值為1週。確定適合您環境的間隔後 ,請使用以下說明設定間隔:

- 1. 在CA伺服器工作列上,按一下開始。選擇Administrative Tools > Certificate Authority。
- 2. 在左窗格中,展開CA。按一下右鍵Revoked Certificates資料夾,然後選擇Properties。
- 3. 在「CRL發佈間隔」欄位中,輸入所需的數字並選擇時間段。按一下OK關閉視窗並應用更改 。在本示例中,配置了7天的發佈間隔。

certsrv - [Certification Authority (Local)\abtomar-WIN-231PNBS

File Action View He	elp		
🗢 🄿 🖄 🔚 🙆 🖬			
 Certification Authority abtomar-WIN-231P Revoked Certification 	(Local) NBS4IPH-I	Request ID	Revocation [
Ssued Cert	All Tasks	>	
Pending Re Failed Regu	View	>	
Certificate	Refresh		
	Export Lis		
	Properties		
	Help		

Revoked Certificates Properti	? ×		
CRL Publishing Parameters	iew CRLs		
A Certificate Revocation List (consider invalid.	CRL) describes or	ertificates that clie	nts should
CRL publication interval:	7 Day	ys ∨	
Next update:	12/5/2020 1	0:39 AM	-
Publish Delta CRLs Publication interval: Next update:	1 Day	ys V	l
ок	Cancel	Apply	Help

4. 輸入certutil -getreg CA\Clock*命令以確認ClockSkew值。預設值為10分鐘。

輸出示例:

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

5.輸入**certutil -getreg CA\CRLov*命令**以驗證是否已手動設定CRLOverlapPeriod。預設情況下 ,CRLOverlapUnit值為0,表示未設定手動值。如果該值不是0,請記錄該值和單位。

輸出示例:

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

6. 輸入certutil -getreg CA\CRLpe*命令以驗證CRLeriod(已在步驟3中設定)。

輸出示例:

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

7.按以下方式計算CRL寬限期:

a.如果在步驟5中設定CRLOverlapPeriod:重疊= CRLOverlapPeriod(分鐘);

其他:重疊=(CRLeriod / 10),分鐘

b.如果重疊大於720,則重疊= 720

c.如果重疊<(1.5 * ClockSkewMinutes),則重疊=(1.5 * ClockSkewMinutes)

d.如果OVERLAP > CRLPeriod,則重疊= CRLPeriod,以分鐘為單位

e.寬限期=重疊+ 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 計算出的寬限期是CA發佈下一個CRL到當前CRL到期之間的時間量。需要配置ISE以相應地檢索 CRL。

8.登入到ISE主管理節點,然後選擇**管理>系統>證書**。在左窗格中,選擇 **受信任的證書**

■ Cisco ISE	Administration - System										
Deployment Licensing	Certificate	s Logging M	Maintenance	Upgrade	Health Checks	Backup & Resto	re Admin Acce	ess Settings			Click h
Certificate Management V System Certificates	Trus	ted Certific	ates								
Trusted Certificates	0 Edit	+ Import 🕁 Expo	t 👩 Delete	Q View							
OCSP Client Profile	0	Eriendly Name		A Status	Trusted For	Sarial Number	lesued To	leened By	Valid From	Expiration Date	Expiratio
Certificate Signing Requests	0	Priendly Name		~ otatus	Trusted For	Serial Humber	Issued to	Issued by	valid From	Expiration Date	Expiratio
Certificate Periodic Check Se		Baltimore CyberTrust Roo	e .	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust	Baltimore CyberTrust	Sat, 13 May 2000	Tue, 13 May 2025	2
Certificate Authority >		CA_Root		Enabled	Infrastructure Endpoints AdminAuth	4D 9B EE 97 53	abtomar-WIN-231PN	abtomar-WIN-231PN	Wed, 20 Feb 2019	Sun, 20 Feb 2039	
	0	Cisco ECC Root CA 2099		Enabled	Cisco Services	03	Cisco ECC Root CA	Cisco ECC Root CA	Thu, 4 Apr 2013	Mon, 7 Sep 2099	
		Cisco Licensing Root CA		Enabled	Cisco Services	01	Cisco Licensing Root _	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

9.選中要為其配置CRL的CA證書旁邊的覈取方塊。按一下「Edit」。

10.靠近視窗底部, 選中Download CRL覈取方塊。

11.在「CRL分發URL」欄位中,輸入CRL分發點的路徑,該分發點包括第2部分建立的.crl檔案。在 此示例中,URL為:

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

12. ISE可以配置為按固定間隔或基於過期時間(通常也是固定間隔)檢索CRL。 當CRL發佈間隔為 靜態時,使用後一個選項可獲得更及時的CRL更新。按一下Automatically單選按鈕。

13.將檢索的值設定為小於步驟7中計算的寬限期的值。如果值集大於寬限期,ISE將在CA發佈下一 個CRL之前檢查CRL分發點。在此示例中,寬限期計算為730分鐘或12小時10分鐘。檢索將使用 10小時的值

14.根據您的環境設定重試間隔。如果ISE無法按上一步中配置的間隔檢索CRL,它將按此較短間隔

重試。

15.選中**Bypass CRL Verification if CRL is not Received**覈取方塊,如果ISE在其上次下載嘗試中無 法檢索此CA的CRL,則允許基於證書的身份驗證正常進行(並且不進行CRL檢查)。如果未選中此 覈取方塊,則如果無法檢索CRL,則此CA頒發的證書的所有基於證書的身份驗證都將失敗。

16.選中**忽略CRL無效或過期覈取方塊,以允許ISE使用已過期(或無效)的CRL檔案,就像它們有** 效一樣。如果未選中此覈取方塊,則ISE會將CRL視為在其生效日期之前和下次更新時間之後無效 。按一下「Save」以完成設定。

Certificate Status Validation							
	To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first. OCSP Configuration Validate against OCSP Service Reject the request if OCSP returns UNKNOWN status Reject the request if OCSP Responder is unreachable Certificate Revocation List Configuration Ocentificate Revocation List Configuration Ocentificate Revocation List Configuration						
	CRL Distribution URL	http://win-23	1pnbs4iph/crld/abt	omar-WIN-231F	PNBS4IPH-CA.crl		
	Retrieve CRL	Automatically Every	1		Hours	~	before expiration.
	If download failed, wait	10		Minutes	~	before retry.	
	Enable Server Ide	ntity Check 🕕	Descined				
	bypass CRC Venn	cation if GRL is no	Received				
		not per valid or es					

Save

思科內部資訊

1.微軟。"為證書配置CRL分發點。" <u>http://technet.microsoft.com/en-</u> us/library/ee649260%28v=ws.10%29.aspx,2009年10月7日[2012年12月18日]

2.微軟。"手動發佈證書吊銷清單。" <u>http://technet.microsoft.com/en-</u> us/library/cc778151%28v=ws.10%29.aspx,2005年1月21日[2012年12月18日]

3.微軟。"配置CRL和增量CRL重疊週期。" <u>http://technet.microsoft.com/en-us/library/cc731104.aspx</u>,2011年4月11日[2012年12月18日]

4. MS2065 [MSFT]。「如何計算EffectiveDate(this isupdate)、NextUpdate和NextCRLPublish。 」<u>http://blogs.technet.com/b/pki/archive/2008/06/05/how-effectivedate-thisupdate-nextupdate-and-nextcrlpublish-are-calculated.aspx</u>,2008年6月4日[2012年12月18日]