配置Microsoft CA服务器以发布ISE的证书撤销列 表

目录
<u>简介</u>
前提条件
使用的组件
在CA上创建并配置文件夹以容纳CRL文件
<u>在IIS中创建站点以公开新的CRL分发点</u>
配置Microsoft CA服务器以将CRL文件发布到分发点
验证CRL文件存在且可通过IIS访问
<u>配置ISE以使用新的CRL分发点</u>
<u>验证</u>
<u>故障排除</u>

简介

本文档介绍运行Internet Information Services(IIS)以发布证书吊销列表(CRL)更新的Microsoft证书颁 发机构(CA)服务器的配置。它还说明如何配置思科身份服务引擎(ISE)(3.0版及更高版本)以检索 更新以用于证书验证。ISE可以配置为检索它在证书验证中使用的各种CA根证书的CRL。

前提条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 思科身份服务引擎版本3.0
- Microsoft Windows Server 2008 R2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

配置

本部分提供有关如何配置本文档所述功能的信息。

在CA上创建并配置文件夹以容纳CRL文件

第一项任务是配置CA服务器上的位置以存储CRL文件。默认情况下,Microsoft CA服务器将文件发 布到 C:\Windows\system32\CertSrv\CertEnroll\

请为这些文件创建一个新文件夹,而不是使用此系统文件夹。

1. 在IIS服务器上,选择文件系统上的位置并创建新文件夹。在本示例中,创建了 C:\CRLDistribution文件夹。

🏪 🛃 📙 🖛 Local Di	sk (C:)
File Home Shar	e View
← → ~ ↑ 🏪 > T	his PC > Local Disk (C:) >
	Name
🖈 Quick access	CRLDistribution
📃 Desktop 🛛 🖈	inetpub
👆 Downloads 🛛 🖈	PerfLogs
😭 Documents 🛛 🖈	Program Files
📰 Pictures 🛛 🖈	Program Files (x86)
System32	Users
This PC	Windows
📃 Desktop	

2. 要使CA将CRL文件写入新文件夹,必须启用共享。右键单击新文件夹,选择Properties并单击选 Sharing项卡,然后单击Advanced Sharing它。

CRLDistribution Properties	×
General Sharing Security Previous Versions Customize	
Network File and Folder Sharing	ř
CRLDistribution Not Shared	
Network Path: Not Shared	
Share	-10
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.	-8
Close Cancel Apply	1

3. 要共享文件夹,请选中此复选框,然后在"共享名称"字段中的共享名称末尾添加一个美元符号 (\$)以隐藏共享Share this folder。

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	100 000

4. 单Permissions击(1),单Add击(2),单Object Types击(3),然后选中Computers复选框(4)。

Advanced Sharing	Permissions for CRLDistributio	in\$	S	lect Users, Co	mputers, Service Accounts, or Gro	oups	? X
✓ Share this folder	Share Permissions			elect this object	type:	_	
- Settings	Group or user names:			Users, Groups, c	r Built-in security principals	3	Object Types
Share name:	& Everyone			From this location	6		
CRLDistribution\$				rtpaaa.local			Locations
Add Remove				Inter the object r	names to select (<u>examples</u>):		
Limit the number of simultaneous us				Object T	ibos		Check Names
Comments:	2	Add	Remo	Select th	e types of objects you want to find.		
	Permissions for Everyone	Allow	Deny	A Object ty	pes:		
	Full Control				Built-in security principals		
1 Permissions Caching	Change Bead				Service Accounts		
					Groups		
ок С					Users		
	Learn about access control and per	missions					
	ОК	Cancel	Apply			OK	Cancel

5. 要返回"选择用户"、"计算机"、"服务帐户"或"组"窗口,请单oK击。在Enter the object names to select(输入要选择的对象名称)字段中,输入CA服务器的计算机名称(本例中为 WIN0231PNBS4IPH),然后单Check Names击。如果输入的名称有效,该名称将刷新并显示下 划线。单击。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

在"组或用户名"字段中,选择CA计算机。检查AllowFull Control以授予对CA的完全访问权限。
 单击。ок再次ок单击以关闭"高级共享"窗口并返回到"属性"窗口。

Permissions for CRLDistrib	ution\$	>
Share Permissions		
Group or user names:		
Everyone WIN-231PNBS4IPH (ABT	omar\win-231Pne	BS4IPH\$)
	Add	Remove
Permissions for WIN-231PNBS4IPH	Allow	Deny
Full Control		
Change		
Read		
OK	Cancel	Apply

7. 要允许CA将CRL文件写入新文件夹,请配置相应的安全权限。单击Security(1)选项卡,单击 (Edit2),单击(Add3),单击Object Types(4),然后选中Computers复选框(5)。

[CRLDistribution Properties	Permissions for CRLDistribution	
General Sharii Security Previous Versions Customize	Security	
Object name: C:\CRLDistribution	Object name: C:\CRLDistribution	
Group or user names:	Sroup or user pames:	
CREATOR OWNER	CREATOR OWNER	
SYSTEM	SYSTEM	
Administrators (RTPAAA\Administrators)	Administrators (RTPAAA\Administrators)	
To change permissions, click Edit. 2 Edit		
Permissions for CREATUR OW/NER Allow Deny	3 Add Remove	
Full control	Permissions for CREATOR Allow Deny	
Modify	Full control	
Head & execute	Modify 🗖 🗖	
Bead	Read & exec	? ×
Write	List folder co	
Select Users, Computers, Service Accounts, or Groups	Select the types of objects you want to find.	
Select this object type:	ac Object types:	
Users, Groups, or Built-in security principals 4	Object Types	
From this location:		
rtpaaa.local	Locations	
Enter the object names to select (<u>examples</u>):	Users	
	Check Names	
Bovanced		2

8. 在"输入要选择的对象名称"字段中,输入CA服务器的计算机名称,然后单Check Names击。如果 输入的名称有效,该名称将刷新并显示下划线。单击。OK

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

9. 在Group or user names字段中选择CA计算机,然后选中AllowFull control以授予对CA的完全访问权限。单击OK,然后单击Close以完成任务。

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

在IIS中创建站点以公开新的CRL分发点

要使ISE访问CRL文件,请使包含CRL文件的目录可通过IIS访问。

1. 在IIS服务器任务栏上,单击Start。选择 。Administrative Tools > Internet Information Services (IIS) Manager

2. 在左侧窗格(称为控制台树)中,展开IIS服务器名称,然后展开Sites。



3. 右键单Default Web Site击并选Add Virtual Directory择,如下图所示。

💐 Internet Information Services (IIS) Manager



4. 在"别名"字段中,输入CRL分发点的站点名称。在本示例中,输入CRLD。

Add Virtual Dire	ectory			? ×
Site name: Path:	Default Web Site /			
Alias: CRLD Example: ima	ges			
Physical path: C:\CRLDistrib	ution			
Pass-through Connect as.	authentication Test Settings			
		ОК	0	Cancel

5. 单击省略号(...)在Physical path(物理路径)字段右侧并浏览到第1部分中创建的文件夹。选 择文件夹并单击ок。点击ок以关闭"添加虚拟目录"窗口。

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			
C	ж	Cancel	

6. 在步骤4中输入的站点名称必须在左窗格中突出显示。否则,请立即选择它。在中心窗格中 ,双击Directory Browsing。

Internet Information Services (IIS) N	Manager					
← → ² → WIN-231PNBS4IF	PH 🕨 Sites 🕨	Default Web	Site + CRLD	•		
File View Help						
Connections	CRI	LD Home	2			
VIII Start Page	Filter:		• 🦻 Go - 🖣	Show All	Group by:	
Application Pools Control Control Control Control Control Control Control Control Control Content Control Content Control Content Control Content Control Content Control Content Con	IIS ASP	Authentic	Compression	Default	Directory	Error Pages
> - 🔐 CertSrv > - 🔁 CRLD	Failed Request Tra	Handler Manpingr	HTTP	HTTP	Logging	MIME Types
	Modules	Output	Request			
	Managemen	Caching	Filtering	SSC Settings		^

7. 在右侧窗格中,Enable单击以启用目录浏览。

🖏 Internet Information Services (IIS) Manager –							
← → 🛃 • WIN-231PNB54I	PH + Sites + Default Web Site + CRLD +		10 8	6	0.		
File View Help							
Connections	Directory Browsing Use this feature to specify the information that displays in a directory listing. Time Size Extension Date Long date	Alerts Directory b disabled. Actions Actions Apply Cancel Enable Help		ng has b	een		

8. 在左侧窗格中,再次选择站点名称。在中心窗格中,双击Configuration Editor。



9. 在Section下拉列表中,选择system.webServer/security/requestFiltering。在下allowDoubleEscaping拉列表中 ,选择True。在右侧窗格中,点Apply击,如下图所示。

🐚 Internet Information Services (IIS)	Manager			- 🗆 X
← → Ø WIN-231PNB54	IPH + Sites + Default Web Site + CRLD	•		📅 🖂 🔂 😯
File View Help				
Connections	Configuration Editor Section: system.webServer/security/reques	IFiltering • From: Default Web Site/CRLD Web.config	-	Actions Apply X Cancel Generate Script Configuration Configuration
> - CertSnroll > - CertSnroll > - CertSrv > - CRLD	allownighnic haracters allwaysAllowedQueryStrings allwaysAllowedUrJs denyQueryStringSequences denyUrJSequences	False (Count=0) (Count=0)		Section Consignation Section Lock Section 'allowDoubleEscaping'

现在必须通过IIS访问该文件夹。

配置Microsoft CA服务器以将CRL文件发布到分发点

现在已配置新文件夹来容纳CRL文件,并且该文件夹已在IIS中公开,请将Microsoft CA服务器配置 为将CRL文件发布到新位置。

- 1. 在CA服务器任务栏上,单Start击。选择 。Administrative Tools > Certificate Authority
- 2. 在左窗格中,右键单击CA名称。选择Properties并点击该选项Extensions卡。要添加新的CRL分发 点,请点击Add。

		lerues					
Enrollment Agents	Auditing	Recover	y Agents	Sec	urity		
General	Policy Mor	Policy Module Exit					
Extensions	Storage	Storage Certificate					
Coloct outcosion:							
Select extension.	(000)						
CRL Distribution Point	t (CDP)				~		
Specify locations from	which users can	obtain a ce	ertificate rev	vocation li	st		
(CRL).							
C:\Windows\system3	2\CertSrv\CertE	nroll\ <cana< td=""><td>ame><crl< td=""><td>NameSuff</td><td>fix><</td></crl<></td></cana<>	ame> <crl< td=""><td>NameSuff</td><td>fix><</td></crl<>	NameSuff	fix><		
Idap:///CN= <catrun< td=""><td>catedName><cf< td=""><td>RLNameSuf</td><td>fix>,CN=<s< td=""><td>ServerSho</td><td>rtNa</td></s<></td></cf<></td></catrun<>	catedName> <cf< td=""><td>RLNameSuf</td><td>fix>,CN=<s< td=""><td>ServerSho</td><td>rtNa</td></s<></td></cf<>	RLNameSuf	fix>,CN= <s< td=""><td>ServerSho</td><td>rtNa</td></s<>	ServerSho	rtNa		
http:// <serverdnsna< td=""><td>ame>/CertEnroll/</td><td><caname></caname></td><td><crlname< td=""><td>eSuffix><l< td=""><td>Delta</td></l<></td></crlname<></td></serverdnsna<>	ame>/CertEnroll/	<caname></caname>	<crlname< td=""><td>eSuffix><l< td=""><td>Delta</td></l<></td></crlname<>	eSuffix> <l< td=""><td>Delta</td></l<>	Delta		
Tile:// <serverunsina< td=""><td>me >/Lenennii/c</td><td>I aName'r</td><td></td><td>SUMBORD</td><td></td></serverunsina<>	me >/Lenennii/c	I aName'r		SUMBORD			
		our fullior s					
<		our turner v	Contention to		>		
<					>		
<		Ad	d	Remov	> e		
 Publish CRLs to thi 	slocation	Ad	d	Remov	> e		
 Publish CRLs to thi Include in all CRLs 	s location	Ad to publish i	id	Remov	> e		
 Publish CRLs to thi Include in all CRLs when publishing matrix 	s location . Specifies where anually.	Ad to publish i	in the Activ	Remov re Directo	> re		
Publish CRLs to thi Include in all CRLs when publishing ma	s location . Specifies where anually.	Ad to publish i	in the Activ	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing ma Include in CRLs. Classes 	s location . Specifies where anually. lients use this to f	Ad to publish i ind Delta C	in the Activ	Remov re Directo	> re		
Publish CRLs to thi Include in all CRLs when publishing ma Include in CRLs. Cl Include in the CDP	s location . Specifies where anually. lients use this to f	Ad to publish i ind Delta C ied certifica	in the Activ RL location	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing main of the comparison of the comparis	s location . Specifies where anually. lients use this to f extension of issu	Ad to publish i ind Delta C ied certifica	in the Activ	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing mains Include in CRLs. Cl Include in the CDP Publish Delta CRLs Include in the IDP 	s location . Specifies where anually. lients use this to f extension of issues to this location extension of issue	Ad to publish i ind Delta C ied certifica	in the Activ	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing main include in CRLs. Clinclude in the CDP Include in the CDP Publish Delta CRLs Include in the IDP of the CDP 	s location . Specifies where anually. lients use this to f extension of issues to this location extension of issue	Ad to publish i ind Delta C ied certifica	in the Activ	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing mains Include in CRLs. Clinclude in the CDP Publish Delta CRLs Include in the IDP of the CDP 	s location . Specifies where anually. lients use this to f extension of issues to this location extension of issue	Ad to publish i ind Delta C ied certifica	d in the Activ RL location ites	Remov re Directo	> re		
 Publish CRLs to thi Include in all CRLs when publishing mains Include in CRLs. Clinclude in the CDP Publish Delta CRLs Include in the IDP of the	s location . Specifies where anually. lients use this to f extension of issues to this location extension of issue	Ad to publish i ind Delta C ied certifica	d in the Activ RL location ites	Remov re Directo	> re		

3. 在Location字段中,输入在第1部分创建和共享的文件夹的路径。在第1部分的示例中,路径为 :

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:	
\\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. 填写Location字段后,从 Variable下拉列表中选择,然后点击 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. 从变量(Variable)下拉列表中,选择并 单击"变量"Insert。

Add Location	\times
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> V Insert Description of selected variable:</crlnamesuffix>	
Used in URLs and paths for the CRL Distribution Points extension Appends a suffix to distinguish the CRL file name Example location: http:// <servername>/CertEnroll/<caname><crlname< td=""><td>SI</td></crlname<></caname></servername>	SI
< 2	>
OK Cancel	

6. 在Location字段中,.crl追加到路径末尾。在本示例中,位置为:

\\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><CRLNameSt OK

7. 点击OK以返回到Extensions(分机)选项卡。选中此复Publish CRLs to this location选框,然后单击 关OK闭"属性"窗口。

系统将显示一个提示符,询问是否有权重新启动Active Directory证书服务。单击。Yes

Х

Enrollment Agents	Auditing	Recovery Agents	Security	
General	Policy Mo	dule Ext	t Module	
Extensions	Storage	Certificate	Managers	
Select extension:				
CRL Distribution Point	(CDP)		~	
specify locations from '	terminent i segure de las		a a shi a sa bi sh	
(CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsnar \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\</serverdnsnar </serverdnsna </catrun 	2VC cate ame me>	ion Authority You must restart Ac take effect. Do you	tive Directory Ce want to restart th	rtificate Services for the changes to te service now?
(CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsnar file://<serverdnsnar NWIN-231PNBS4IPF < Publish CRLs to this</serverdnsnar </serverdnsnar </catrun 	2VC cate me MC	ion Authority You must restart Ac take effect. Do you	ocation list tive Directory Ce want to restart th	rtificate Services for the changes to te service now? Yes No

8. 在左窗格中,右键单Revoked Certificates击。选择 。All Tasks > Publish确保选中"New CRL(新建 CRL)",然后单OK击。

Certification Author	ity (Local)\abtoma	r-WI	V-231PNBS4IPH-	CA\Revoked Certificates]	
Certification Authority (Local)	Request ID	Re	vocation Date	Effective Revocation Date	t
Revoked Certifica****	All Tester		Dublish	reare no items to show in th	nis vi
Issued Certificates	All Tasks	1	Publish		
Pending Requests Failed Requests	View	>			
📔 Certificate Templa	Refresh Export List				
	Properties				
	Help				

Microsoft CA服务器必须在第1节中创建的文件夹中创建新的.crl文件。如果成功创建新的

CRL文件,则单击"确定"(OK)后将不会出现对话框。如果返回有关新分发点文件夹的错误,请 仔细重复本节中的步骤。

验证CRL文件存在且可通过IIS访问

在开始本部分之前,验证新的CRL文件是否存在,以及是否可以从其他工作站通过IIS访问这些文件 。

1. 在IIS服务器上,打开第1部分中创建的文件夹。必须存在一个.crl文件,其格

.crl 式 为CA服务器的名称。在本示例中,文件名是:

abtomar-WIN-231PNBS4IPH-CA.crl



 2. 从网络上的工作站(最好与ISE主管理节点位于同一网络中),打开Web浏览器,浏览到第 2部分中配置的IIS服务器的服务器名称http://

,以及第2部分中为分发点选择的站点名

。在本示例中,URL为:

/

http://win-231pnbs4iph/CRLD

系统随即会显示目录索引,其中包括在步骤1中观察到的文件。



配置ISE以使用新的CRL分发点

在将ISE配置为检索CRL之前,请定义发布CRL的时间间隔。确定此间隔的策略不在本文档的讨论 范围之内。潜在值(在Microsoft CA中)为1小时到411年(含)。默认值为1周。确定适合您环境的 间隔后,请使用以下说明设置间隔:

- 1. 在CA服务器任务栏上,单Start击。选择。Administrative Tools > Certificate Authority
- 2. 在左侧窗格中,展开CA。右键单击该文件Revoked Certificates夹并选择Properties它。
- 3. 在CRL发布间隔字段中,输入所需的编号并选择时间段。单击οκ关闭窗口并应用更改。在本 例中,配置七天的发布间隔。



4. 输入命certutil -getreg CA\Clock*令以确认ClockSkew值。默认值为10分钟。

示例输出:

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

5. 输入命certutil -getreg CA\CRLov*令以验证是否已手动设置CRLOverlapPeriod。默认情况下 ,CRLOverlapUnit值为0,表示未设置手动值。如果该值不是0,请记录该值和单位。 Values: CRLOverlapPeriod REG_SZ = Hours CRLOverlapUnits REG_DWORD = 0 CertUtil: -getreg command completed successfully.

6. 输入命certutil -getreg CA\CRLpe*令以验证在步骤3中设置的CRLPeriod。

示例输出:

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

7. 按如下方式计算CRL宽限期:

a.如果在第5步中设置CRLOverlapPeriod:OVERLAP = CRLOverlapPeriod,以分钟为单位 ;

否则:重叠=(CRLeriod / 10),以分钟为单位

b.如果重叠超过720,则重叠为720

c.如果重叠<(1.5 * ClockSkewMinutes),则重叠=(1.5 * ClockSkewMinutes)

d.如果OVERLAP > CRLPeriod,则重叠= CRLPeriod,以分钟为单位

e.宽限期=重叠+时滞Minutes

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

计算出的宽限期是CA发布下一个CRL到当前CRL到期之间的时间量。需要配置ISE以相应地检 索CRL。

8. 登录到ISE主管理节点并选择Administration > System > Certificates。在左侧窗格中,选择Trusted Certificate

E Cisco ISE	Administration · System										
Deployment Licensing	Certificate	s Logging	Maintenance	Upgrade	Health Checks	Backup & Restor	e Admin Acce	ss Settings			Click h
Certificate Management ~ System Certificates	Trus	ted Certif	icates								
Trusted Certificates	0 Edit	+ Import 🏠 🗈	ixport 👩 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		Baltimore CyberTrus	t 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	
		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	
	0	Cisco Licensing Roo	t CA	Enabled	Cisco Services	01	Cisco Licensing Root	Cisco Licensing Root	Fri, 31 May 2013	Mon, 31 May 2038	

- 9. 选中要为其配置CRL的CA证书旁边的复选框。单击。Edit
- 10. 在窗口底部附近,选中此Download CRL复选框。

0

11. 在CRL分发URL字段中,输入CRL分发点的路径,其中包括第2部分中创建的.crl文件。在本示 例中,URL为:

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

- 12. ISE可配置为按固定间隔或基于到期时间(通常也是固定间隔)检索CRL。当CRL发布间隔为 静态时,使用后一个选项可获得更及时的CRL更新。单击单Automatically选按钮。
- 13. 将检索值设置为小于在步骤7中计算的宽限期的值。如果值集大于宽限期,ISE会在CA发布下 一个CRL之前检查CRL分发点。在此示例中,宽限期计算为730分钟或12小时10分钟。检索将 使用10小时的值。
- 14. 根据您的环境设置重试间隔。如果ISE无法按上一步中配置的间隔检索CRL,它将按此较短间 隔重试。
- 15. 如果Bypass CRL Verification if CRL is not Received ISE在上次下载尝试时无法检索此CA的CRL,请选中 此复选框以允许基于证书的身份验证正常进行(并且不选中CRL检查)。如果未选中此复选框 ,则在无法检索CRL时,使用此CA颁发的证书的所有基于证书的身份验证都将失败。
- 16. 选中此Ignore that CRL is not yet valid or expired复选框可允许ISE使用已过期(或尚未有效)的CRL文件,就像它们有效一样。如果未选中此复选框,则ISE会将CRL视为在其生效日期之前和下次更新时间之后无效。点击Save以完成配置。

Certificate Status Validation						
To verify certificates, enable the OCSP Configuration	e methods below. If b	oth are enabled, C	CSP will always be	tried first.		
Validate against OCSP S Reject the request i Reject the request i	OCSP returns UNKNO OCSP Responder is t	DWN status unreachable	×			
Certificate Revocation List Cont	guration					
CRL Distribution UR	http://win-231	pnbs4iph/crld/a	btomar-WIN-23	1PNBS4IPH-CA.crl		
Retrieve CRL	 Automatically Every 	10		Hours	~	before expiration.
If download failed, v	ait 10		Minutes	~	before retry.	
 Enable Server Bypass CRL Ve 	dentity Check (i) rification if CRL is not	Received				
Signore that CRI	is not yet valid or ex	pired				

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。