# 通过CAPF在线CA配置自动证书注册和续订

### 目录

<u>简介</u> <u>先决条件</u>

<u>要求</u>

<u>使用的组件</u>

#### <u>背景信息</u>

<u>验证服务器时间和日期</u>

<u>更新服务器计算机名称</u>

### <u>配置</u>

AD服务、用户和证书模板 IIS身份验证和SSL绑定配置

### <u>CUCM 配置</u>

#### <u>验证</u>

<u>验证IIS证书</u>

<u>验证CUCM配置</u>

<u>相关链接</u>

## 简介

本文档介绍通过适用于Cisco Unified Communications Manager(CUCM)的证书授权代理功能 (CAPF)在线功能进行的自动证书注册和续订。

作者:Michael Mendoza,思科TAC工程师。

## 先决条件

### 要求

Cisco 建议您了解以下主题:

- Cisco Unified Communications Manager
- X.509证书
- Windows 服务器
- Windows Active Directory(AD)
- Windows Internet信息服务(IIS)
- NT(新技术)LAN管理器(NTLM)身份验证

### 使用的组件

本文档中的信息基于以下软件和硬件版本:

- CUCM 版本 12.5.1.10000-22
- Windows Server 2012 R2
- IP电话CP-8865/固件:SIP 12-1-1SR1-4和12-5-1SR2。

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。

## 背景信息

本文档介绍该功能的配置和相关资源,以供进一步研究之用。

### 验证服务器时间和日期

确保Windows服务器配置了正确的日期、时间和时区,因为它影响服务器的根CA(证书颁发机构 )证书及其颁发的证书的有效时间。

### 更新服务器计算机名称

默认情况下,服务器的计算机名具有随机名称,例如WIN-730K65R6BSK。启用AD域服务之前需要 做的第一件事是,确保在安装结束时将服务器的计算机名称更新为您希望服务器的主机名和根CA颁 发者名称的名称;否则,在安装AD服务后需要执行许多额外的步骤来更改此设置。

- 导航到本地服务器,选择计算机名称以打开系统属性
- 选择Change按钮并键入新的计算机名称:

Server M	lanager • l	Local Server		• @ I	r	Manage	Tools	View	Help
⊧ge Services ≯	Computer na Workgroup Windows Fi Remote ma Remote Der NIC Teamin Ethernet0 Coperating s Handware in	International Server's and Server's Se	Lest int Window	Computer can chan computer can LAB-OC-RTP Rail computer LAB-OC-RTP Member of O Doman Workp Workp	repuiter repetiter re reame: reame: reame: reame: reame: reame:	Name/Do	main Cr renbenho ess to nets	More d the of resource	
		OK Canosi Ap	sh	<b>€</b> v	Vin	dows	Serv	ver 2	012 F

• 重新启动服务器以应用更改

## 配置

AD服务、用户和证书模板

启用和配置Active Directory服务

 在服务器管理器中选择Add Roles and Features选项,选择Role-based or feature-based installation,然后从池中选择服务器(池中必须只有一个),然后选择Active Directory域服务

<u>.</u>	Add Roles and Features Wizard
Select serv	ver roles
Before You Beg Installation Typ Server Selectio	Select one or more roles to install on the selected server.      Roles     Description     Active Directory Certificate Services     Active Directory Domain Services
Features Confirmation Results	Active Directory Federation Services       Add Roles and Features Wizard         Active Directory Federation Services       Active Directory Sights Management Services         Active Directory Rights Management Services       Add features that are required for Active Directory Domain Services (Poince Server)         DHCP Server       DHCP Server         DHS Server       Fax Server         Fax Server       (Tooth) Group Policy Management         Hyper-V       Active Directory and Access Services         Network Policy and Access Services       AD DS and AD UDS Tools         Remote Desktop Services       (Tooth) Active Directory Administrative Center         Bernote Desktop Services       Fools Active Directory and Command-Line Tools
	EPReviou           BPA results         Previou           BPA results         Previou           BPA results         Previou           BPA results         Previou           Add Features         Cancel

- 继续选择下一步按钮,然后选择安装
- 安装完成后,选择Close按钮
- Server Manager > AD DS下将出现一个警告选项卡,标题为Active Directory域服务所需的配置;选择more链接,然后选择可用操作以启动安装向导:

€ Server M	anager • AD DS 🛛 • 🎯 I 🍢	Manage Tools View Help	
Dashboard     Local Server     Al Servers     Al DIS	SURVERS       Al servers   1 total       A Configuration required for Active Directory Domain Services at WN-730485       Filter       P       (8) •		
III File and Storage Services ≥	and All Servers	Task Details	
	All Servers Task Details and Notification	ns	
	Flav P (8 * (8 *		$\odot$
	C Status Task Name Stage Message	Action	N
	Post-deployment Configuration Not Sta Configuration re-	pired for Active Directory Do <u>Expendic Bi</u>	is server to a domain-

• 按照域设置向导中的提示,使用所需的根域名添加新的林(本实验使用michamen.com),并在可 用时取消选中DNS框,定义DSRM密码(本实验使用C1sc0123!):

) – – – – – – – – – – – – – – – – – – –	Active Directory Domain Services Configuration	Wizard - C X	
Deployment Conf	iguration	TARGET SERVER	
Deployment Configuration Domain Controller Options DNS Options	Select the deployment operation O Add a domain controller to an existing domain O Add a new domain to an existing forest		
Additional Options	Add a new forest		
	Specify the domain information for this operation Root domain name: michamen.com	3	

<b>L</b> .	Active Directory Domain Services (	Configuration Wizard	_	D X
Domain Controlle Deployment Configuration	er Options Select functional level of the new forest	and root domain	TARG LAB-DC-RTRmin	ET SERVER
Additional Options	Forest functional level:	Windows Server 2012 R2	-	
Paths Review Options	Coards domain controller canabilitier	windows server 2012 K2	•	
Prerequisites Check	Domain Name System (DNS) server			
	Global Catalog (GC) Read only domain controller (RODC)			
	Type the Directory Services Restore Mod	le (DSRM) password		
	Passwordt	•••••		
	Confirm password:	•••••		

- 需要指定NetBIOS域名(本实验中使用了MICHAMEN1)。
- 按照向导完成操作。然后,服务器重新启动以完成安装。
- 下次登录时需要指定新域名。 例如MICHAMEN1\Administrator。

€ Server I	Manager + AD DS	· @ I
Dashboard     Local Server     All Servers	SERVERS       All servers   1 total       Filter         Image: Contract of the servers in total	
AD DS	Server Name IPv4 Address Manageability	Last Update
File and Storage Services	LA8-DC-RTP 14.48.31.153 Online - Performance counters not started	2/26/2019 4/20:10 PM

### 启用和配置证书服务

- 在服务器管理器中,选择Add Roles and Features
- 选择Active Directory证书服务(Active Directory Certificate Services), 然后按照提示添加所需 功能(所有可用功能均是从为此实验启用的角色服务中选择的)
- 对于角色服务,请检查证书颁发机构Web注册

<b>b</b>	Add Roles and Features Wizard	_ 0 X
Select role service	S	DISTINATION SERVER LAB-DC-RTP.michamen.com
Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation Results	Select the role services to install for Active Directory Certificat Role services   Certification Authority  Certificate Enrollment Policy Web Service  Certificate Enrollment Web Service  Certificate Enrollment Web Enrollment  Network Device Enrollment Service  Online Responder	e Services Description Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
Ł	Add Roles and Features Wizard	_ <b>0</b> X
Select role service Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Web Server Role (IIS) Role Services Confirmation Results	S Select the role services to install for Web Server (IIS) Role services	Description Description Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.

< Previous Next >

Install

Cancel

"服务器管理器"(Server Manager)>"AD DS"下必须出现一个警告选项卡,标题为"Active Directory证书服务所需的配置"(Configuration required for Active Directory Certificate Services);选择more链接,然后选择可用的操作:

€ • Server M	anager + AD CS			@   🍢 🏎	Task Vew Help	
Deshtoard     Local Server     Al Server     Ad Server     Ad Co	SERVERS All servers   1 total Configuration required for Filter	Anive Directory Certificate Series	on at U-8-02-879		tais • Minto •	•
₩ A0.05	Seventiane Del Addres	Manageability	Last Update	Windows-Activation		
RE File and Storage Services P	DERICHTP SUBJECTS (	Online - Performance counters no	CAMER 205/2019 42100	PM Not activated		
to o		6		All Servers Task Det	ala	-
		All Servers Task	Details and No	tifications		
	and with	Filter	ρ () •	® •		
	All-events (2 total	Status Task Name	Steps M	naye	Action	Notice
	film	🛕 Post-deployment Co	refiguation Notifia. Co	eligention required for Active D	incloy Co <u>Configuratio</u>	See Directory Gerli-

- 在AD-CS安装后配置向导中,浏览以下步骤:
- 选择证书颁发机构和证书颁发机构Web注册角色
- 选择Enterprise CA with options:
- 根 CA
- 创建新的私钥
- 使用私钥 SHA1的默认设置
- 设置CA的公用名(必须与服务器的主机名匹配):

2	AD CS Configuration	_ <b>D</b> X
CA Name	U	DESTINATION SERVER A8-DC-RTRmichamen.com
Credentials Role Services	Specify the name of the CA	
Setup Type CA Type	Type a common name to identify this certification authority (CA). This na certificates issued by the CA. Distinguished name suffix values are autom be modified.	ame is added to all natically generated but can
Private Key	Common name for this CA:	
CA Name	LA8-DC-RTP	
Validity Period	Distinguished name suffic	
Certificate Database	DC=michamen,DC=com	
Confirmation	Preview of distinguished name:	
Progress Results	CN=LA8-DC-RTP,DC=michamen,DC=com	

• 将有效期设置为5年(如果需要,还可以设置更多)

• 通过向导的其余部分选择Next按钮

为CiscoRA创建证书模板

- 打开MMC选择Windows开始徽标,然后在"运行"中键入mmc
- 打开MMC窗口并添加以下管理单元(用于配置的不同点),然后选择确定:

	File	Action	View	Favorites	Window	Help
٠		New			0	trl+N
		Open Save			c c	trl+O trl+S
4		Save As				
		Add/Rem Options	ove Sna	ip-in	Ct	d+M

sp-in	Vendor	$\sim$		Console R	oot			Edit Extensions
Active Directory Do	Microsoft Cor			Active	Directory	Domains a	and True	
Active Directory Site	Microsoft Cor			🔤 Active	Directory	Users and	Comps	Remove
Active Directory Use	Microsoft Cor	-		Certifi	ation Aut	hority (Lo	cal)	
ActiveX Control	Microsoft Cor			Certifi	ate Temp	kates (LAB	HOC.mic	Move Up
ADSI Edit	Microsoft Cor			Intern	et Inform	ation Servi	ces (IIS	
Authorization Manager	Microsoft Cor							Move Down
Certificate Templates	Microsoft Cor		Add >					
Certificates	Microsoft Cor							
Certification Authority	Microsoft Cor							
Component Services	Microsoft Cor							
Computer Managem	Microsoft Cor							
Device Manager	Microsoft Cor							
Disk Management	Microsoft and							
016	Microsoft Cor	Y		<			>	Advanced
DNS	Microsoft Cor	Y		<		-	<u>&gt;</u>	Advanced

- 选择File > Save,并将此控制台会话保存到桌面以便快速重新访问
- 从管理单元中,选择证书模板
- 创建或克隆模板(最好是"根证书颁发机构"模板,并将其命名为CiscoRA

🚡 Co	nsole1 - [Console Root\Certificate T	emplates (LAB-DC-
🚡 File Action View Favorites Window Help		
Console Root  Active Directory Domains and Trusts  Active Directory Users and Computers  Certification Authority (Local)  Certificate Templates LA8-DC-RTP.michamen.com)  Thermet Information Services (IIS) Manager	Template Display Name Administrator Authenticated Session Basic EFS CA Exchan CEP Encryp Code Signi Reenroll All Certific	Schema Version 1 1 1 2 e cate Holders

- 修改模板。右键单击它并选择"属性"
- 选择General选项卡,将有效期设置为20年(如果需要,也可以设置其他值)。在此选项卡中 ,确保模板的"显示名称"和"名称"值匹配

	CiscoRA Prope	rties	? X
Subject Name	ls	suance Require	ments
Superseded Templates	Extensions	Security	Server
General Compatibility	Request Handling	Cryptography	Key Attestation
Template display name:			
CiscoRA			
Template name: CiscoRA Validity period:	Renewal (	period: tays ∨	
Publish certificate in Do not automatic Directory	Active Directory ally reenroll if a duplic	ate certificate ex	ásts in Active
OK	Cancel	Apply	Help

• 选择Extensions选项卡,突出显示Application Policies,然后选择Edit



- 删除出现的窗口中显示的所有策略
- 选择Subject Name选项卡,然后选择Supply in Request单选按钮
- 选择Security选项卡并授予显示的所有组/用户名的所有权限

CiscoRA Prop	erties	? X
General Compatibility Request Handling Subject Name	Cryptography Key Issuance Requirement	Attestation ts
Superseded Templates Extensions	Security	Server
Group or user names:		
& Authenticated Users		
Administrator Domain Admins (MICHAMEN1\Domain Enterprise Admins (MICHAMEN1\Enter	Admins) prise Admins)	
Permissions for Authenticated Users	Add Re Allow	move Deny
Full Control	<b>V</b>	
Read	✓	
Write		
Enrol		
Autoenroll For special permissions or advanced settings Advanced.	s, click Adva	nced
OK Cancel	Apply	Help

使证书模板可供颁发

- 在MMC管理单元中,选择证书颁发机构并展开文件夹树以查找"证书模板"(Certificate Templates)文件夹
- 在包含"名称"和"目标用途"的框架中的空白处右键单击
- 选择New和Certificate Template to Issue
- 选择新创建和编辑的CiscoRA模板



### Active Directory CiscoRA帐户创建

- 导航到MMC管理单元并选择Active Directory用户和计算机
- 在最左窗格中的树中选择Users文件夹
- 在包含"名称"、"类型"和"说明"的框架中的空白处右键单击
- 选择New和User
- 使用用户名/密码(ciscora/Cisco123用于本实验)创建CiscoRA帐户,并在显示密码时选中 Password never expires复选框



### IIS 身份验证和SSL绑定配置

enable NTLM 身份验证

- 导航到MMC管理单元,然后在"Internet信息服务(IIS)管理器"管理单元下选择服务器名称
- 功能列表将显示在下一帧中。双击Authentication功能图标



• 突出显示Windows Authentication,然后从Actions帧(右窗格)中选择Enable选项

E C S LAB-DC-RTP +				
Connections  O,	Authentication Group by: No Grouping •			Actions Enable Help
Application Pools	Name Anonymous Authentication ASP.NET Impersonation Windows Authentication	Status Enabled Disabled	Response Type	
	windows Authentication	Disabled	HTTP: 401 Challenge	

• 操作窗格显示高级设置选项;选择该选项,并取消选中启用内核模式身份验证

E AB-DC-RTP				<b>₩</b> = \$ 0
Connections	Authentication Group by: No Grouping •			Alerts Alerts Click here to learn how to configure Extended Protection.
Application Pools     Joan Stes	Name Anonymous Authentication ASP_NET Impersonation Windows Authentication	Status Enabled Disabled Enabled	Response Type HTTP 401 Challenge	Actions Disable Advanced Settings Providers
	Ad Extended Protection: Off v Click here for more information onl Enable Kernel-mode authentical By default, IS enables kernel-mode authentication performance and p	ins ion e authentication, w	hich may improve	<table-cell> Holp</table-cell>

• 选择Providers并按NTML顺序排列,然后选择Negotiate。

Connections	Antheodoral and			Alerts
<b>0,-</b> 🗟   🖄 😣	Authentication			Click here to learn how
Start Page	Group by: No Grouping .			Configure Extended Protection.
Application Pools	Name *	Status	Response Type	Artista
p-🙀 Stes	Anonymous Authentication ASP.NET Impersonation	Enabled Disabled		Disable
	Windows Authentication	Enabled	HTTP 401 Challenge	Advanced Settings
		houldare	7 X	Providers
	Enabled Providers: Negotiate Negotiate Kerberos Select a provider from the list o to add it to the enabled provide Available Providers:	f available provide trs.	Move Up Move Down Remove	

生成Web服务器的身份证书

如果尚未出现这种情况,您需要为Web服务生成证书和身份证书,该证书由CA签名,因为如果 Web服务器的证书是自签名,则CiscoRA无法连接到该证书:

• 从IIS管理单元选择Web服务器,然后双击Server Certificates功能图标:



 默认情况下,您可以看到此处列出的一个证书;即自签名的根CA证书;从操作菜单中选择创 建域证书选项。在配置向导中输入值,以创建新证书。确保公用名是可解析的FQDN(完全限 定域名),然后选择下一步:

C C 1 + LALICATE					<b>₩</b> ≈ S <b>₩</b> -
Connections Q + Li   (1)   (0), - R) Start Pape - R) LAB-CO-RP (MCO-MAR)/r - R) LAB-CO-RP (MCO-MAR)/r	Server Certi Use this fasture to request	ficates and manage cotificates that the W	eb server can use with websites cor a flur. No Grouning .	eligueed for 552	Actions Import Could Conflicate Report Complete Conflicate Report
A Stes A Default Web Ste	Name *	Insued To LAB-DC-RTP	LAB-DC-87P	Expiration Date 2/26/2504 4:34:42	Create Domain Certificate Create Self-Signed Certificate
s 🕐 CetSiv		Create Certif	icate	7 2	Enable Automatic Rabind of Renewed Certificate
	Specify the required information of the required information of the required information of the provided informati	Name Properties tion for the cettificate. State/provin- rot contain ablensiations.	e and City/locality must be specifi	ed m	
	Common name Organization	UAB-DC-IS-michamen.com Cisco			
	City/locality Statulorovice	RTP RTP	]		
< =	Country/region	VS VS	, ,		

• 选择您的根CA的证书作为颁发者,然后选择Finish:

Create Certificate	?	X
Online Certification Authority		
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember. Specify Online Certification Authority: LAB-DC-RTP\LAB-DC-RTP.michamen.com Select Example: CertificateAuthorityName\ServerName Friendly name: Web Cert issued by LAB-DC-RTP		
Previous Next Finish C	ancel	

• 您可以看到列出的CA证书和Web服务器的身份证书:



Web服务器SSL绑定

 在树视图中选择一个站点(您可以使用默认网站或使其更精细到特定站点),然后从"操作"窗 格中选择绑定。此时将显示绑定编辑器,通过该编辑器可以创建、编辑和删除网站的绑定。选 择Add以将新的SSL绑定添加到站点。



• 新绑定的默认设置为端口80上的HTTP。在类型下拉列表中选择https。从SSL Certificate下拉列表中选择在上一节中创建的自签名证书,然后选择OK。

			Site	Bindings	? ×
Type http	Host Name	Port 80	IP Address	Binding Informa	Add Edit
			Add Site Bi	nding	? X emove
Ho	ps v st name: Require Server Nar	All Unass	igned m	v 443	
SSL We	. certificate: tb Cert issued by L	AB-DC-RTP		✓ Select Vie	W Close
No Ma LAI	t selected b Cert issued by L/ B-DC-RTP	AB-DC-RTP	p.	ок са	ancel

• 现在,您的站点上有新的SSL绑定,剩下的就是从菜单中选择Browse \*:443(https)选项验证该 绑定是否有效,并确保默认IIS网页使用HTTPS:

			Site	Bindings	? X
Type http https	Host Name	Port 80 443	IP Address	Binding Informa	Add Edit Berove
					Glose



证书也是不错的主意,因为需要为终端启用(或将要启用)安全信令加密;如果集群处于混合 模式,则可能需要此证书。

- 导航到System > Service Parameters。在"服务器"字段中选择Unified CM发布服务器,在"服务"字段中选择思科证书颁发机构代理功能
- 将Certificate Issuer to Endpoint的值设置为Online CA,并为Online CA Parameters字段输入 值。确保使用Web服务器的FQDN、之前创建的证书模板的名称(CiscoRA)、作为Microsoft CA的CA类型以及使用之前创建的CiscoRA用户帐户的凭据

Service Parameter Configuration	
Save 🧬 Set to Default	
Select Server and Service	
Server* cucm125pubCUCM Voice/Video (Active)	
Service* Cisco Certificate Authority Proxy Function (Active)	
All parameters apply only to the current server except parameters that are in the clust	ter-wide group(s).
Cisco Certificate Authority Proxy Function (Active) Parameters on server cu	cm125pubCUCM Voice/Video (Active)
Parameter Name P Contificate Issues to Endpoint *	Parameter Value
	Online CA
Duration Of Certificate Validity (in days)	1825
Key Size * 1	024
Maximum Allowable Time For Key Generation *	30
Maximum Allowable Attempts for Key Generation *	3
_ Online CA Parameters	
Online CA Hostname	lab-dc-iis.michamen.com
Online CA Port	443
Online CA Template	CiscoRA
Online CA Type *	Microsoft CA 🗸 🗸
Online CA Username	•••••
Online CA Password	•••••

 弹出窗口通知您需要重新启动CAPF服务。但首先,通过Cisco Unified Serviceability > Tools
 > Service Activation激活思科证书注册服务,在Server字段中选择Publisher并选中Cisco Certificate Enrollment Service复选框,然后选择Save按钮:

Security Services		
	Service Name	Activation Status
2	Cisco Certificate Authority Proxy Function	Activated
	Cisco Certificate Envolment Service	Deactivated
R	Cisco CTL Provider	Activated

## 验证

### 验证IIS证书

• 从连接到服务器的PC的Web浏览器(最好与CUCM发布服务器位于同一网络)导航至URL:

https://YOUR\_SERVER\_FQDN/certsrv/

• 显示证书不受信任警报。添加例外并检查证书。确保它与预期的FQDN匹配:



• 接受例外后,您需要进行身份验证;此时,您需要使用之前为CiscoRA帐户配置的凭证:

Authenticatio	n Required X
(?) User Name:	https://lab-dc-iis.michamen.com is requesting your username and password.
Password:	••••••

lab-dc-iis.michamen.com uses an invalid security certificate.

• 身份验证后,您必须能够看到AD CS(Active Directory证书服务)欢迎页面:

#### Microsoft Active Directory Certificate Services - LAB-DC-RTP

#### Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can ver with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security ta

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CI request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

#### Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

### 验证CUCM配置

执行通常要遵循的步骤,以便在其中一台电话上安装LSC证书。

步骤1:打开CallManager Administration页面,依次打开Device和Phone

- 第二步:选择Find按钮以显示电话
- 第三步:选择要安装LSC的电话
- 第四步:向下滚动至证书颁发机构代理功能(CAPF)信息
- 第五步:从Certificate Operation中选择Install/Upgrade。
- 第六步:选择Authentication Mode。(通过Null字符串可用于测试目的)

步骤 7.滚动到页面顶部,然后为电话选择save,然后选择Apply Config。

步骤 8电话重新启动并重新注册后,使用LSC状态过滤器确认已成功安装LSC。

- 从AD服务器侧打开MMC并展开证书颁发机构管理单元以选择"已颁发的证书"文件夹
- 电话条目显示在摘要视图内,以下是显示的一些详细信息:
  - 。请求ID:唯一序列号

相关链接

- Requester Name:必须显示已配置的CiscoRA帐户的用户名
- 证书模板:必须显示所创建的CiscoRA模板的名称
- 。已颁发的公用名:必须显示设备名称附加的电话型号
- 证书生效日期和证书到期日期

📔 Console Root	Request ID	Requester Name	Binary Certificate	Certificate Template	Issued Common Name	Certificate Effective Date	Certificate Expiration Date
Active Directory Domains and Tru	<b>2</b>	MICHAMEN1\Administrator	BEGIN CERTI	Web Server (WebSer	LAB-DC-IIS.michamen	2/26/2019 9:56 PM	2/25/2021 9:56 PM
Active Directory Users and Computer	3	MICHAMEN1\LAB-DC-RTP\$	BEGIN CERTI	Domain Controller (	LAB-DC-RTP.michame	2/26/2019 10:20 PM	2/26/2020 10:20 PM
A Certification Authority (Local)	4	MICHAMEN1\ciscora	BEGIN CERTI	CiscoRA (1.3.6.1.4.1.3	CP-8865-SEP74A02FC0	2/26/2019 10:31 PM	2/26/2021 10:41 PM
a 🛃 LAB-DC-RTP	-						
Revoked Certificates							
Issued Certificates							
Pending Requests							
Failed Requests							
Certificate Templates							

- CAPF在线CA故障排除
  技术支持和文档 Cisco Systems

### 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)。