

在Prem上配置CSSM并在ISE中注册许可证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[在VMWARE ESXi上本地安装CSSM。](#)

[本地CSSM的初始配置。](#)

[将CSSM内部与智能帐户集成](#)

[选项1：通过Internet连接在本地注册CSSM。](#)

[选项2：无需互联网连接即可自行注册CSSM。](#)

[将CSSM内部部署与ISE集成。](#)

[从Windows CA创建证书。](#)

[在Windows服务器上添加DNS记录。](#)

[故障排除](#)

[主机/IP地址无法访问。\(ISE上出错\)](#)

[SSO服务：无法访问思科。\(本地CSSM出错\)](#)

[CSR中的公用名不是DNS可解析的主机名或IP地址，请重试。\(CSSM本地错误\)](#)

简介

本文档介绍如何将CSSM本地与思科身份服务引擎(ISE)和思科智能帐户集成，以确保无缝设置。

先决条件

要求

ISE 3.X

思科智能软件管理器(CSSM)版本8版本202304 +

使用的组件

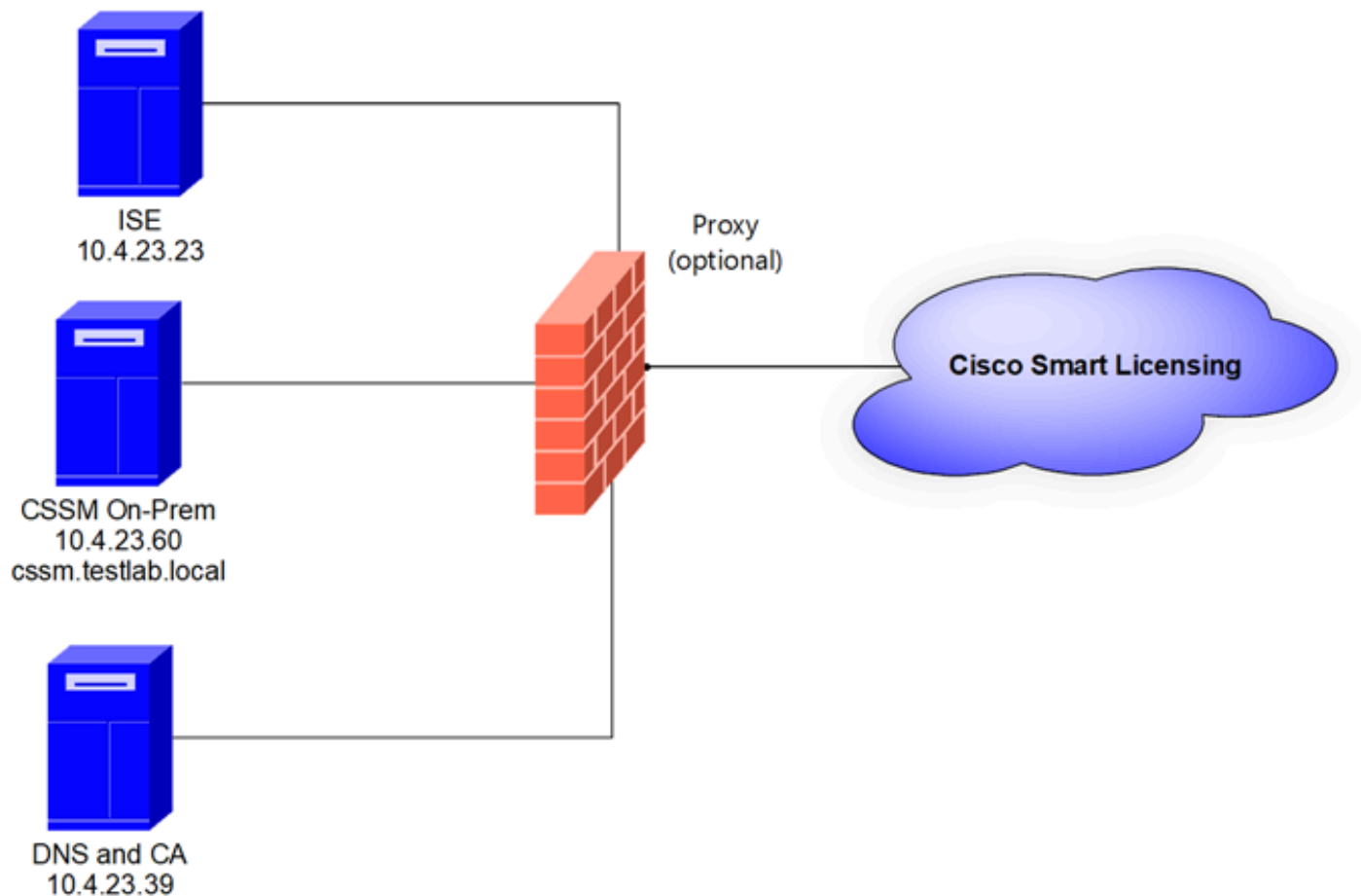
- 身份服务引擎3.2补丁2
- Prem 8.20234上的SSM
- Windows Active Directory 2016(DNS和证书颁发机构服务)
- VMWare ESXi版本7

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

网络图



常规拓扑

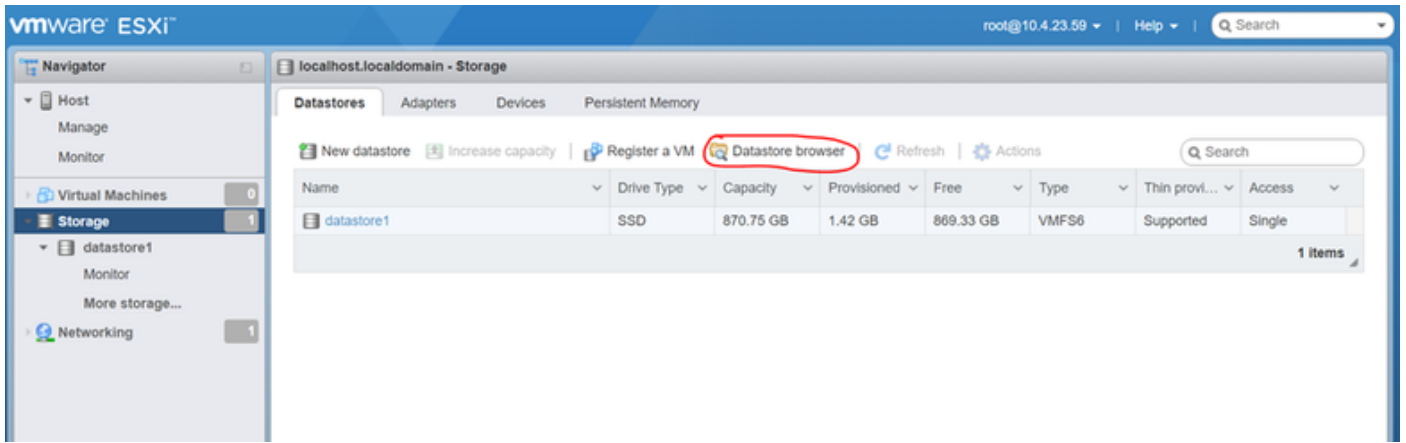
在VMWARE ESXi上本地安装CSSM。

1. 下载Cisco IOS®。您可以使用下一个链接

: <https://software.cisco.com/download/home/286285506/type/286326948/release/8-202304>

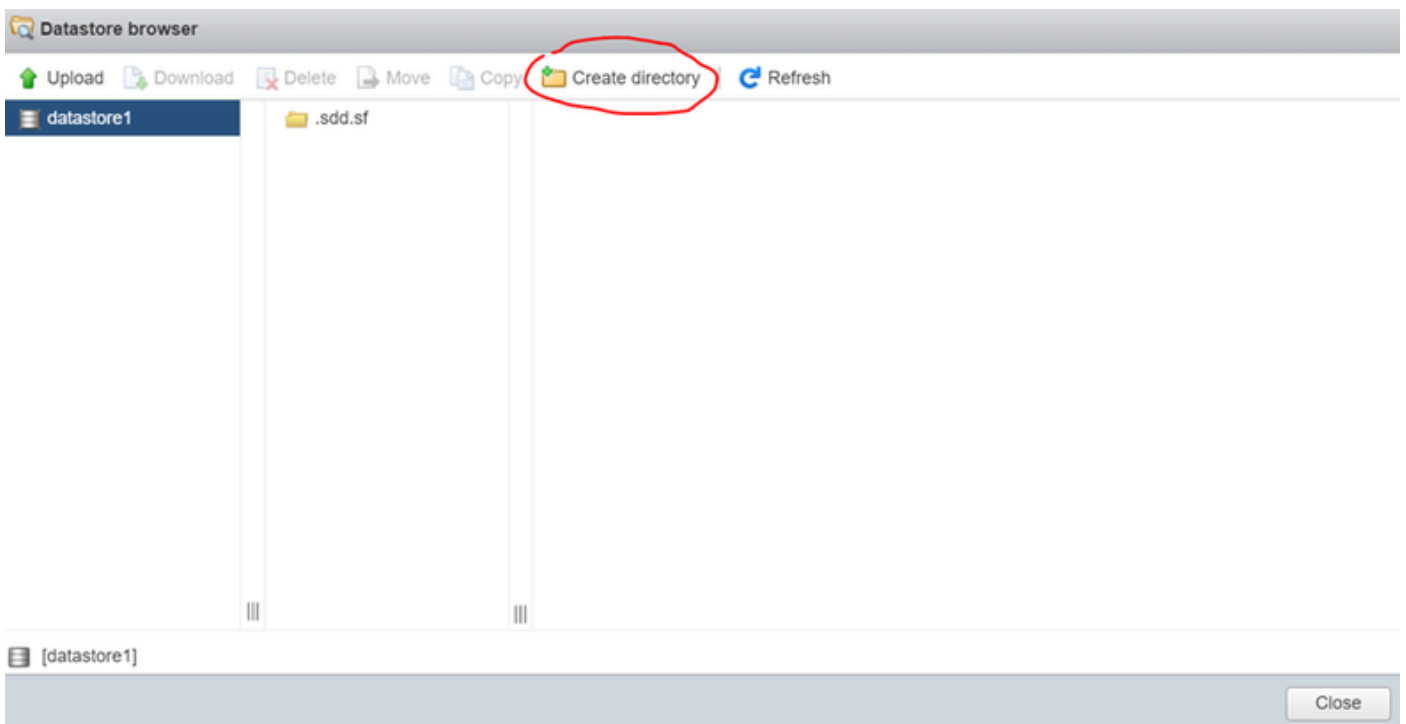
2. 在VMWARE ESXi中上传ISO。

导航到存储>数据存储浏览器。



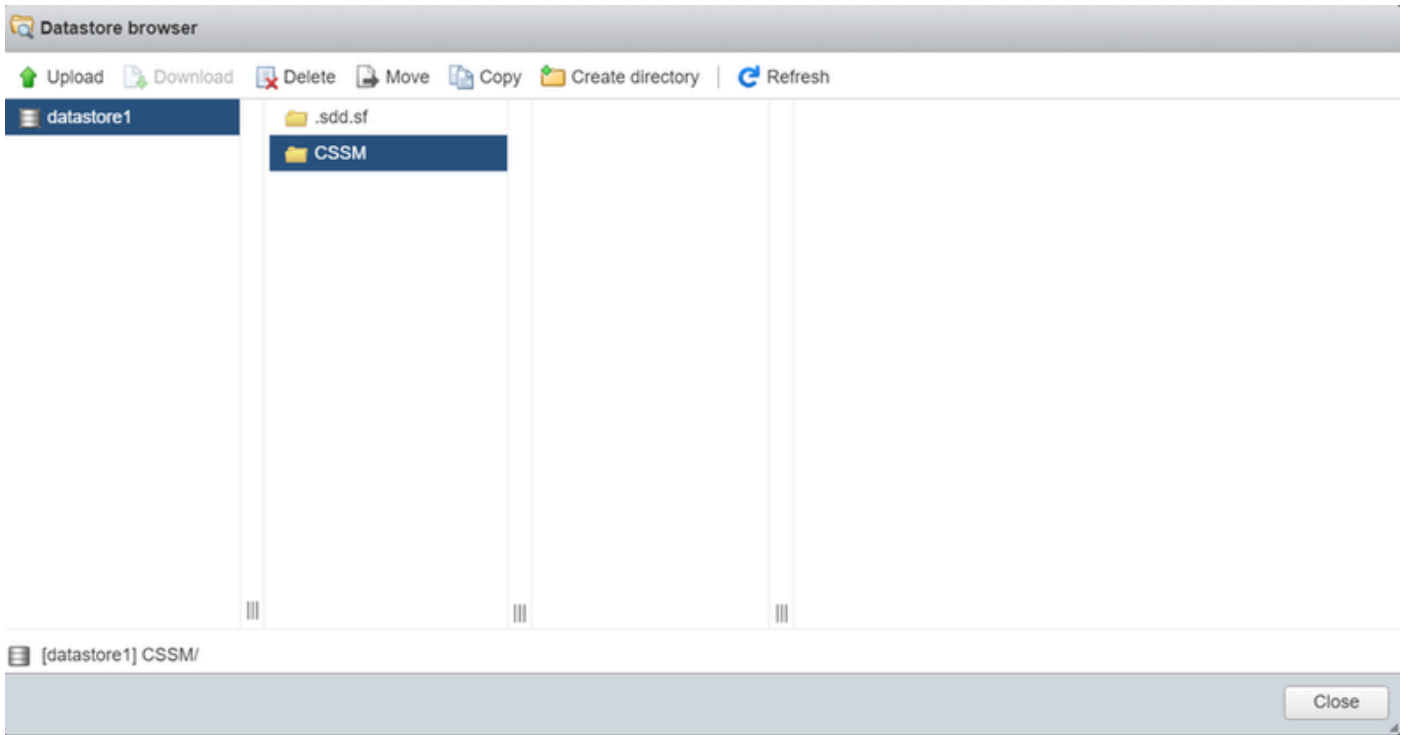
Data Browser部分

3. 单击创建目录以创建新文件夹（可选）。



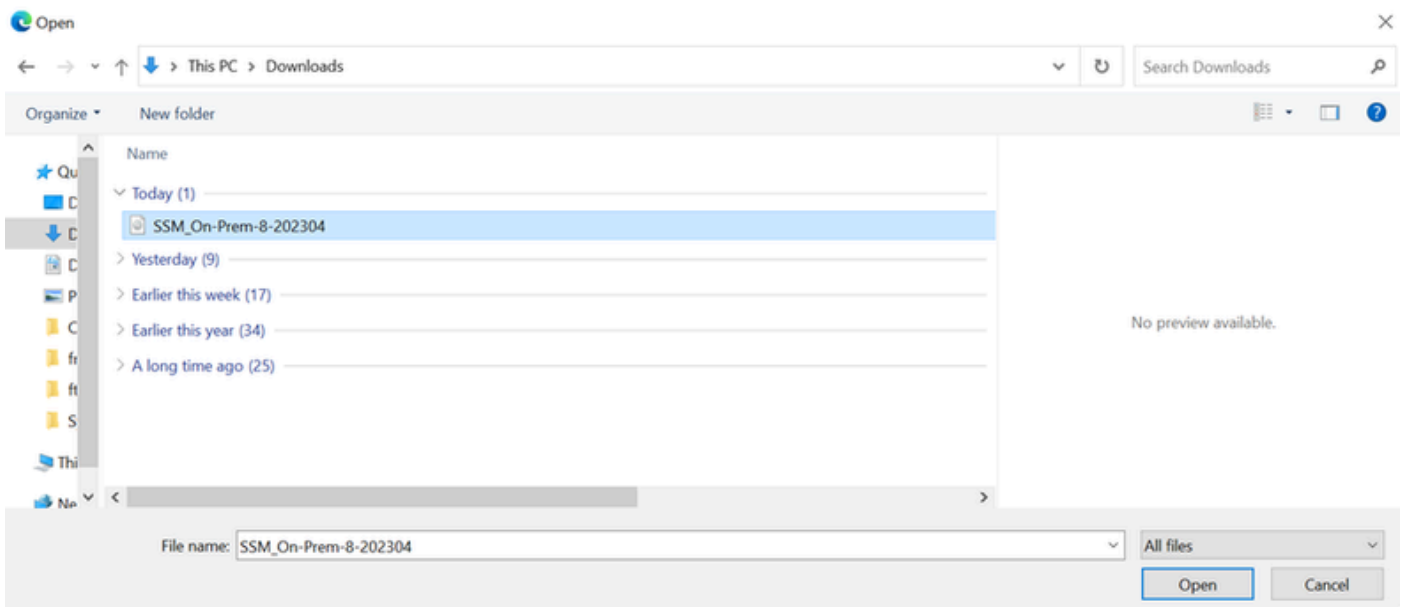
创建目录

在本示例中，创建了CSSM文件夹：



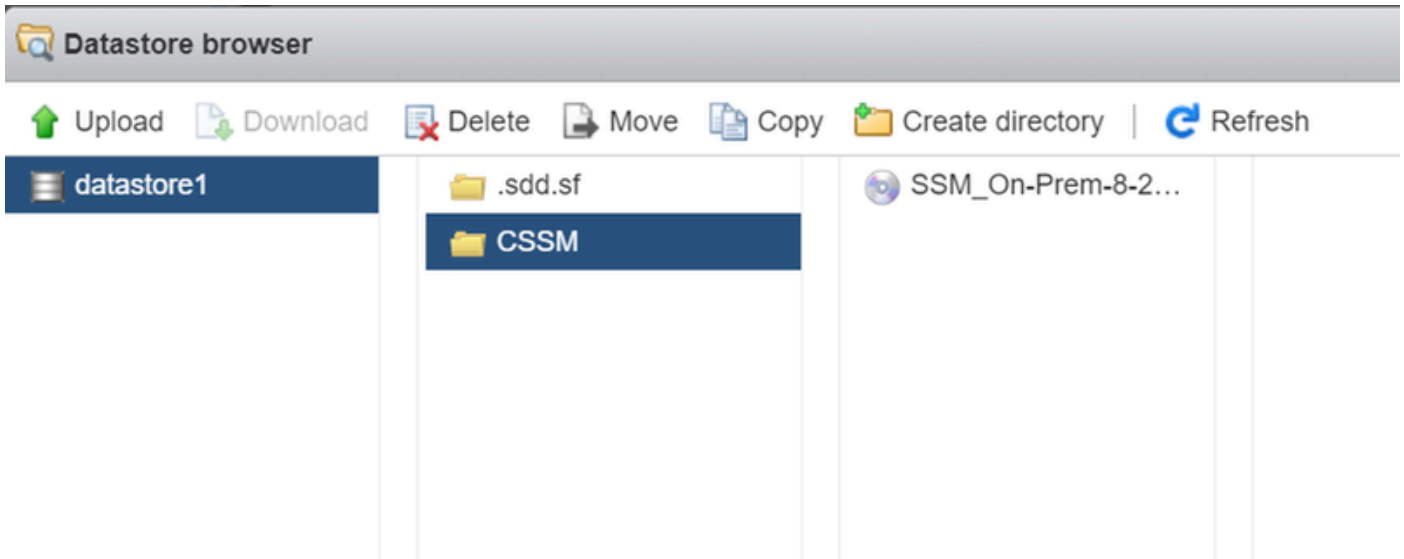
创建文件夹

4. 单击上传，然后选择ISO文件。



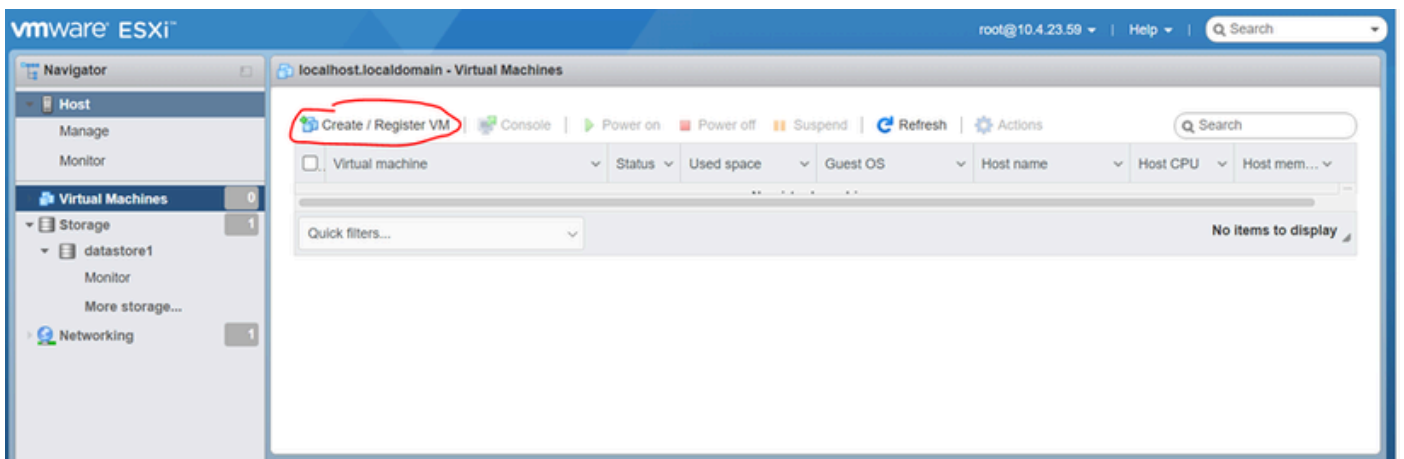
上传ISO

现在ISO文件位于CSSM文件夹中：



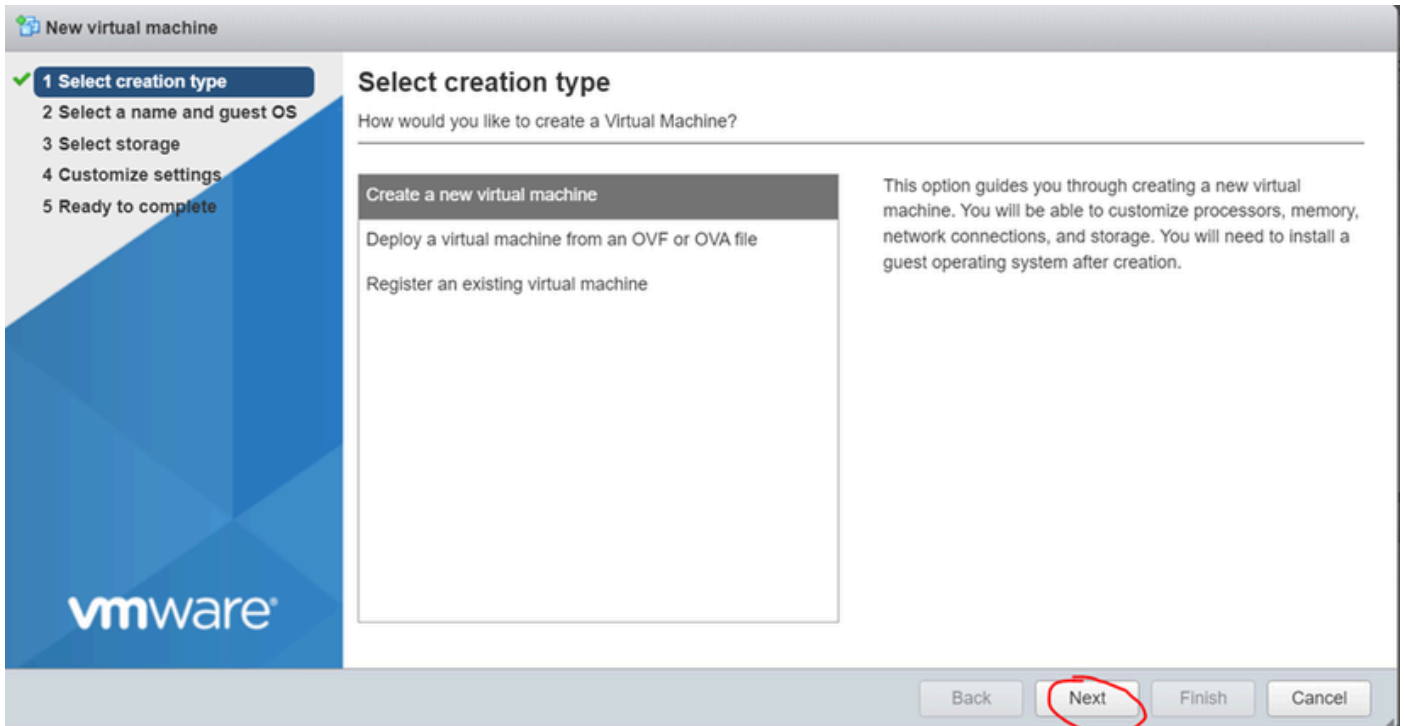
ISO上传完成

5. 创建虚拟机。导航到虚拟机>创建/注册VM。



创建新的VM第01步

6. 选择创建新虚拟机，然后单击下一步。

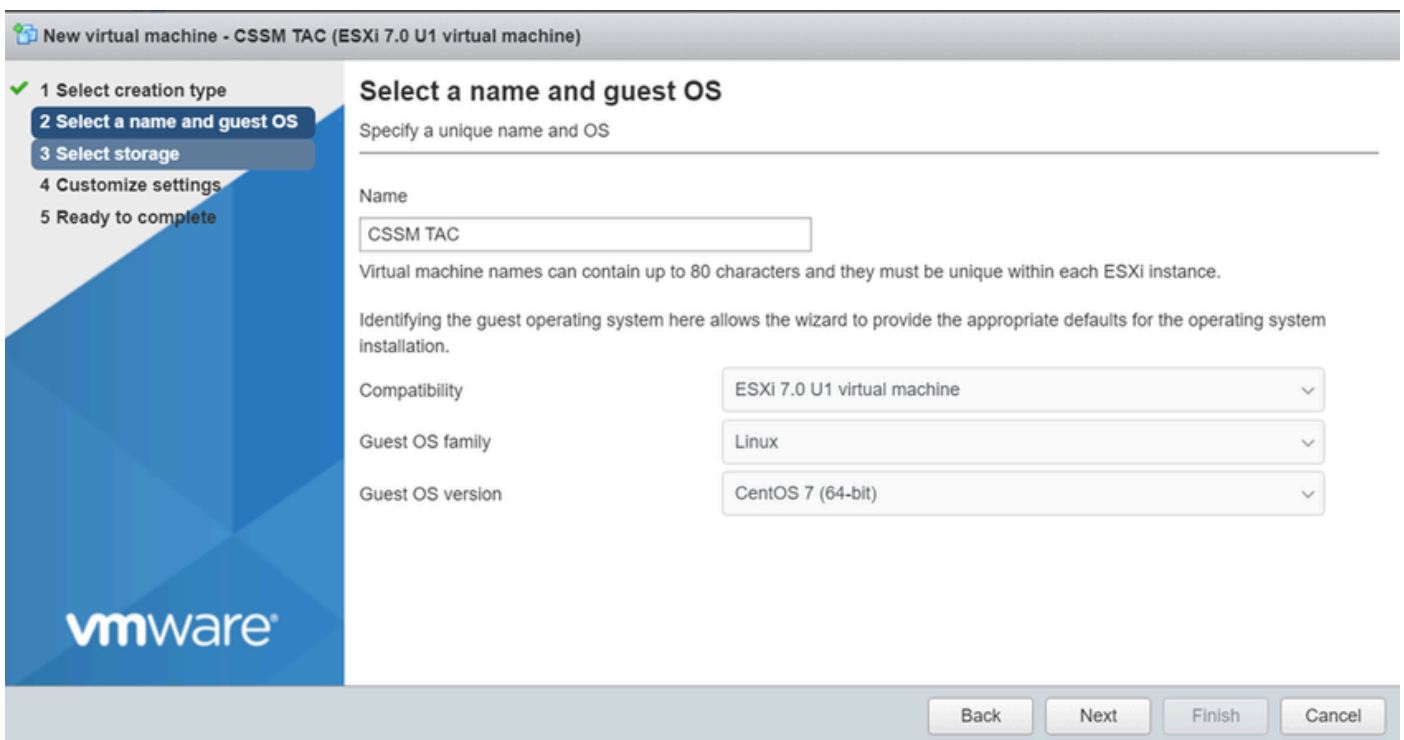


创建新的VM第02步

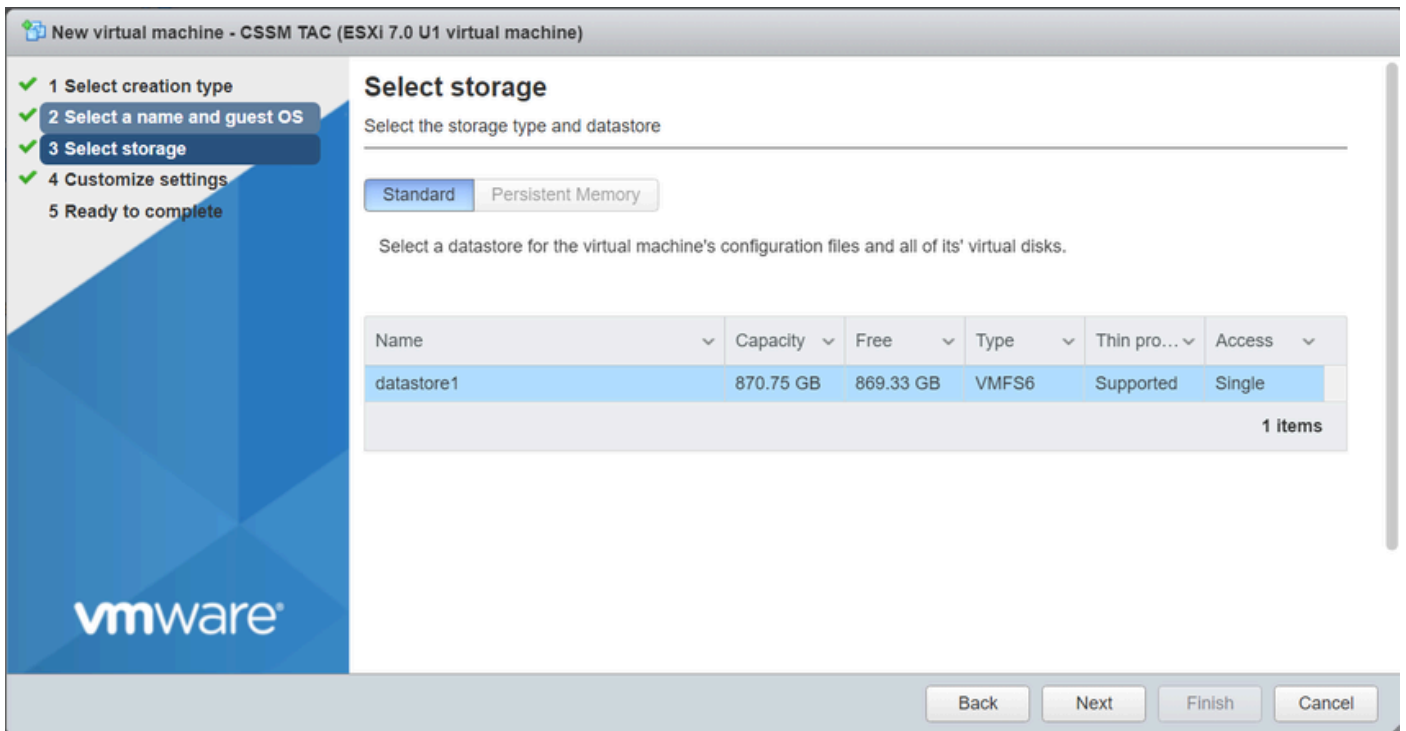
7. 然后配置以下参数：

- Name：输入虚拟机的名称。
- 兼容性：选择ESXi 6.0或更高版本或ESXi 6.5或更高版本。
- 访客操作系统系列：Linux。
- 访客操作系统版本：选择CentOS 7（64位）或其他2.6x Linux（64位）

单击 Next。



8. 选择您的存储，然后单击下一步。



存储列表

9. 配置以下参数：

- CPU：最少4个。实际的vCPU设置取决于您的扩展要求



注意：无论选择的虚拟插槽数量是多少，每个插槽的核心数量都需要设置为1。例如，4个vCPU配置需要配置为4个插槽，每个插槽1个核心。

| | | | |
|------------------|---|---|------------|
| ▼ CPU | 4 | ▼ | ⓘ |
| Cores per Socket | 1 | ▼ | Sockets: 1 |

核心配置

- 内存：8 GB
- 硬盘：200 GB，并确认调配设置为精简调配。

| | | | |
|-------------------|--|----|--|
| ▼ Hard disk 1 | 200 | GB | |
| Maximum Size | 869.33 GB | | |
| Location | [datastore1] CSSM TAC | | <input type="button" value="Browse..."/> |
| Disk Provisioning | <input checked="" type="radio"/> Thin provisioned <input type="radio"/> Thick provisioned, lazily zeroed <input type="radio"/> Thick provisioned, eagerly zeroed | | |

磁盘配置

- 网络适配器：选择E1000适配器类型，然后选择开机时连接。

| | |
|----------------------|---|
| ▼ Network Adapter 1 | VM Network |
| Status | <input checked="" type="checkbox"/> Connect at power on |
| Adapter Type | E1000e |

配置网络设置

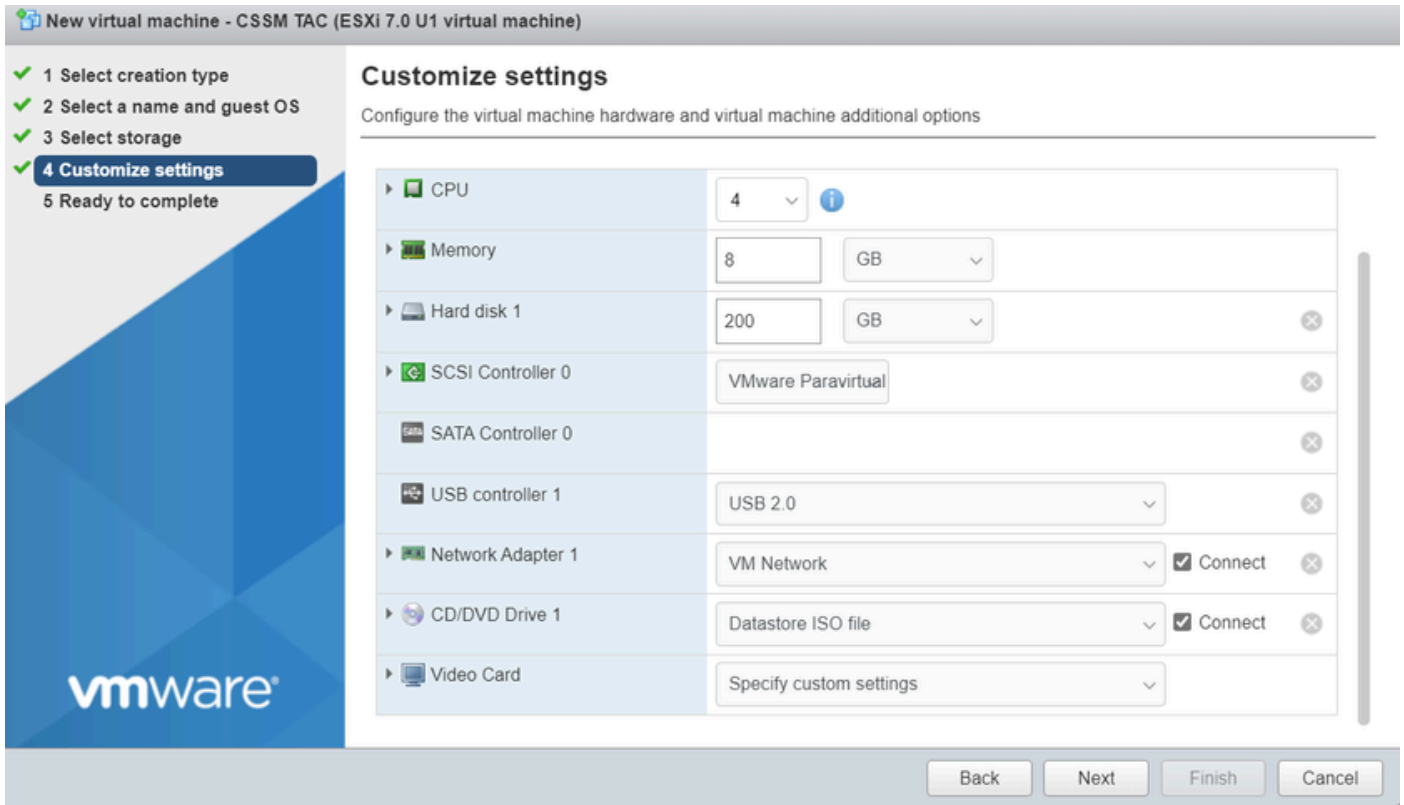
- CD/DVD驱动器：选择“数据ISO文件”并选择ISO文件。

Datastore browser

| | | | |
|--|---|---------------------------|---|
| <p>datastore1</p> <ul style="list-style-type: none"> vmimages | <ul style="list-style-type: none"> .sdd.sf CSSM | <p>SSM_On-Prem-8-2...</p> | <p>SSM_On-Prem-8-2023... 2.92 GB Wednesday, July 26, 2...</p> |
|--|---|---------------------------|---|

ISO映像

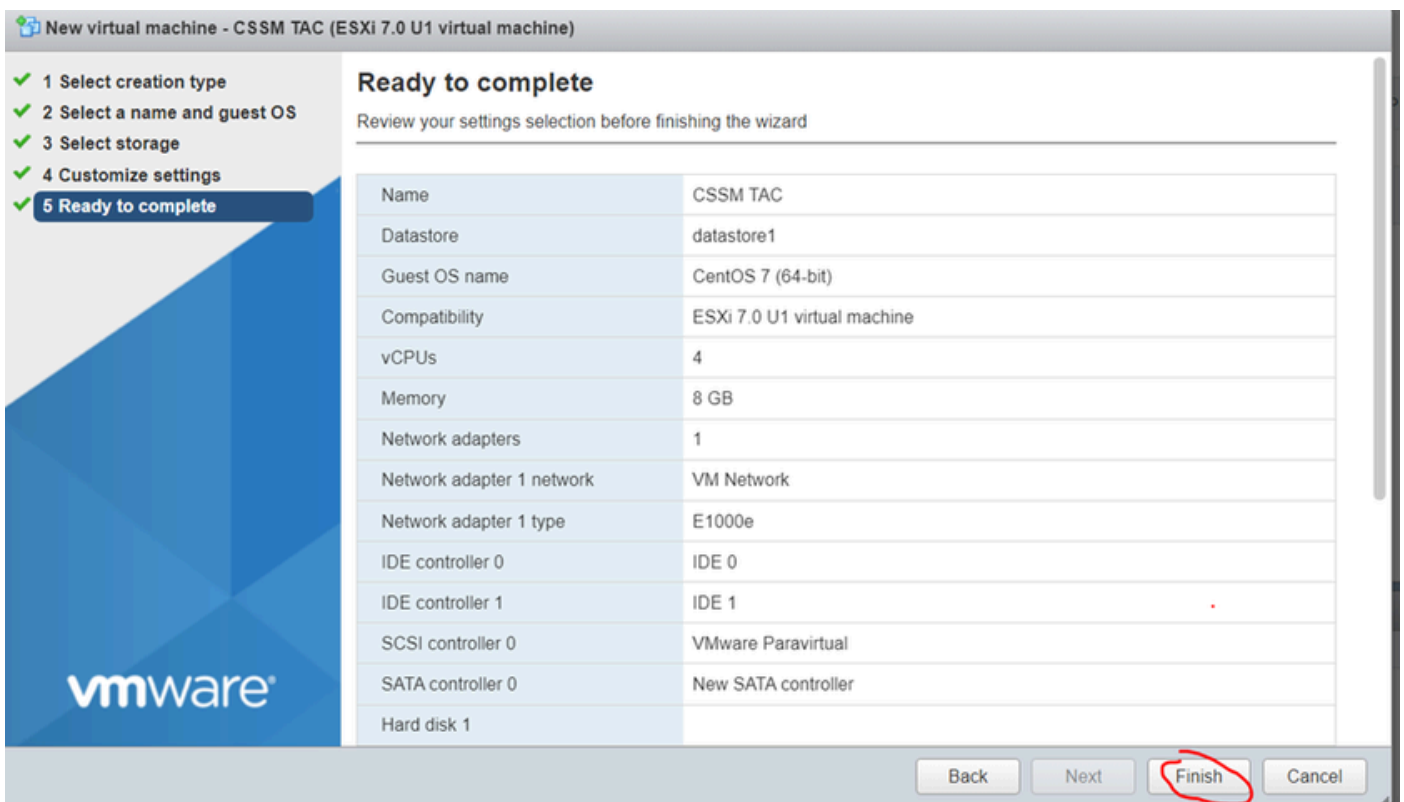
完成前面的步骤后，您可以验证设置的摘要。



摘要VM配置01

单击 Next。

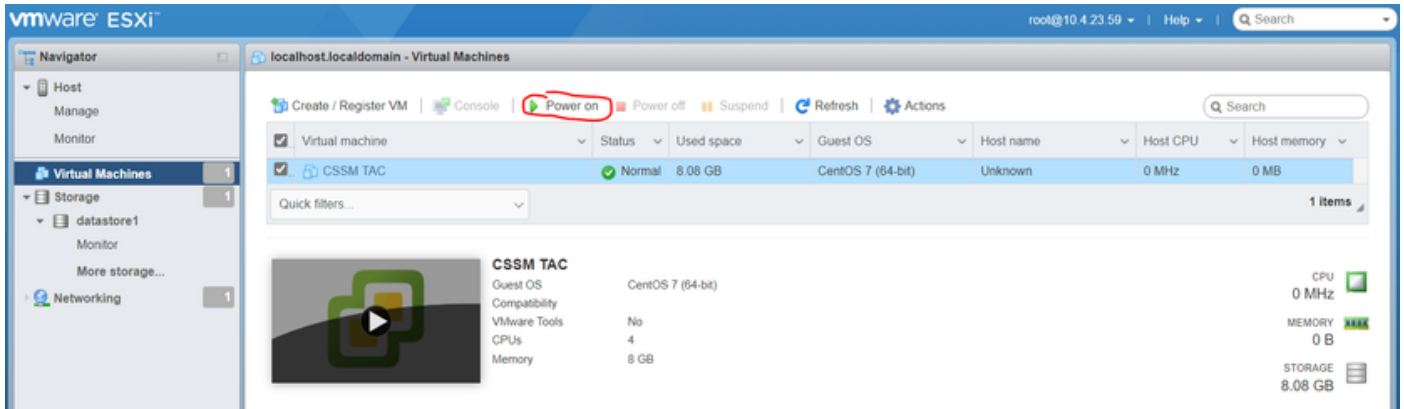
10. 单击完成。



摘要VM配置02

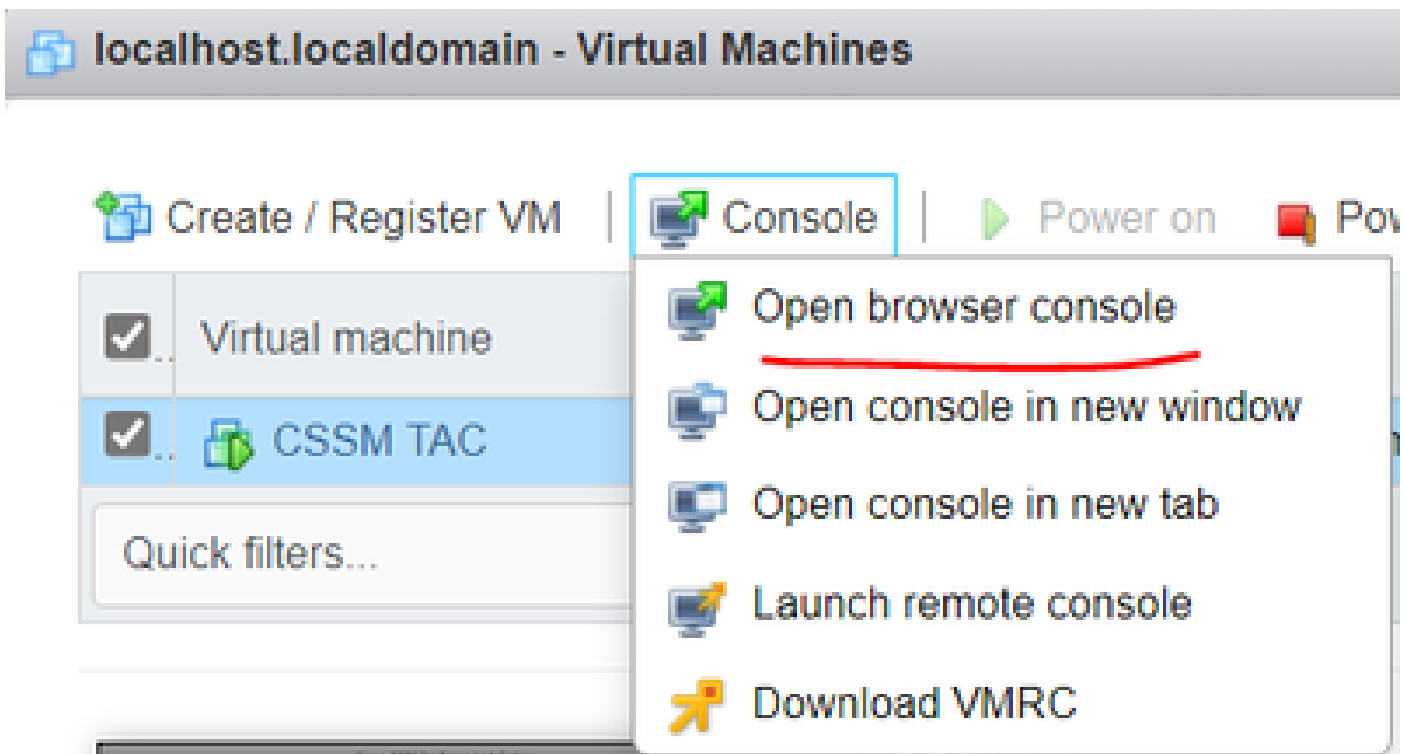
CSSM本地的初始配置。

1. 在VMWARE ESXi中，导航到虚拟机并选择VM，然后单击开机。



开机选项

2. 您可以通过多个选项来管理VM控制台。选择Console > Open browser console。

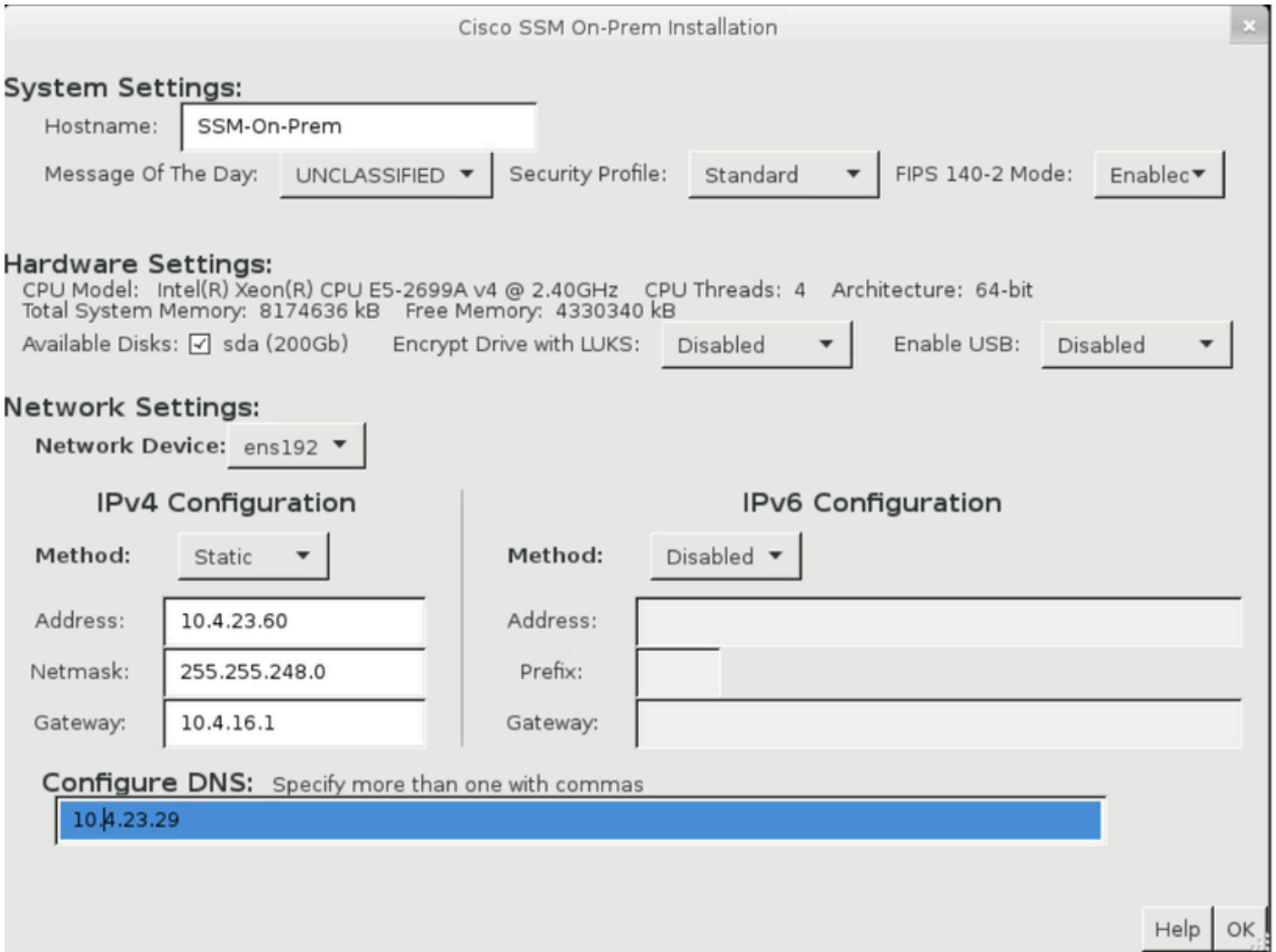


用于管理虚拟机的选项

3. 配置您的网络设置。



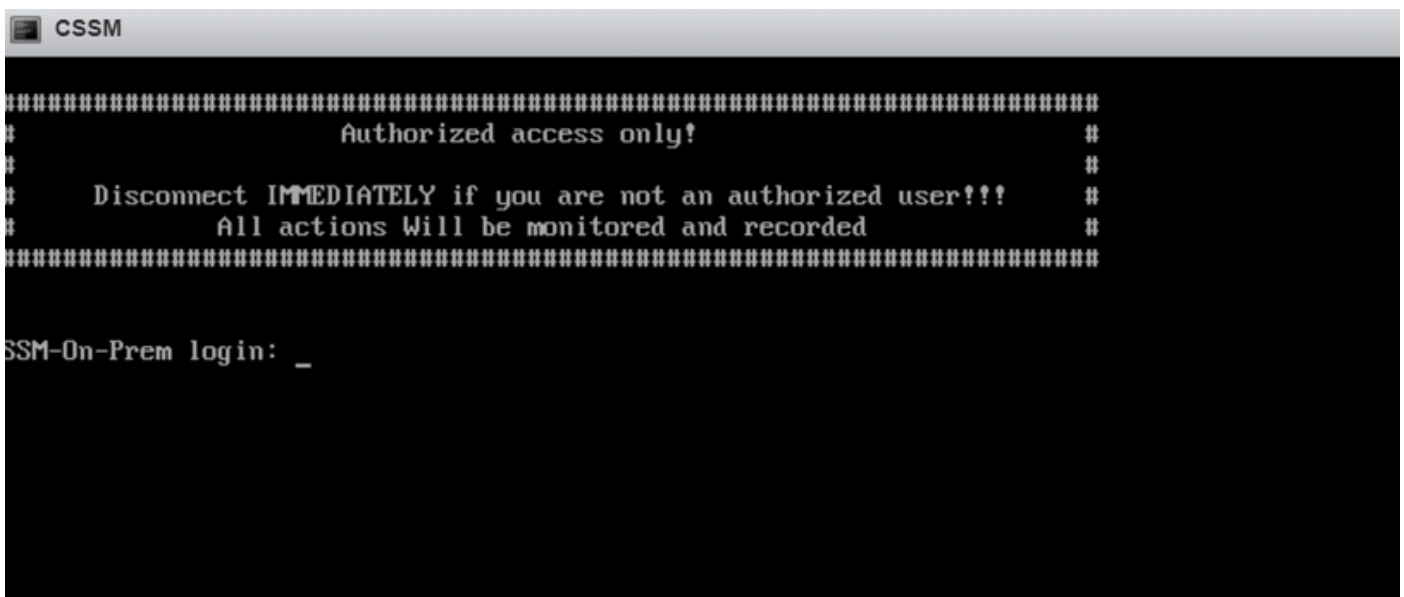
注意：配置解析CSSM FQDN的DNS服务器的IP地址非常重要。



配置CSSM网络设置

单击Ok 配置您的新CLI密码。

4. 然后，安装过程开始并完成，直到您看到访问提示符。



CSSM初始配置已完成

5. 打开浏览器并输入https:// <ip_address_CSSM>。



Log into an Existing Account

User Name

Password

Log In

[Forgot Password](#)

Welcome to Smart Software Manager On-Prem where you can locally manage Smart Licensing and perform local Account Management functions for your organization.

CSSM登录页

使用默认凭证：

用户名：admin

密码：CiscoAdmin!2345

6. 选择您的语言。
7. 创建新的GUI密码。
8. 配置主机公用名。（示例：hostname.yourdomain）。

在本例中，cssm.testlab.local被配置为主机公用名。

Welcome to Cisco Smart Software Manager On-Prem

STEP 1 System Language Selection

STEP 2 Temporary Password Reset

STEP 3 Host Common Name

STEP 4 Review and Confirm

Products that support String SSL Cert Checking require the SSM On-Prem's "Host Common Name" to match the "destination" URL address. For example:

- Products using Smart Transport must use both the "license smart url" configuration and the "cssm.testlab.local" value in the URL string.
- Legacy products using Smart Call Home must use both the "destination address http" configuration and the "cssm.testlab.local" value in the URL string.

If the above URLs do not match expectations, refer to the SSM On-Prem AdminWorkspace -> Security Widget to change the Host Common Name to the correct value.

The option to configure alternative names (SAN) is available in Admin Console under Security -> Certificates and can be configured after the initial setup.

* Host Common Name
cssm.testlab.local

9. 验证您的配置并单击Apply。

| | | | |
|-------------------------------------|------------------------------------|----------------------------|------------------------------|
| STEP 1 System Language Selection | STEP 2 Temporary Password Reset | STEP 3 Host Common Name | STEP 4 Review and Confirm |
|-------------------------------------|------------------------------------|----------------------------|------------------------------|

Once you click "Apply", you will be redirected to the login page where you will need to login with your new password. Please ensure you have securely stored your password for future logins.

Review and Confirm

| | |
|--------------------|----------------------|
| Language Selected: | English |
| Password Reset: | Yes |
| Host Common Name: | sccmtac.ciscotac.com |

Back **Apply**

CSSM初始设置已完成。

将CSSM内部与智能帐户集成

您需要将智能帐户与本地服务器上的CSSM关联。

1. 使用下一个链接打开思科智能帐户：

<https://software.cisco.com/>

2. 然后选择智能软件管理器部分下的管理许可证。

| | | | |
|--|--|---|--|
| | | | |
| | Smart Software Manager Track and manage your licenses. Convert traditional licenses to Smart Licenses. Manage licenses > | Download and Upgrade Download new software or updates to your current software. Access downloads > | Traditional Licenses Generate and manage PAK-based and other device licenses, including demo licenses. Access LRP > |
| | Manage Smart Account Update your profile information and manage users. Manage account > | EA Workspace Generate and manage licenses purchased through a Cisco Enterprise Agreement. Access EA Workspace > | Manage Entitlements eDelivery, version upgrade, and more management functionality is now available in our new portal. Access MCE > |
| | 管理许可证选项 | | |

3. 导航到资产并复制智能帐户名称和虚拟帐户。在本指南中，这是 InternalTestDemoAccount67 和 AAA MEX TEST。

Cisco Software Central

Scheduled Downtime Notification - License Registration Portal (LRP), Manage Smart Account & Account Administration, Plug-N-Play (PnP), Smart Software Manager

Cisco Software Central > Smart Software Licensing

InternalTestDemoAccount67.cisco.com

Smart Software Licensing

SL Product Details Support Help

Alerts **Inventory** Convert to Smart Licensing Reports Preferences On-Prem Accounts Activity

Virtual Account: AAA MEX TEST

General Licenses Product Instances Event Log

Virtual Account

| | |
|--------------------------|----------------|
| Description: | Only for tests |
| Default Virtual Account: | No |

软件思科页面

4. 打开 CSSM GUI 并选择 Admin Workspace 选项。

On-Prem License Workspace

CISCO

Admin Workspace Hello, Local Admin Log Out

Smart Software Manager On-Prem

License

Smart Licensing
Track and manage Smart Licensing

Administration

Request an Account
Get an Account for your organization. The Account must be approved by your System Administrator or System Operator before it can be used.

Request Access to an Existing Account
Submit a request for access to an existing local Account. Approval must be granted by a Smart Account Administrator for your local Account.

Manage Account
Modify the properties of your Accounts and associate existing User IDs with Accounts.

CSSM 主菜单。

5. 然后选择 Accounts。

On-Prem Admin Workspace

Smart Software Manager On-Prem



Access
Management



Settings



Accounts



Support
Center



API Toolkit



Synchronization



Network



Users



Security

Generate CSR

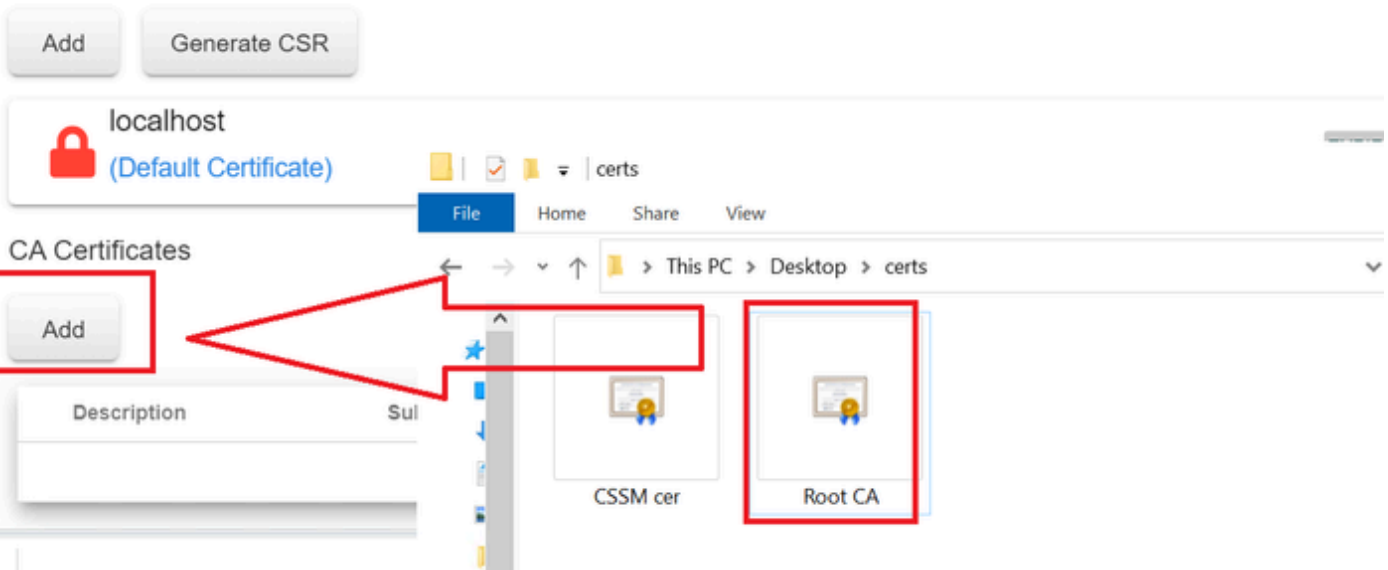
| | |
|--------------------------|---------------------------|
| Common Name | cssm.testlab.local |
| Organizational Unit | Testlab |
| Country | Mexico ▼ |
| State/Province | Mexico City |
| City/Locality | Mexico City |
| Organization | SEC AAA |
| Key Size | 2048 ▼ |
| Subject Alternative Name | cssm.testlab.local |



CSR详细信息。

4. 对CSR签名：有关详细信息，请查阅本文档中的[从Windows CA创建证书](#)。
5. 上传根CA证书。

Browser Certificate



正在上传根CA。

单击Proceed。



Please note that if you are uploading **LDAP Server Certificate**, it is mandatory to reboot your SSM On-Prem server for the certificate to take effect and thus allowing secure communication with the server.

Below are the commands for non-HA(standalone) deployments:

1. Execute "reboot" command in Onprem-console
ssh admin@<IP>
onprem-console
reboot

For HA deployments

1. Execute reboot command on active node in onprem-console. After failover, ensure that DB replication has started. If you wish to restore the previous active node, execute another reboot, after verifying replication has started.

The active node is the node that is serving the virtual IP of the cluster.

Proceed

Proceed选项。

6. 输入说明，选择根证书，然后单击确定。

Upload Certificate

• Description:

• Certificate:

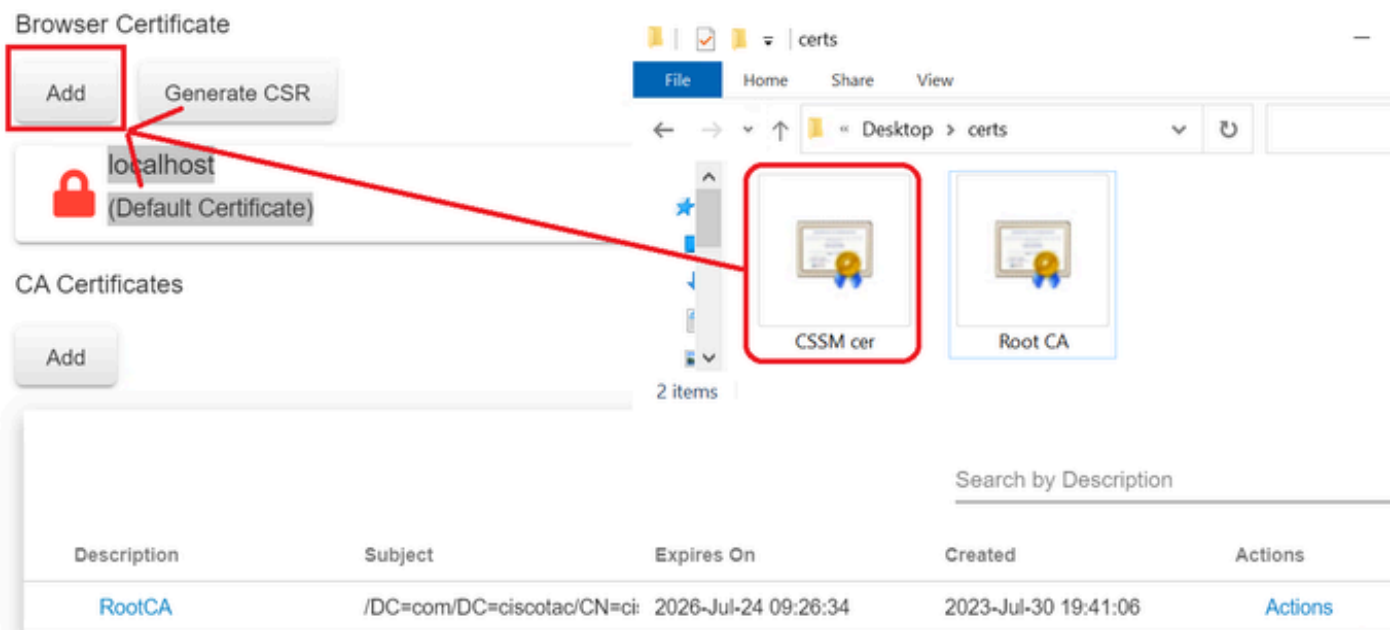
描述根CA。

7. 上传由CA签名的CSR(CSSM身份证书)。

Browser Certificate

localhost
(Default Certificate)

CA Certificates



2 items

Search by Description

| Description | Subject | Expires On | Created | Actions |
|-------------|---------------------------|----------------------|----------------------|-------------------------|
| RootCA | /DC=com/DC=ciscotac/CN=ci | 2026-Jul-24 09:26:34 | 2023-Jul-30 19:41:06 | Actions |

上传CSSM身份证书。



注意：注意：在我们的情况下，中间证书在我们的CA中不存在。但是，如果在架构中使用中间证书，则中间证书是必需的。

8. 然后，确认两个证书均已安装。

Browser Certificate

Add

Generate CSR



cssm.testlab.local

EXPIRATION DATE: 2025-JUL-16

CA Certificates

Add

Search by Description

Description

Subject

Expires On

Created

Actions

RootCA

/DC=local/DC=testlab/CN=tes 2027-Apr-14 22:51:26

2024-Jul-16 21:18:52

[Actions](#)

证书验证。

9. 在SSM本地创建令牌：选择许可工作空间。

On-Prem Admin Workspace

CISCO

Licensing Workspace Log Out

Smart Software Manager On-Prem

Access Management Network Support Center

Accounts Security Synchronization

API Toolkit Settings Users

System Health

Good Your machine is working well

Server Name SSM-On-Prem

Version 8-202304

Uptime 3 days

Resource Monitor Percentage

CPU |

RAM |

DISK |

Interface

ens192 ↑ 6.9 MB/s ↓ 37 KB/s

Recent Alerts

工作空间页面。

10. 导航到智能许可。

On-Prem License Workspace

CISCO

Admin Workspace Hello, Local Admin Log Out

Smart Software Manager On-Prem

Demo Account

License

Smart Licensing

Track and manage Smart Licensing

Administration

Request an Account

Get an Account for your organization. The Account must be approved by your System Administrator or System Operator before it can be used.

Request Access to an Existing Account

Submit a request for access to an existing local Account. Approval must be granted by a Smart Account Administrator for your local Account.

CSSM智能许可页面

11. 查找您的本地虚拟帐户，然后单击新建令牌并单击继续。

Smart Licensing

Alerts | **Inventory** | Convert to Smart Licensing | Reports | Preferences | Activity

Local Virtual Account: [Default](#)

General | Licenses | Product Instances | SL Using Policy | Event Log

Local Virtual Account

Description: This is the default virtual account created during company account creation.
Default Local Virtual Account: Yes

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this Local Virtual Account. For products that support Smart Transport, you must configure the "license smart uri" on the product to use the [Smart Transport Registration URL](#). For products that support Smart Licensing Using Policy that use cslu as transport, you must configure the "license smart transport cslu" to use the [CSLU Transport URL](#). For legacy products that still use Smart Call Home, you must configure the "destination address http" on the product to use the [Smart Call Home Registration URL](#). The recommended method is Smart Transport. Please consult your Products Configuration Guide for setting the destination URL value.

New Token...

新令牌选项。

12. 选择创建令牌并复制它。

Create Registration Token



This dialog will generate the token required to register your product instances with your Account .

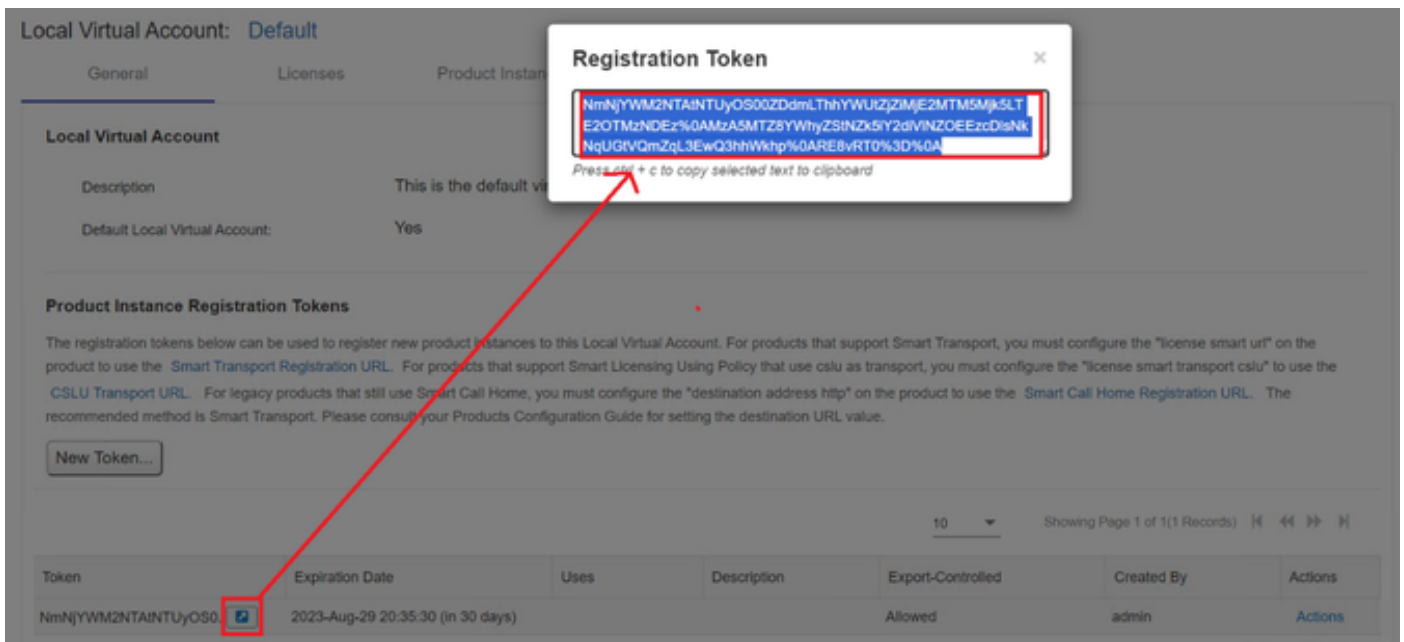
| | |
|-----------------------|--|
| Local Virtual Account | Default |
| Description | <input type="text"/> |
| Expire After | <input type="text" value="30"/> Days <i>Enter a value between 1 and 9999, but Cisco recommends a maximum of 30 days</i> |
| Max. Number of Uses | <input type="text"/> <i>The token will be expired when either the expiration or the maximum uses is reached.</i> |

Allow export-controlled functionality on the products registered with this token

Create Token

Cancel

创建新令牌。



令牌详细信息。

13. 打开ISE GUI并导航到Administration > Systems > Licensing，然后单击Registration details，选择SSM On-Prem server Host method，然后粘贴令牌。

License Type

Choose Registration Details to acquire pre-purchased license entitlements. Choose Permanent License Reservation to enable all Cisco ISE licenses. Enter the required details to enable Cisco ISE licenses. When you click Register, you agree to the terms and conditions detailed in [Smart Licensing Resources](#).

- Smart Licensing Registration
- Permanent License Reservation
- Specific License Reservation

Registration Details

When you register Cisco ISE in the [Cisco Smart Software Manager portal](#), a unique ID called the Registration Token is displayed in the portal. Copy the registration token displayed in the CSSM portal and paste it here.

Registration Token

NmNjYWM2NTAINTUyOS00ZDdmLThhYWU

许可证登记。

14. 在SSM内部部署服务器主机上输入SSM内部部署 FQDN，然后单击注册。

CSSM configuration

Security

Account Password Certificates Event Log

Product Certificate

Host Common Name
cssm.testlab.local

Subject Alternative Name

Save

NOTE: The Host Common Name is typically composed of Host + Domain Name(FQDN) and will look like "www.your-site.com" or "your-site.com". The SSL Server Certificate used for product communications is specific to the Common Name that has been issued at the Host. Therefore, the Common Name must match the Web address you will use to configure the Cisco Product when connecting to SSM On-Prem. The Common name is a part of the Subject Alternative Name by default. If you change the Common Name or add Subject Alternative Name, you must resynchronize your Local Account in order for Cisco to issue a new product certificate(TG cert).

Browser Certificate

Add Generate CSR

cssm.testlab.local

EXPIRATION DATE: 2025-JUL-16

ISE configuration

Connection Method
SSM On-Prem server

SSM On-Prem server Host
cssm.testlab.local

Note: Cisco Support Diagnostics will not work with SSM On-Prem server registration.

Tier
 Essential Advantage Premier Device Admin

Virtual Appliance
 ISE VM License

This enables the ISE features for the purchased licenses to be tracked by Cisco Smart Licensing.

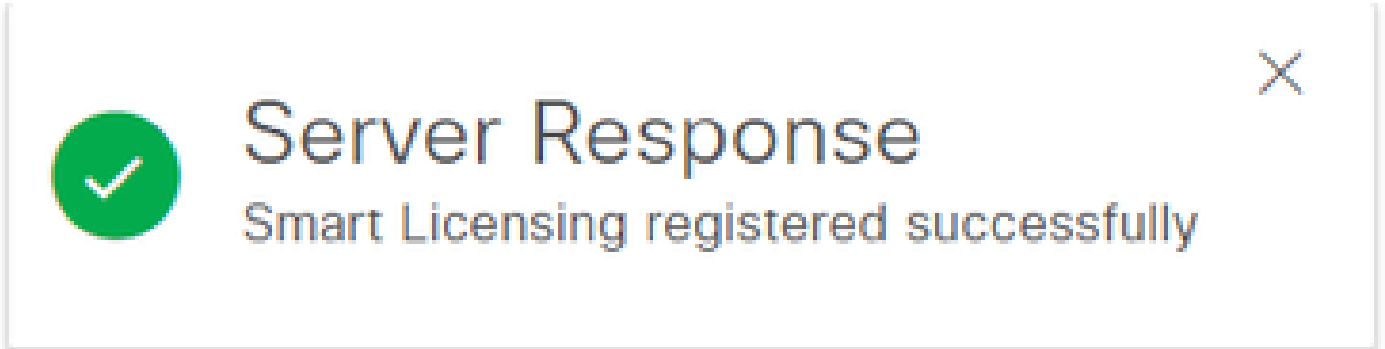
By clicking Register you will agree to the Terms&Conditions. You can download Terms&Conditions on [Smart Licensing Resources](#).

Cancel Register

CSSM和ISE设置。

注意：务必在主机公用名上配置主机名+域，因为ISE使用此参数与CSSM建立连接。您可以使用IP地址而不是主机名+域，但建议使用主机名+域

15. 最后，注册完成。

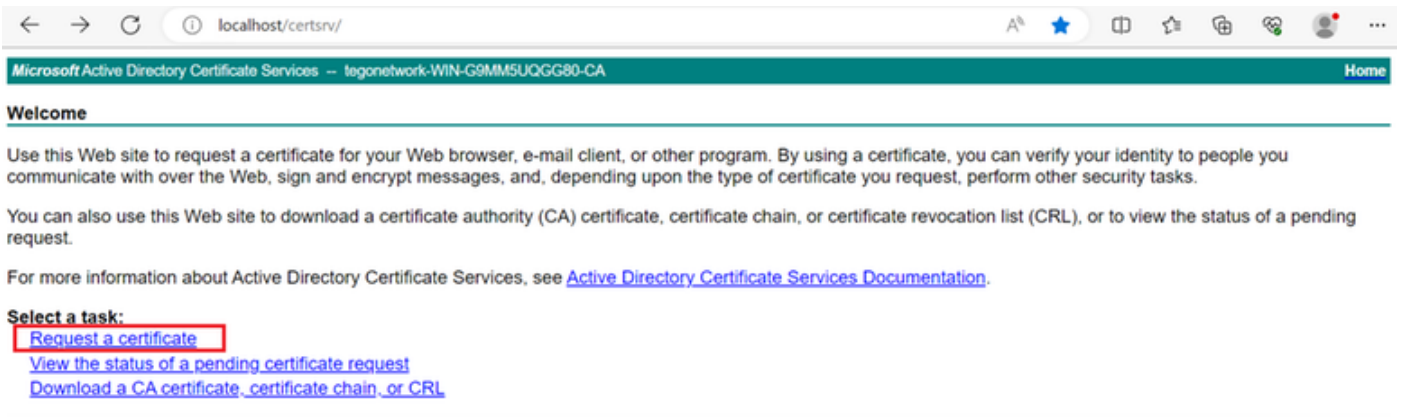


注册已完成。

从Windows CA创建证书。

如果您是证书颁发机构的管理员，则必须执行以下操作：

1. 打开Web浏览器并导航到<http://localhost/certsrv/>
2. 单击Request a certificate。



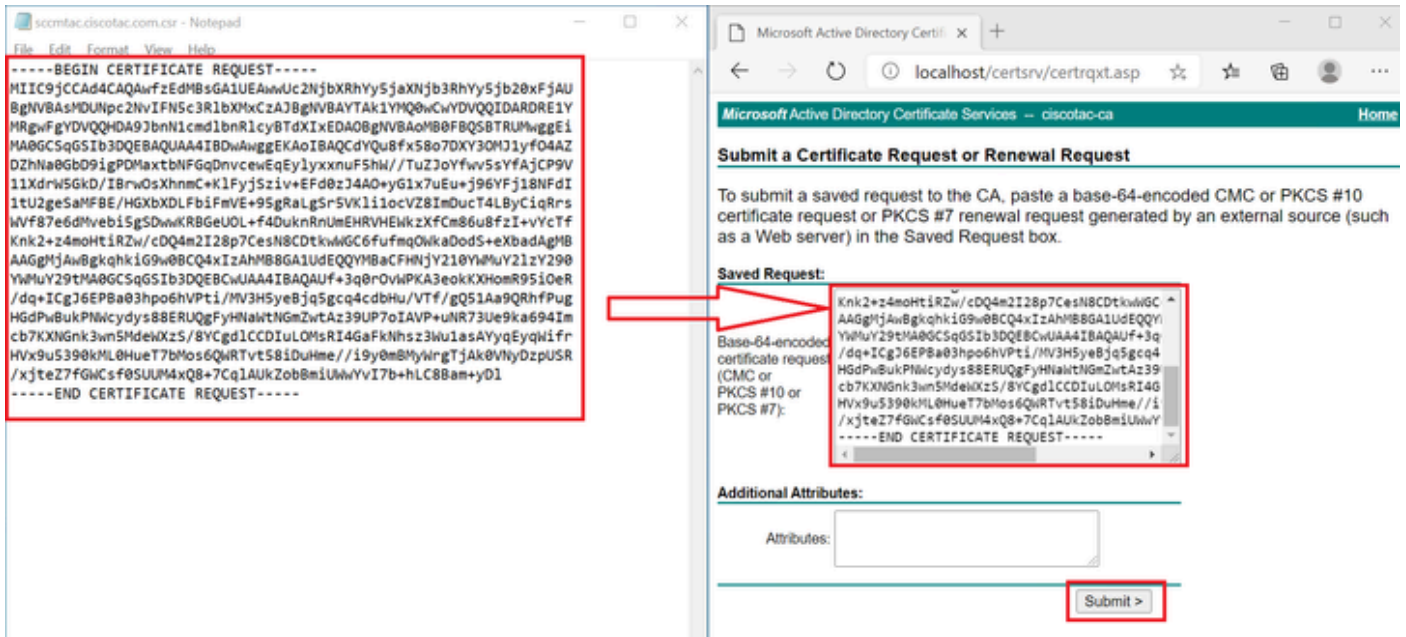
请求证书。

3. 单击高级证书请求。



高级证书请求。

4. 打开以前生成的CSR。 然后复制信息并粘贴到Saved request上。



提交证书。

点击提交后，将自动下载证书。

5. 现在下载CA证书根目录。导航回<http://localhost/certsrv/>并选择下载CA证书、证书链或CRL。

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 verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending 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](#)

下载根CA

6. 使用编码方法下载CA证书作为Base64。

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

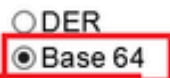
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:



A screenshot of a web interface showing a dropdown menu. The selected item is "Current [ciscotac-ca]". The dropdown is currently closed, showing only the selected item.

Encoding method:



A screenshot of a web interface showing two radio button options for the encoding method. The "Base 64" option is selected and highlighted with a red box.

[Download CA certificate](#)

[Download CA certificate chain](#)

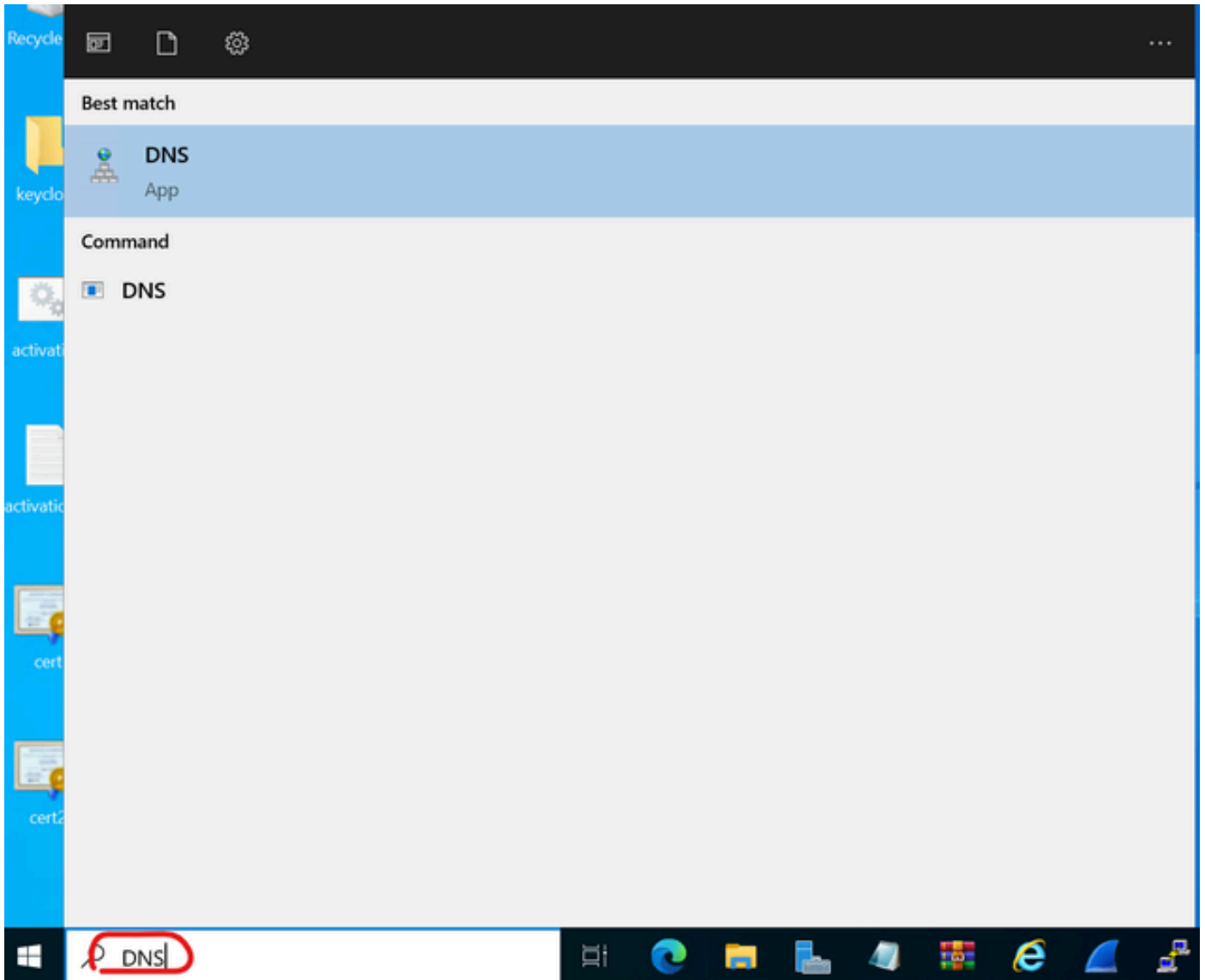
[Download latest base CRL](#)

Base 64选项。

在Windows服务器上添加DNS记录。

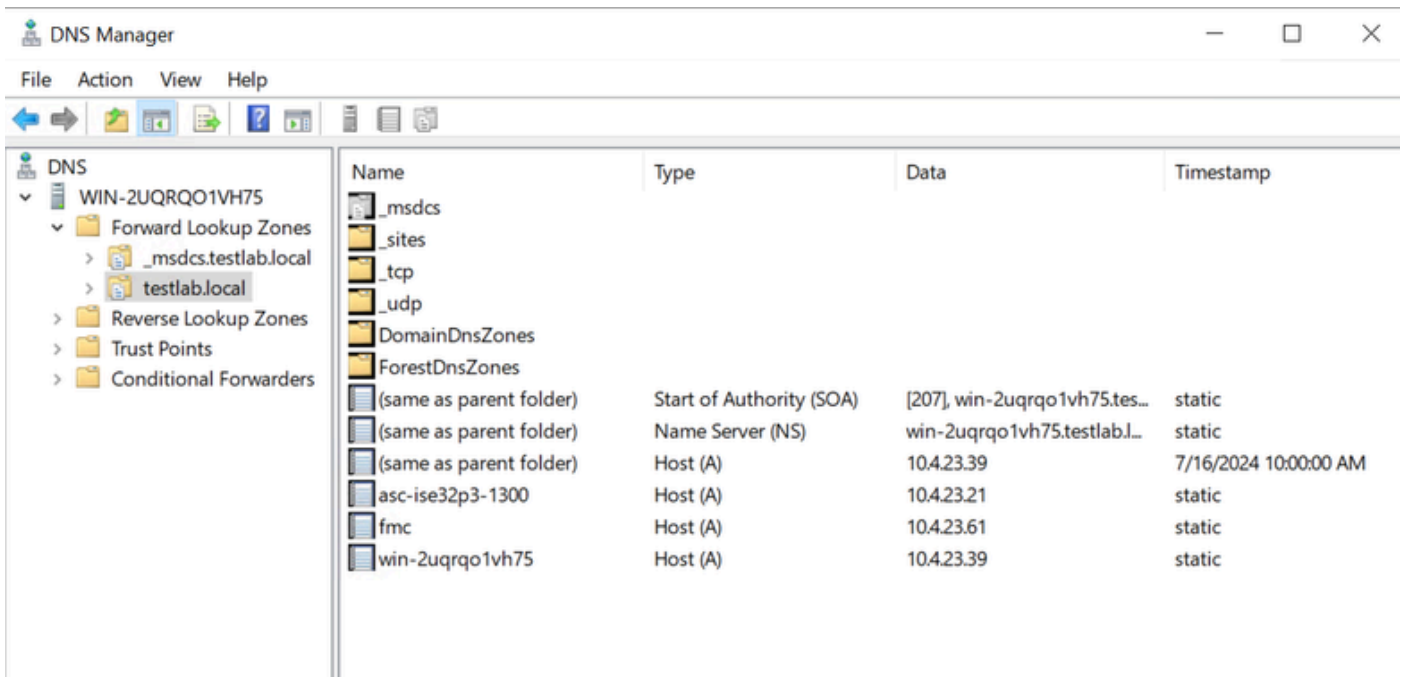
如果您是管理员，请添加ISE和CSSM FQDN。

1. 打开DNS管理器：在Windows查找器上键入“DNS”并打开DNS应用。



DNS选项。

2. 导航到正向查找区域>并选择您的域。



DNS管理器。

3. 右键单击屏幕上的黑色空白并选择“New Host (A or AAAA)”

Update Server Data File

Reload

New Host (A or AAAA)...

New Alias (CNAME)...

New Mail Exchanger (MX)...

New Domain...

New Delegation...

Other New Records...

DNSSEC



All Tasks



Refresh

Export List...

View



Arrange Icons



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）。