使用Nutanix硬件提供商连接问题排除Cisco HCI故障

目录

简介

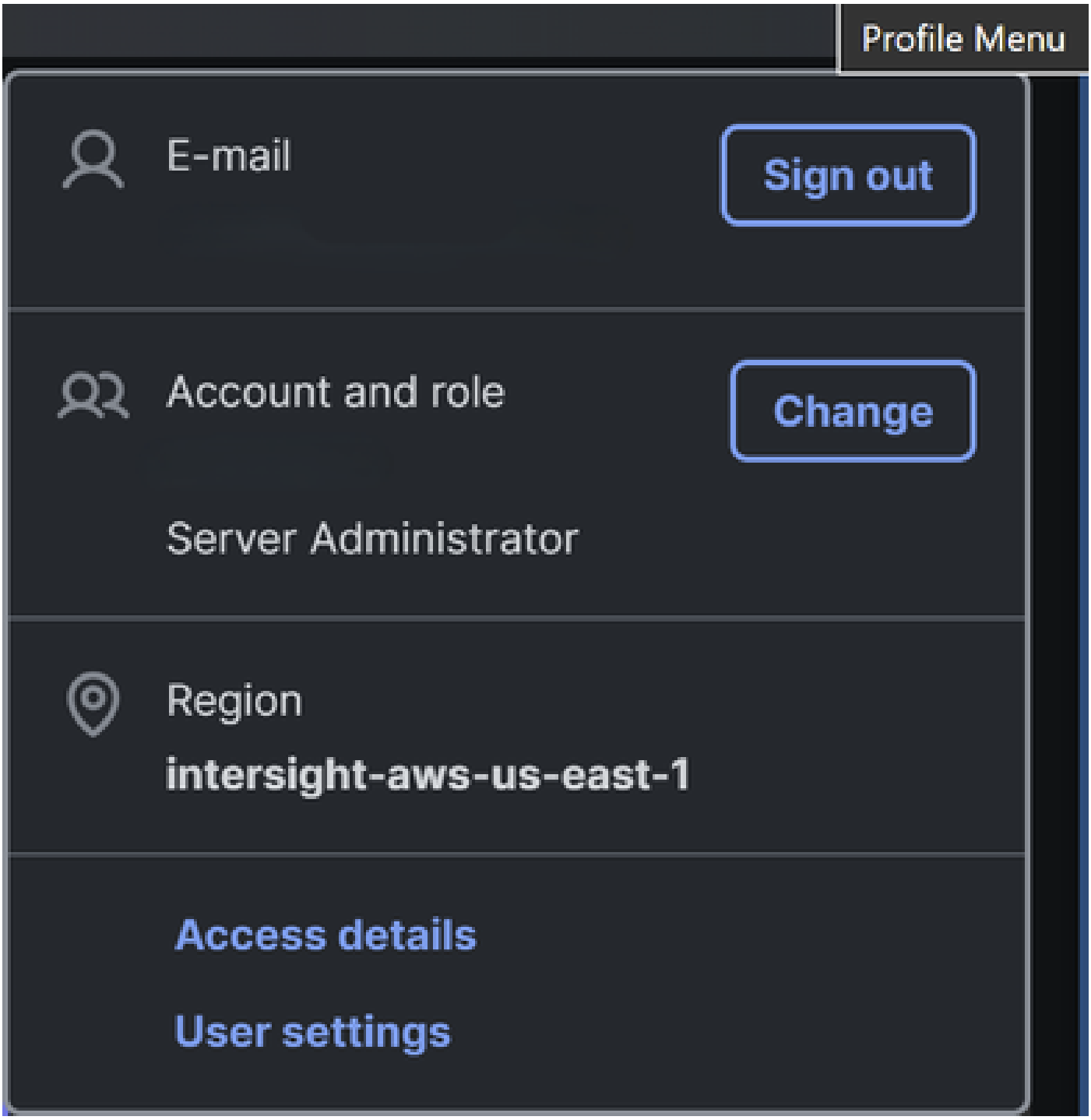
本文档介绍如何解决从Nutanix Foundation Central到Cisco Intersight的硬件提供商连接问题。

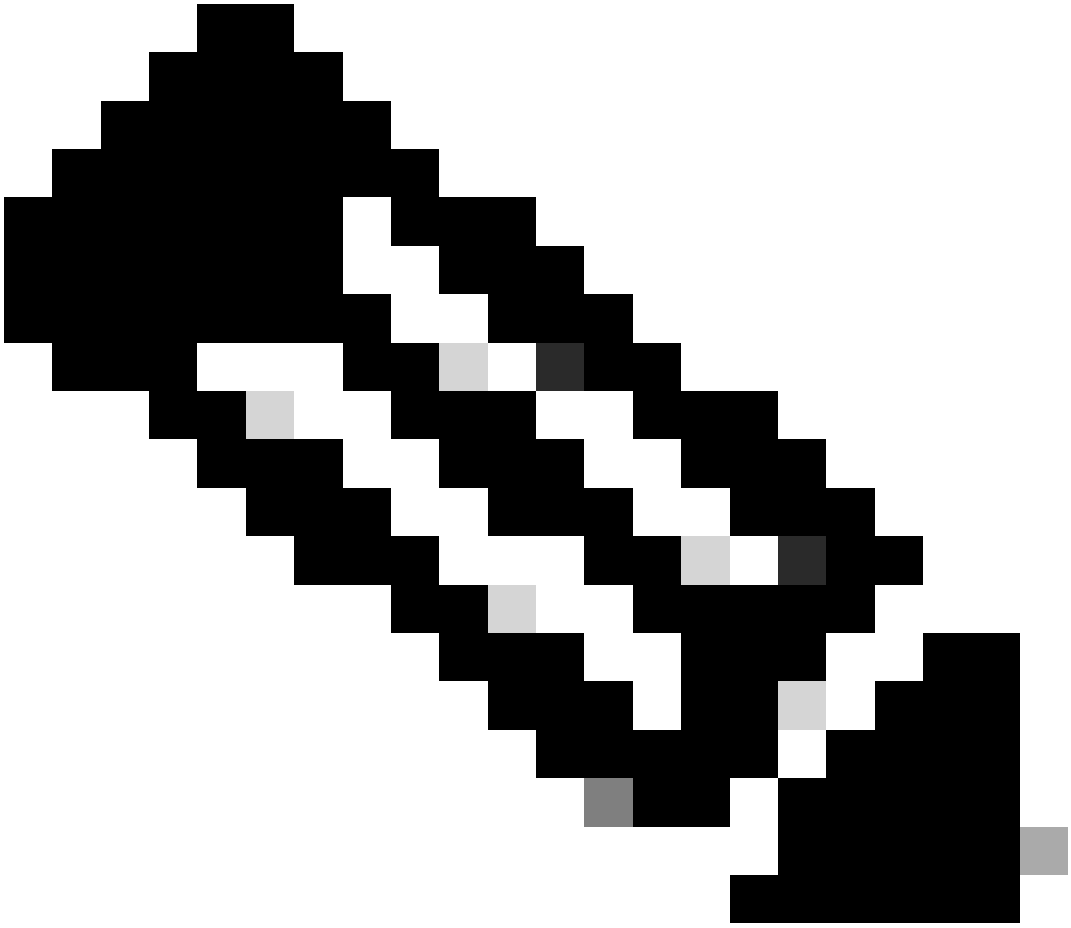
先决条件

要求

Cisco建议您了解这些主题。

- 基本了解网络连接。
- 基本了解Intersight API密钥。
- 至少具有Server Administrator权限的Intersight帐户。


Profile Menu
E-mail
Sign out
Account and role
Change
Server Administrator
Region
intersight-aws-us-east-1
Access details
User settings



注意：Intersight提供基于角色的访问控制(RBAC)，以根据用户角色和权限授权或限制对用户的系统访问。Intersight中的用户角色代表用户必须执行一组操作的权限集合，并提供对资源的精细访问。Intersight为单个用户或“组”下的一组用户提供基于角色的访问。

使用的组件

本文档中的信息基于以下软件和硬件版本：

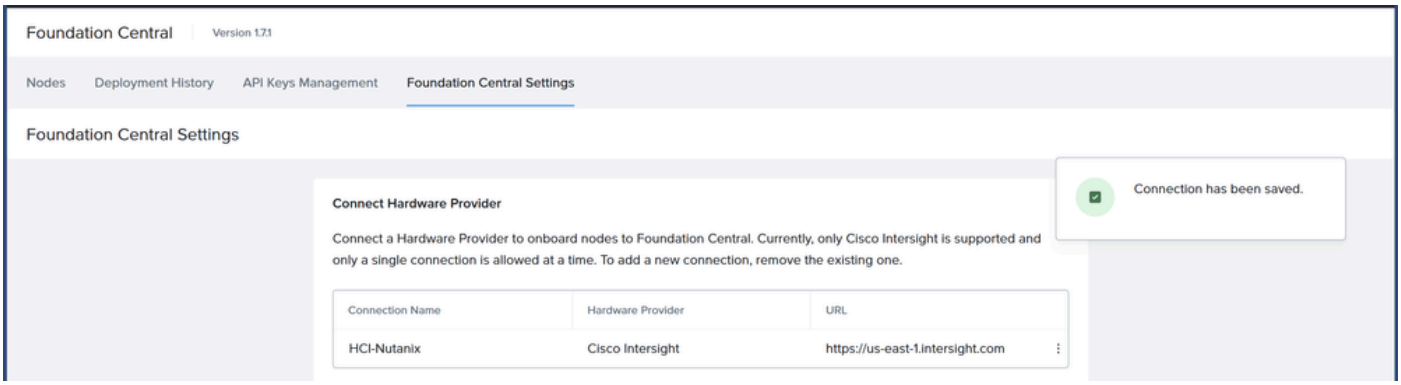
- Foundation Central 1.7.1或更高版本。
- Intersight SAAS、CVA和PVA。

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

需要将Foundation Central作为硬件提供商连接到Cisco Intersight，以便在Intersight独立模式ISM或

Intersight管理模式IMM中部署采用Nutanix解决方案的Cisco HCI。



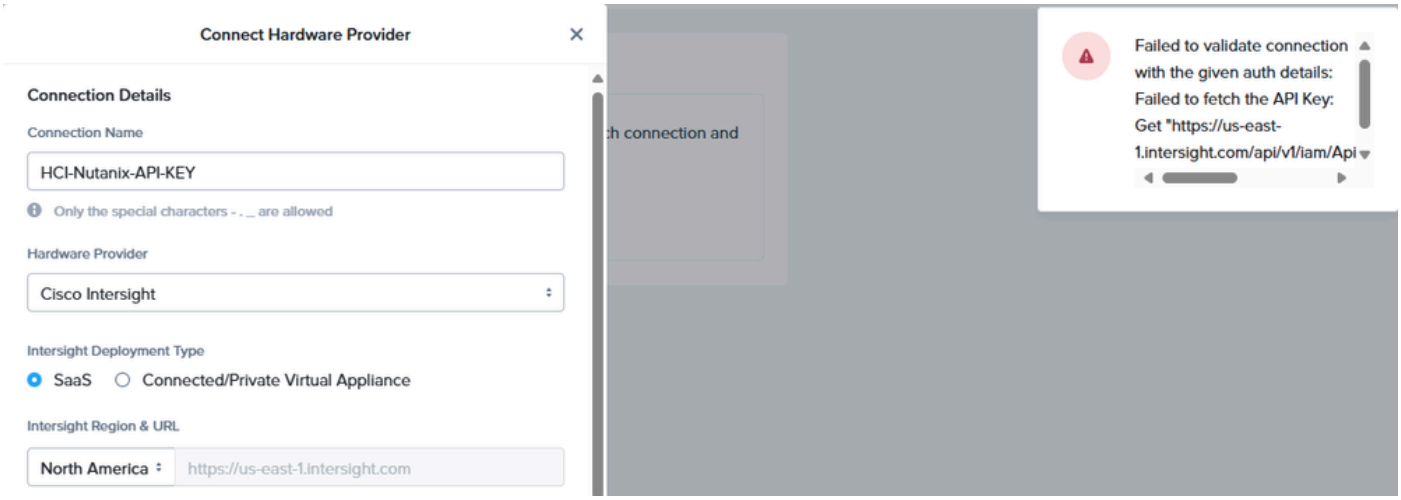
Intersight独立模式：节点连接到一对架顶式(ToR)交换机，服务器使用Cisco Intersight®进行集中管理。虽然部署标准Nutanix集群至少需要三个节点，但是我们还提供一个选项，用于为边缘和分支机构位置以及已安装高性能网络交换矩阵的情况部署单节点集群和双节点集群。

Intersight托管模式： Intersight托管模式将UCS系统的功能和Intersight基于云的灵活性统一起来，从而统一了独立系统和交换矩阵互联连接系统的管理体验。Intersight管理模型标准化了UCS-FI-6454、UCS-FI-64108、UCS-FI-6536、UCSX-S9108-100G交换矩阵互联和Cisco UCS C系列(M5、M6、M7、M8)和Cisco UCS X系列(M6、M7、M8)服务器的策略和操作管理。

故障排除

已超过情景截止时间

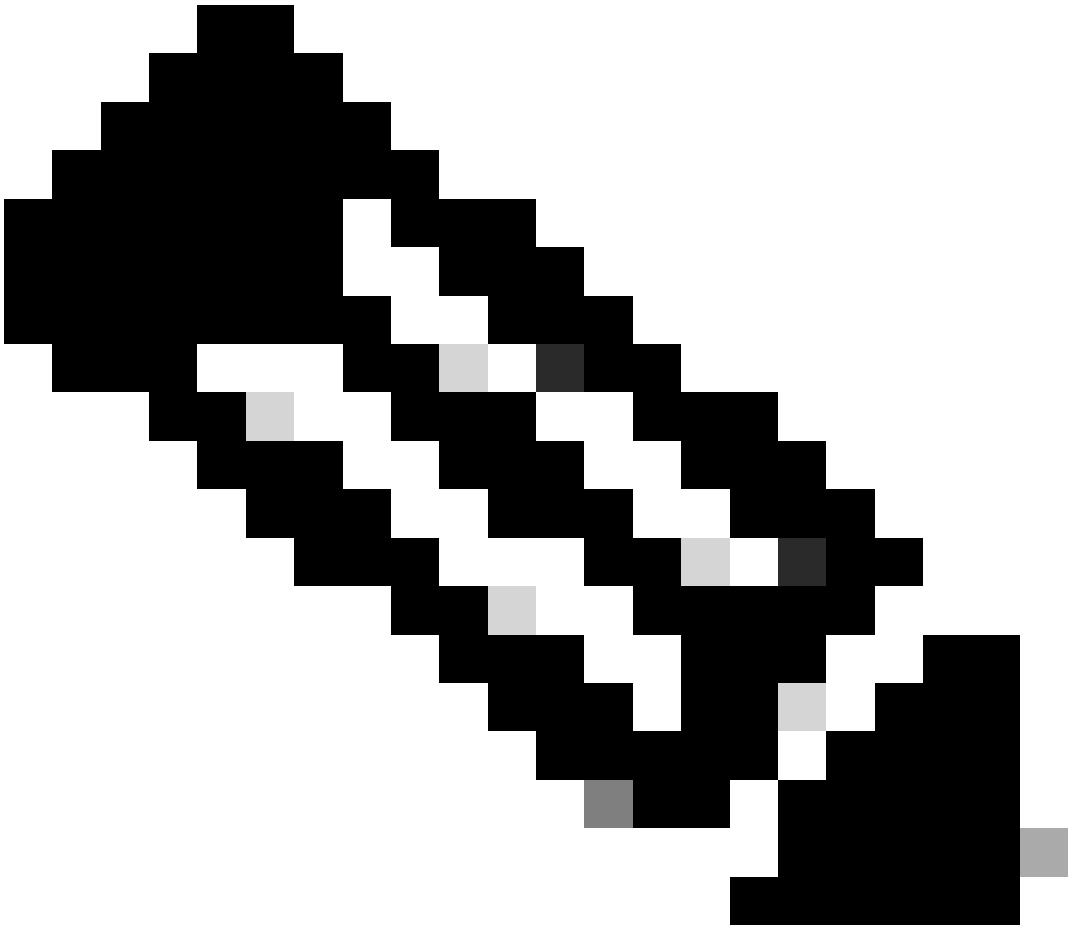
"验证与给定身份验证详细信息的连接失败：获取API密钥失败：已超过情景截止时间。"



确保从Prism Central和Foundation central通过端口443 TCP/UDP和80 TCP与下一个URL具有正确的连接。

地区	URL	设备连接器所需的URL
北美	intersight.com	svc.intersight.com

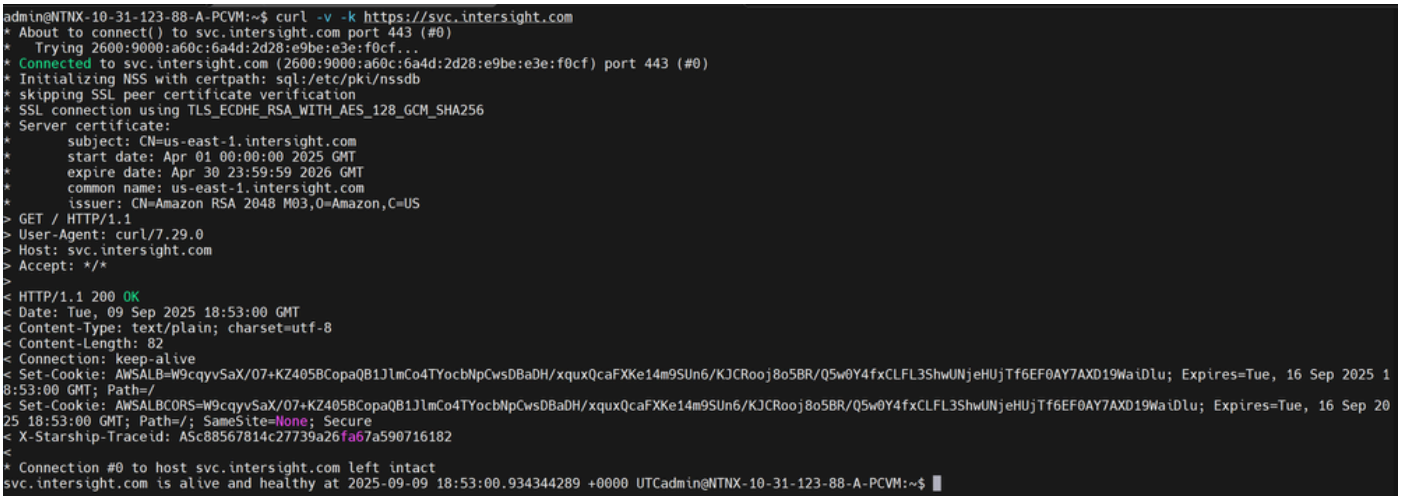
	us-east-1.intersight.com Ips: 52.223.48.112 99.83.178.202	svc.us-east-1.intersight.com svc-static1.intersight.com ucs-starship.com* ucs-connect.com*
欧洲、中东和非洲	Intersight.com eu-central-1.intersight.com Ips: 52.223.57.109 99.83.140.236	svc.eu-central-1.intersight.com svc-static1.eu-central-1.intersight.com



注意：Cisco Intersight支持两个地区：现有北美地区(us-east-1)和欧洲、中东和非洲(EMEA)地区(eu-central-1)。

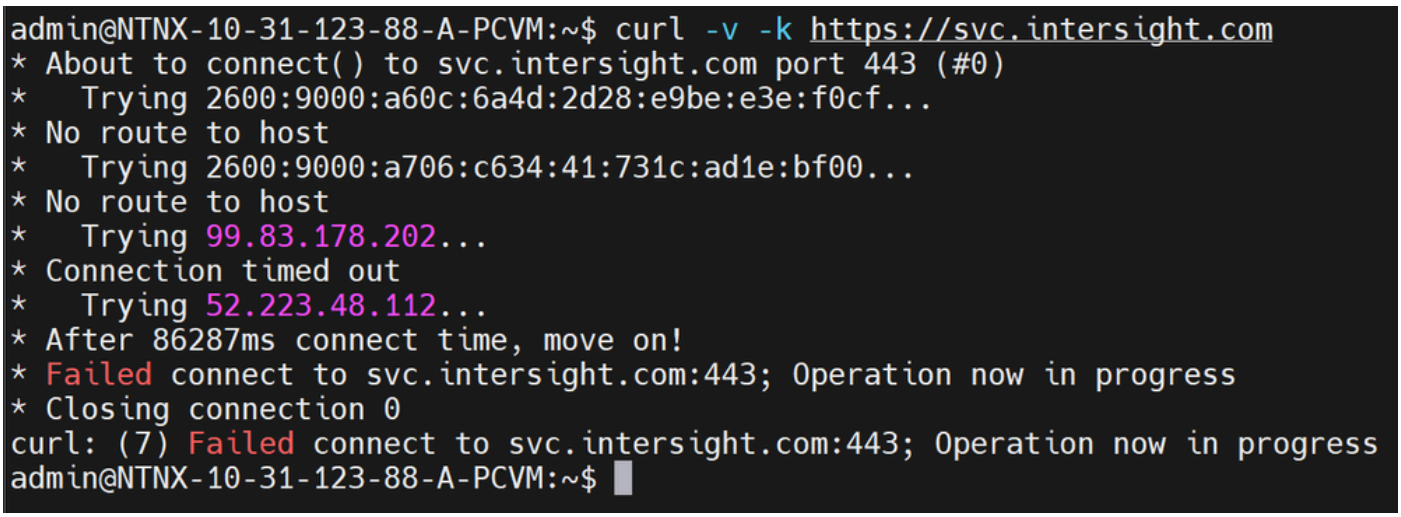
要验证之前的信息，请通过SSH连接到Prism Central或Foundation Central VM，并对上述URL和端口执行curl命令。

```
curl -v -k https://svc.intersight.com
```



成功卷曲连接测试。

如果curl命令失败，请向您的防火墙团队核实是否允许URL和端口进入防火墙或访问列表。



卷曲连接测试失败。

DNS正确名称解析

某些防火墙或访问列表需要从上述URL添加解析IP，这两个URL都会解析为以下IPv4和IPv6地址：

- 52.223.48.112

- 99.83.178.202
- 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
- 2600:9000:a706:c634:41:731c:ad1e:bf00

这可以通过使用nslookup命令进行验证。

```
nslookup svc.intersight.com
```

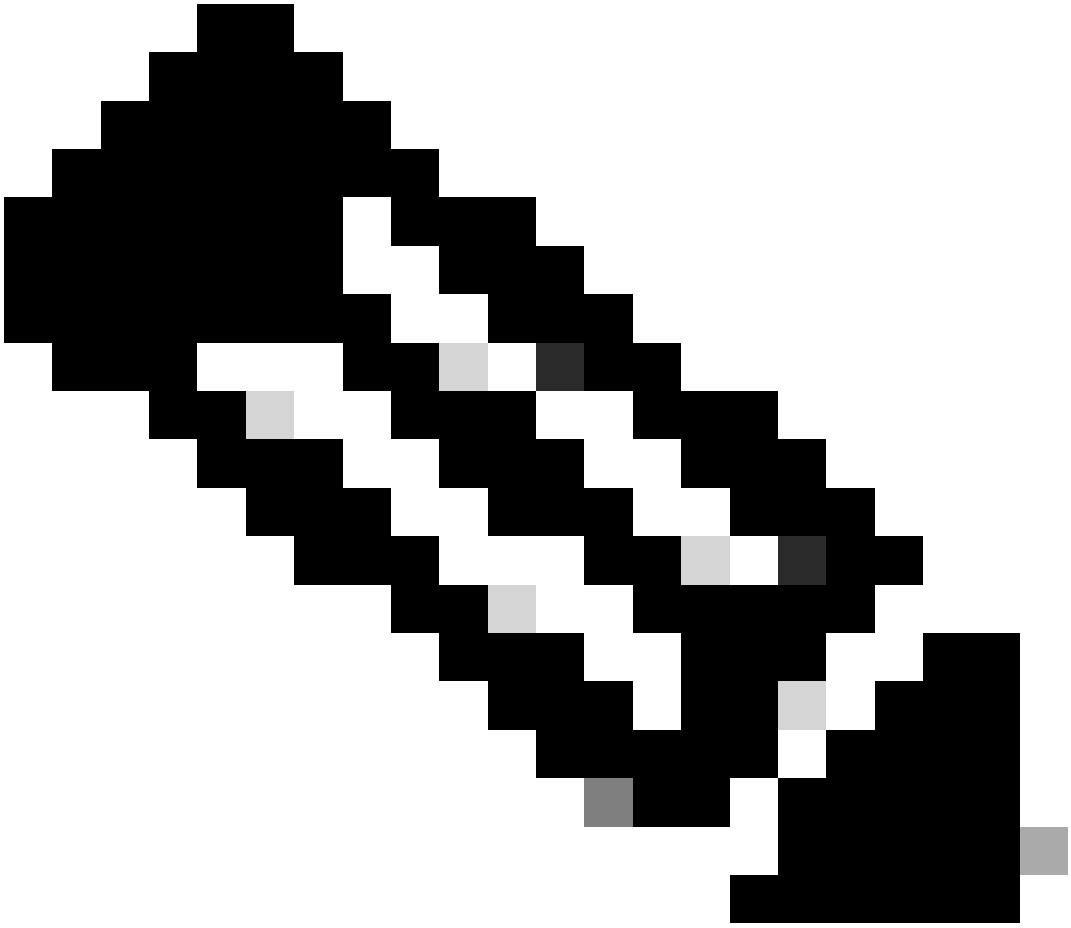
```
admin@NTNX-10-31-123-88-A-PCVM:~$ nslookup svc.intersight.com
Server:         10.31.123.60
Address:        10.31.123.60#53

Non-authoritative answer:
Name:   svc.intersight.com
Address: 52.223.48.112
Name:   svc.intersight.com
Address: 99.83.178.202
Name:   svc.intersight.com
Address: 2600:9000:a60c:6a4d:2d28:e9be:e3e:f0cf
Name:   svc.intersight.com
Address: 2600:9000:a706:c634:41:731c:ad1e:bf00

admin@NTNX-10-31-123-88-A-PCVM:~$
```

nslookup命令

Prism Central虚拟机无法连接到Intersight CVA/PVA

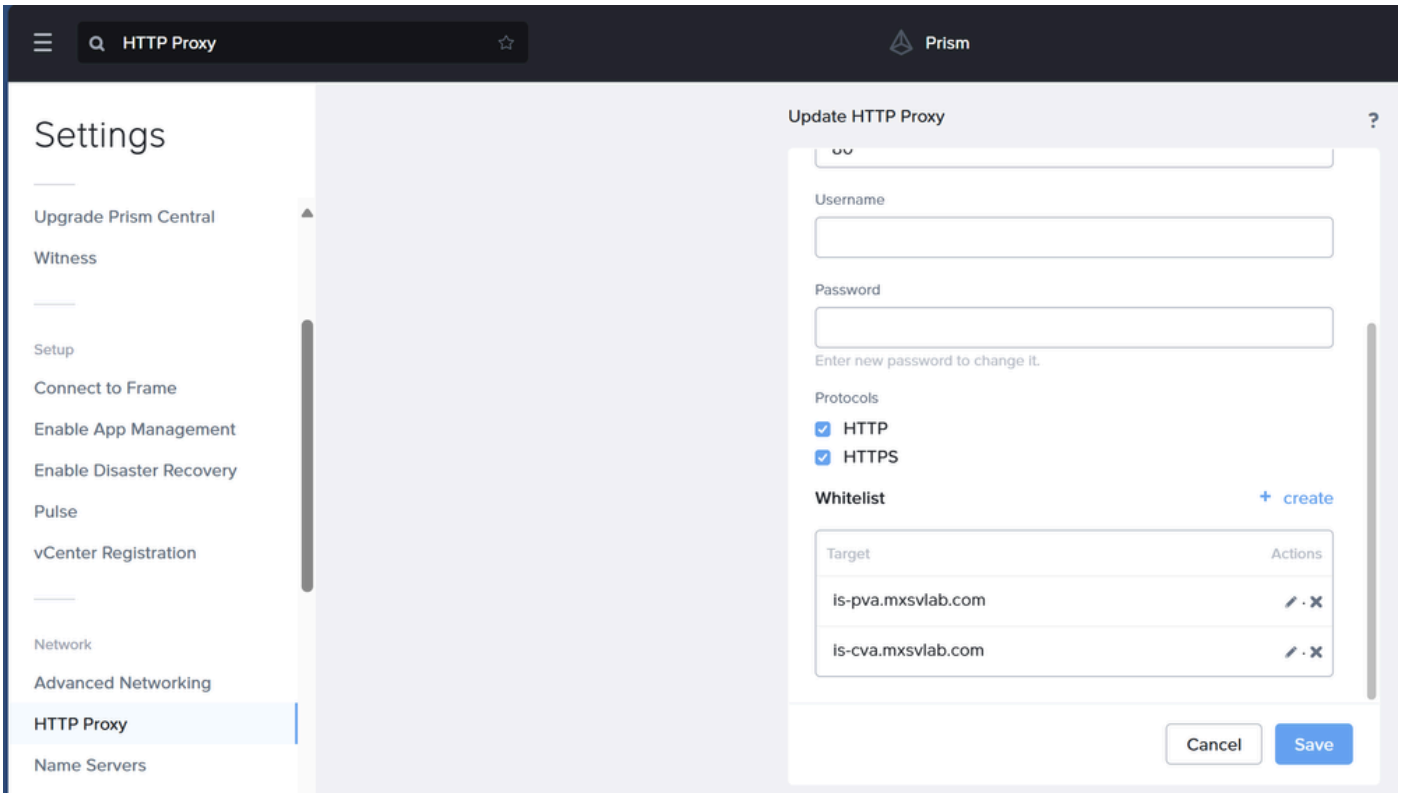
当从Prism Central直接连接到Intersight CVA/PVA时，请确保允许在端口443上连接。

如果PC VM具有配置为连接到互联网执行软件下载或LCM等任务的代理，您需要在Prism中央代理设置中将Intersight CVA/PVA FQDN和IP地址列入白名单。



注意：白名单条目是通过IP地址标识的单个主机或由网络地址和子网掩码标识的网络。添加白名单条目意味着“忽略此地址或网络的代理设置”。

要在Prism Central中更正此问题，请导航至：设置(Settings)>网络(Network)> HTTP代理(HTTP Proxy)>点击铅笔图标编辑(Edit)>白名单(Whitelist)。



HTTP 代理

您可以通过使用curl命令测试与Intersight CVA/PVA的连接来确认这些步骤是否成功。

```
curl -v -k https://is-pva.mxsvlab.com
```

```
                                                curl -v -k https://is-pva.mxsvlab.com
*   Trying            :443...
* Connected to is-pva.mxsvlab.com (           ) port 443
* ALPN: curl offers http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN: server accepted http/1.1
```

卷曲试验

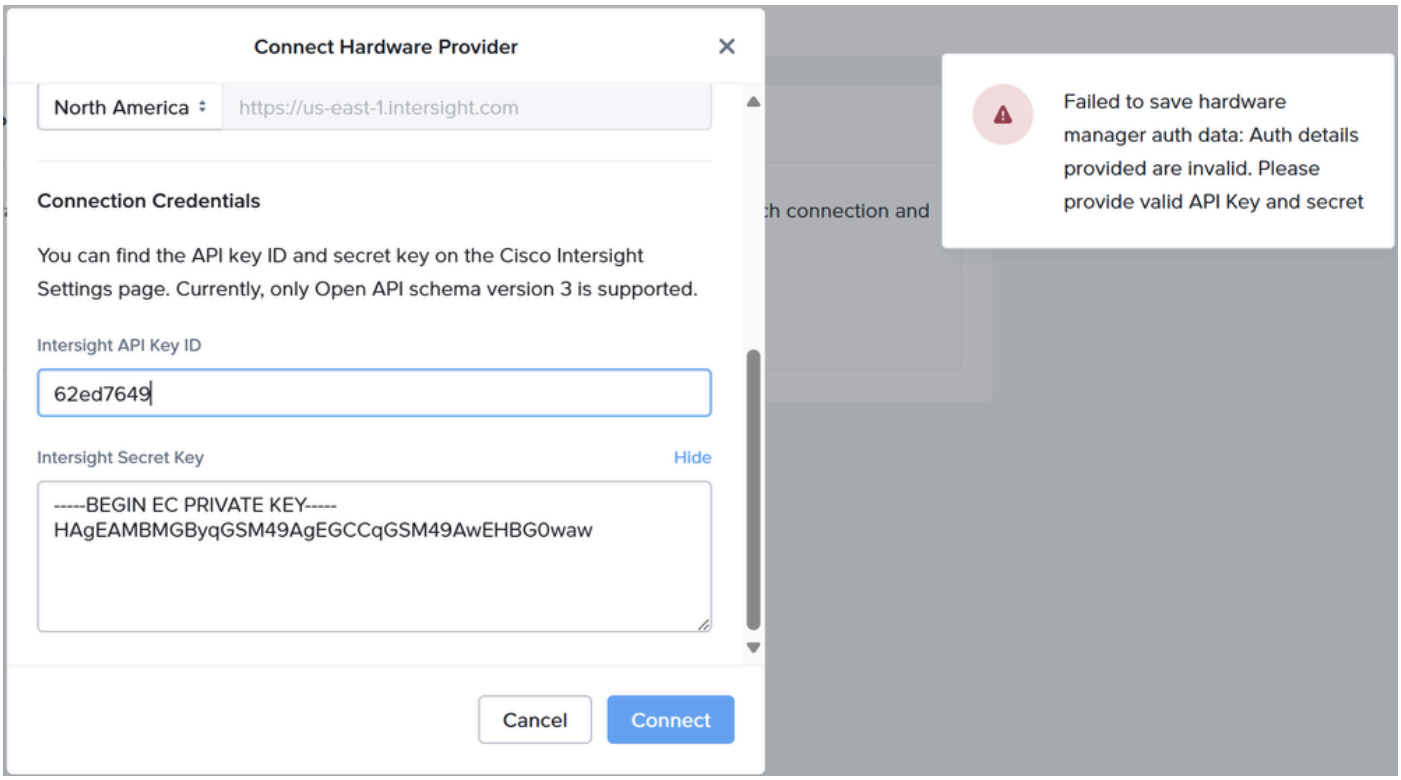
用于测试连通性的Network命令

命令	描述

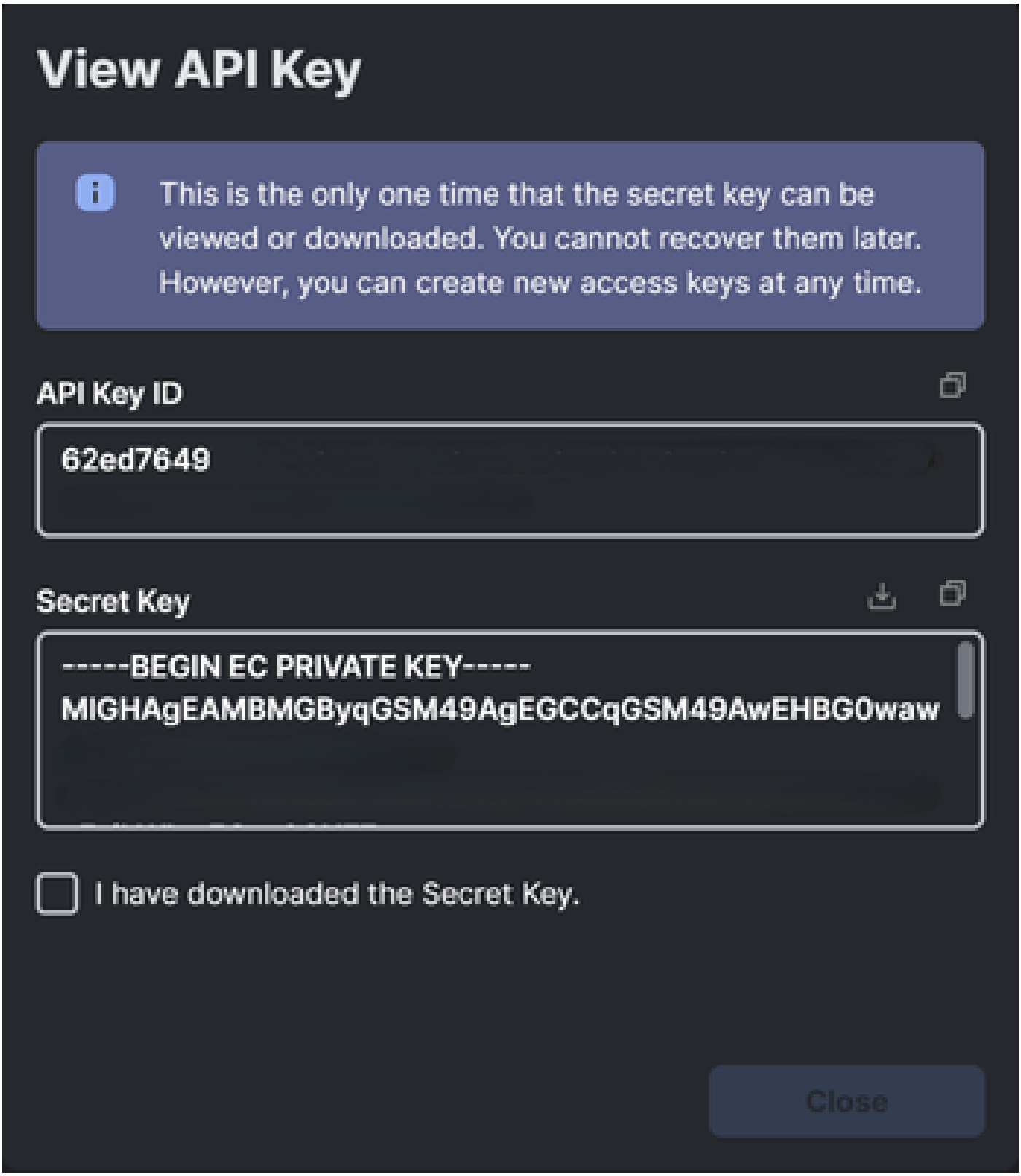
curl -v -k https://<Intersight URL> curl -v -k https://svc.intersight.com	测试通向Intersight所需URL的连接
curl -v -k —proxy <proxy address>:<port> <Intersight URL> curl -v -k -proxy http://proxy.esl.cisco.com:8080 https://svc.intersight.com	在需要代理时测试连接
curl -4|6 -v -k https://<Intersight URL> curl -4 -v -k https://svc.intersight.com	指定到IPV4或IPV6编址的连接测试
tracepath <Intersight IP> tracepath 99.83.178.202	跟踪通往目的主机的数据包
nslookup <URL> nslookup svc.Intersight.com	确定与特定地址关联的IP地址

提供的身份验证详细信息无效

“无法保存硬件管理器身份验证数据：提供的身份验证详细信息无效。请提供有效的API密钥和密钥。"

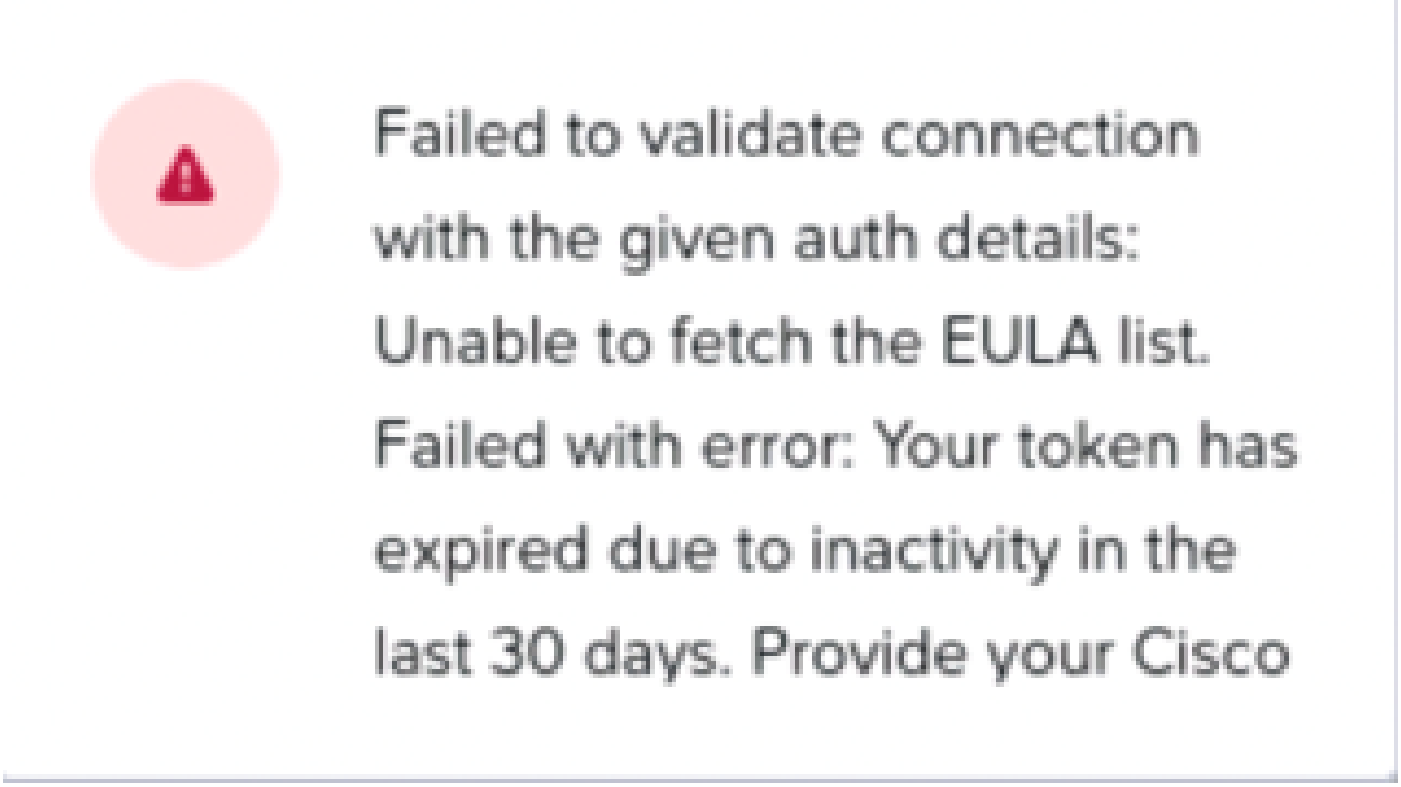


在键入或粘贴Intersight密钥时，您需要确认没有输入错误或缺少字符，否则将无法与硬件提供商建立连接。

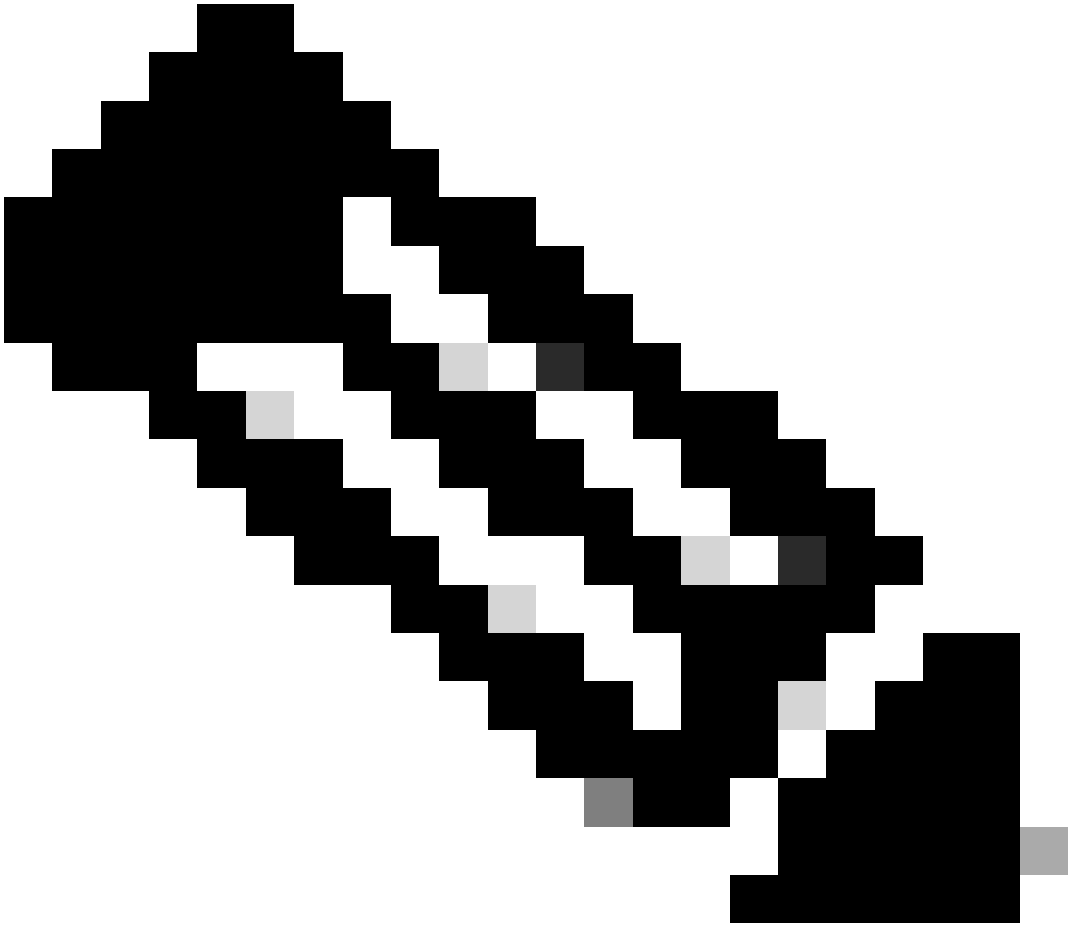


无法获取EULA列表

"验证与给定身份验证详细信息的连接失败：无法获取EULA列表。失败，错误为：由于在过去30天内处于非活动状态，您的令牌已过期。”

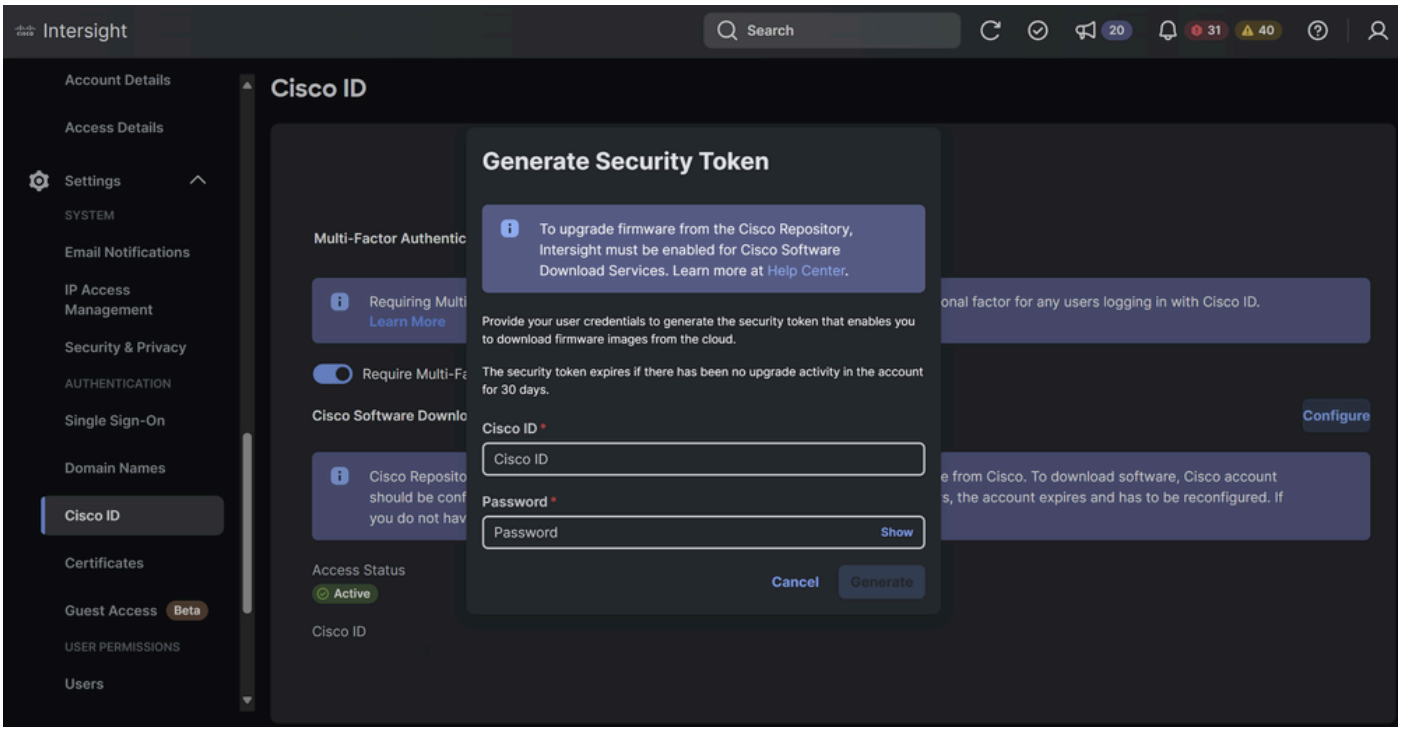


在节点自注册阶段，您可能会遇到错误“无法使用UUID连接到INTERSIGHT硬件管理器”或“您的用户凭证可能已过期”。 如果EULA存在Intersight帐户问题，则会显示此消息。



注意：从今日起，ISM必须接受EULA。将来这种情况会有所改变，因为我们不再依赖EULA下载固件。

要在Intersight中更正此问题，请导航至：设置(Settings)>思科ID(Cisco ID)>配置(Configure)>输入思科ID和密码(Cisco ID and Password)。



相关信息

- Intersight中的组织和角色
- 端口要求
- 声明目标所需的终端URL
- 授予思科软件存储库访问权限并接受EULA

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）。