对于SDA和非SDA网络方案，从Cisco Catalyst Center更改有线和无线设备的设备凭证

目录

简介

本文档介绍交换矩阵和非交换矩阵网络场景下有线和无线设备的Cisco Catalyst Center（以前称为Cisco DNA Center）凭证更改过程的步骤。

背景信息

本文档也适用于具有动态网络访问控制(Cisco Catalyst Center)托管或非托管身份验证、授权和记帐(AAA)的站点。

概述

本文档讨论需要网络更新Cisco Catalyst Center用于自动化的凭证的情况。 受管设备由Cisco Catalyst Center使用用户名和密码发现，Cisco Catalyst Center使用这些凭证与受管设备进行SSH连接（用于自动化/资产收集等）。本文档介绍在Cisco Catalyst Center发现受管设备后更改其密码的最佳实践。

解决方案（最佳实践）

要求

1. 对于使用Cisco Catalyst Center托管AAA的站点

- 要求是更改用户的密码（不更改使能密码）。
- 要求是更改用户的口令和使能口令。

2. 对于具有Cisco Catalyst Center非托管AAA的站点

- 要求是更改用户的密码（不更改使能密码）。
- 要求是更改用户的口令和使能口令。

前提条件

- 确保未在Cisco Catalyst Center中为所有非SDA站点配置AAA。
- 使用Python脚本验证所有Catalyst 9k交换机（SDA或非SDA）是否使用RADIUS到ISE进行SSH登录到VTY线路。修复使用本地凭证的所有设备。
- 对于扩展节点
    - 要更新线路vty 0到4，请使用以下配置命令（这可能是扩展节点的第一步）。

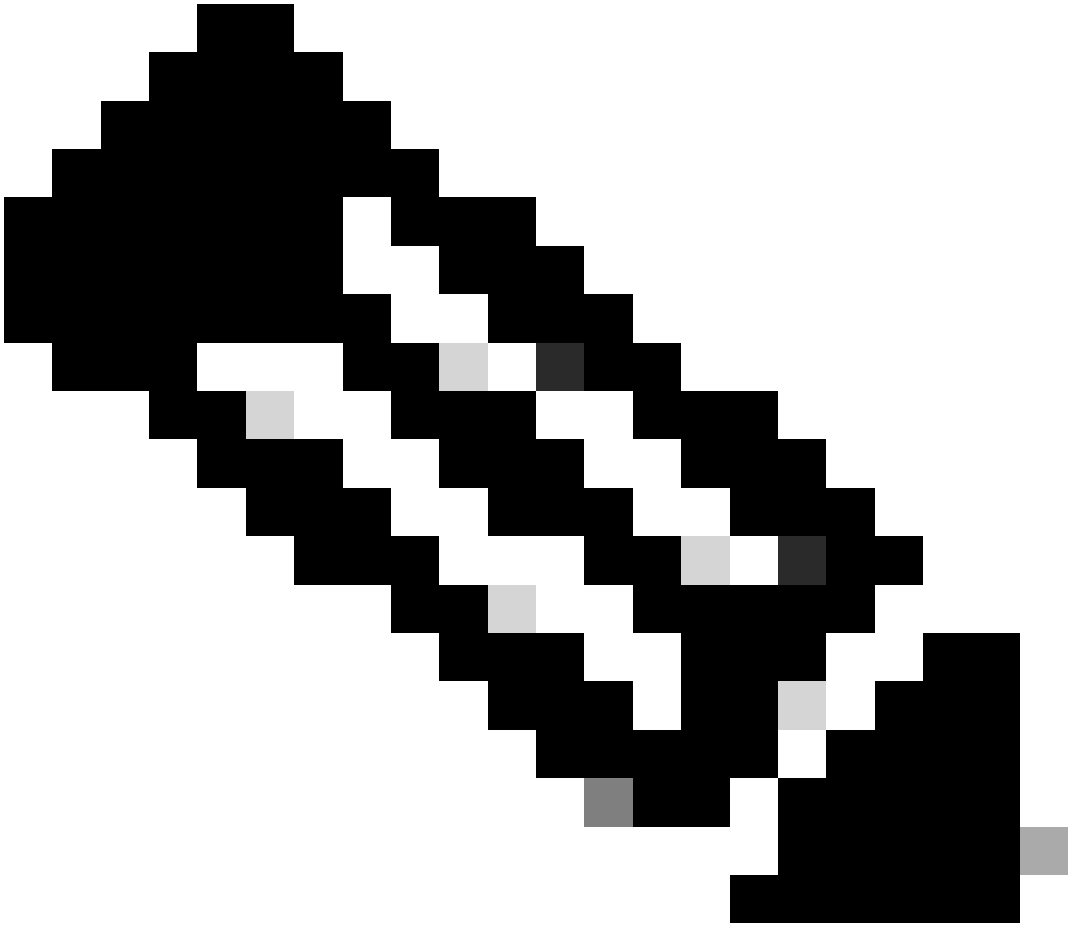
```
line vty 0 4
authorization exec VTY_author
login authentication VTY_authen
```

从Cisco Catalyst Center更改凭据的过程

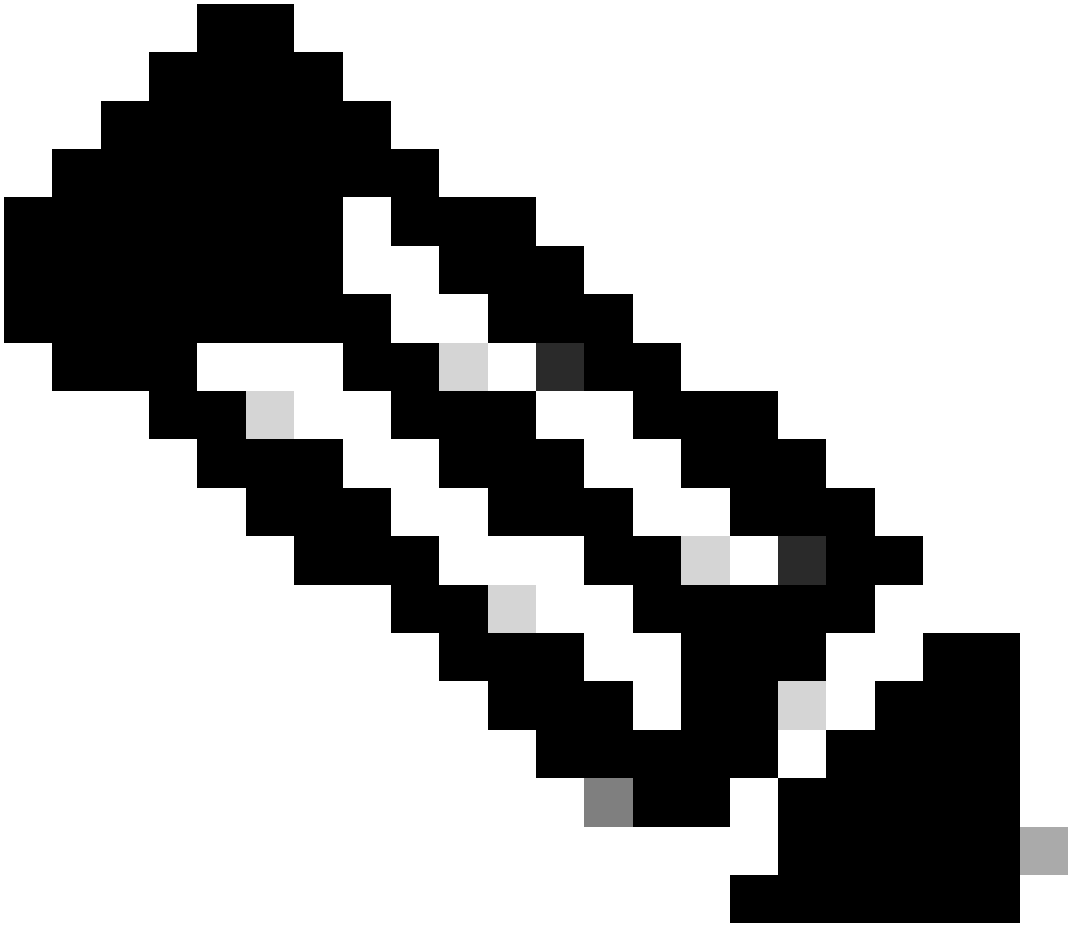
具有Cisco Catalyst Center托管AAA的站点

要求更改用户的密码（不更改使能密码）

1. 首先更新ISE中的凭据（相关用户名的密码）。这将导致资产收集失败，受管设备资产状态将更改为“无法访问”、“部分收集失败”或“凭证错误”。
2. 在Provision > Inventory页面上，选择一个或多个设备并选择Actions > Inventory > Edit Device > Credentials选项卡。然后，使用新的用户名和/或密码（保留相同的启用密码）更新“添加设备特定凭证”。此时，Cisco Catalyst Center将能够使用更新的凭证登录设备，设备资产状态将返回到“托管”。
3. 设备的本地凭证可更新为回退，以确保Cisco Catalyst Center能够在无法访问外部AAA服务器时登录到设备。可以使用Cisco Catalyst Center的模板编辑器、自定义Python脚本或手动更新本地凭证。
4. 最后一步是在Global Credentials页面上更新这些相同的凭证。 这可确保新发现的设备或使用LAN自动化添加的设备使用更新的凭据。这些凭据来自“设计”页面>“网络设置”>“设备凭据”>“CLI凭据”>“编辑用户名”>“更新用户密码”，而不更改启用密码。



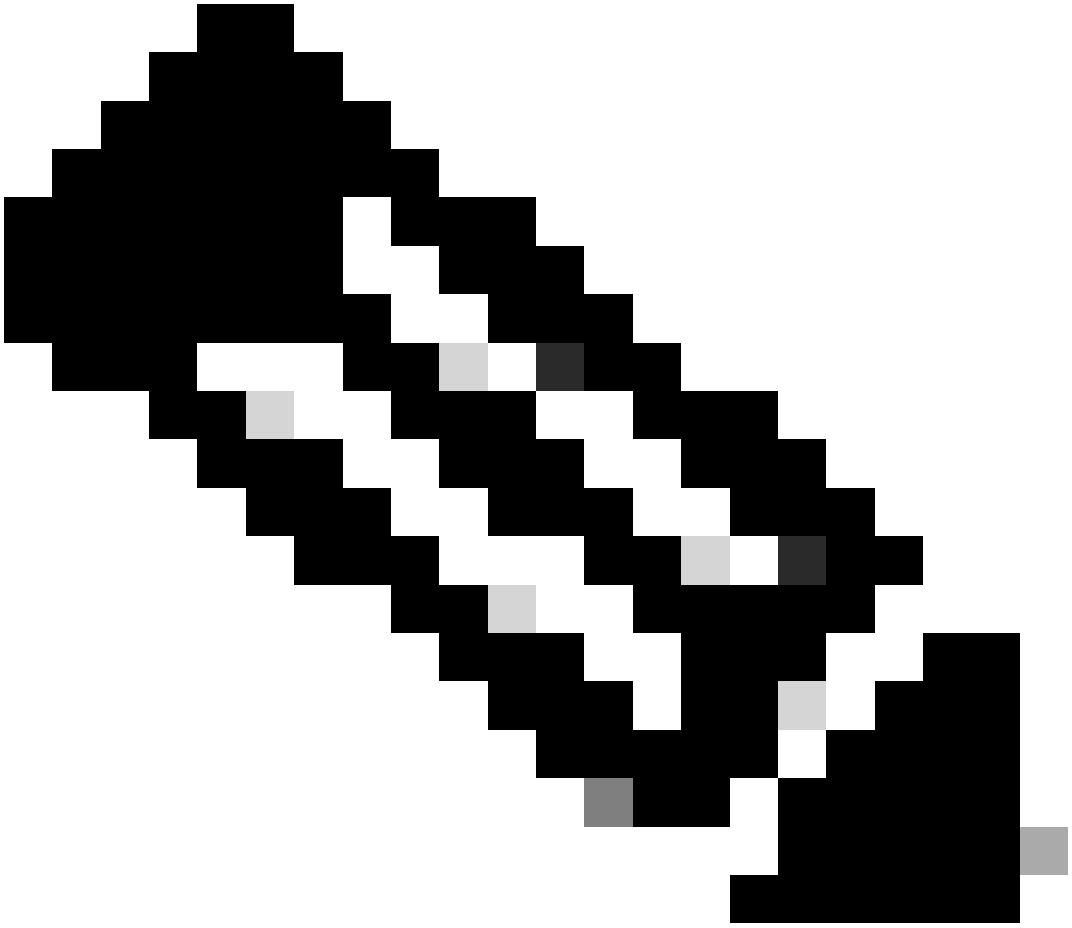
注意：SSH/Telnet登录由外部AAA服务器进行身份验证。 本地设备凭证未更新。



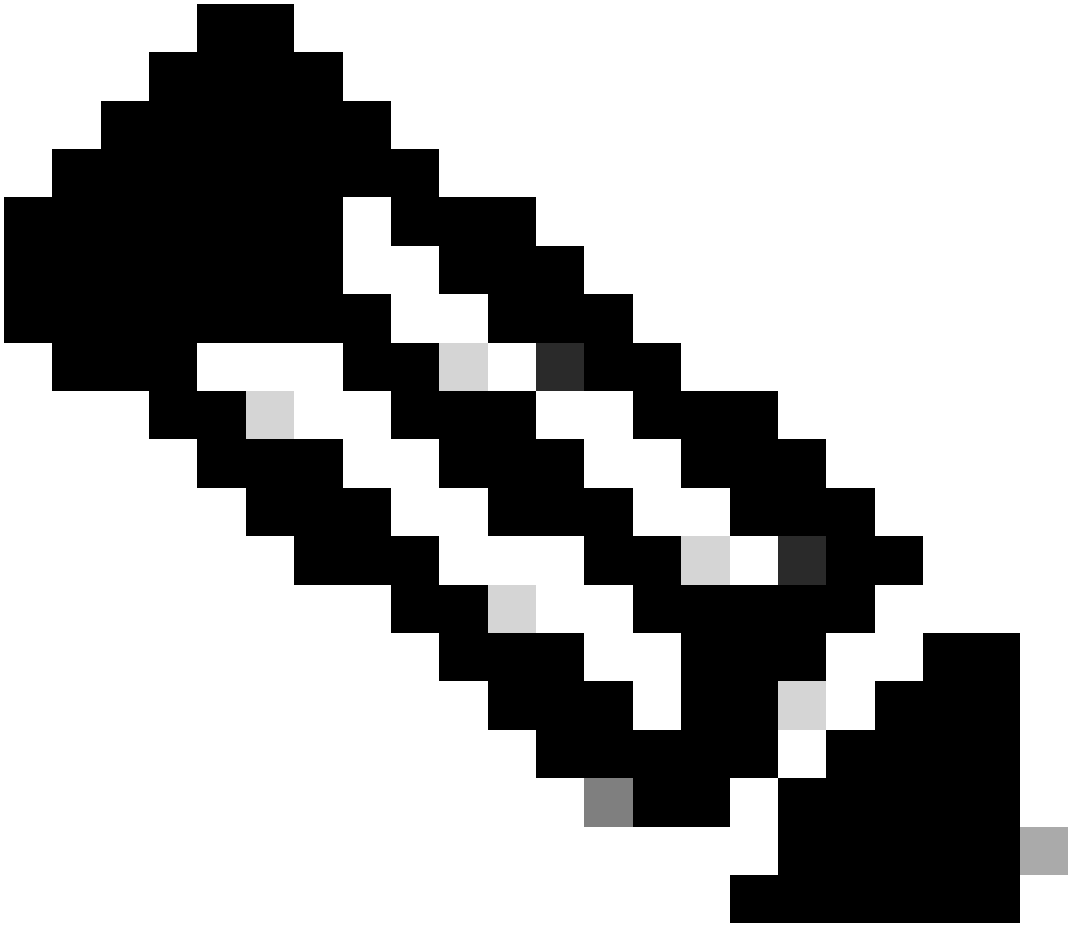
注意：在Cisco Catalyst Center的“设计”页面上为站点配置外部AAA服务器时，当您更改/修改“全局凭证”(Global Credentials)页面上的凭证时，Cisco Catalyst Center不会对受管设备或ISE采取任何操作。

要求是更改用户的口令和使能口令

1. 首先更新ISE中的凭据（相关用户名的密码）。这将导致资产收集失败，受管设备资产状态将更改为“无法访问”、“部分收集失败”或“凭证错误”。
2. 在Provision > Inventory页面上，选择一个或多个设备并选择Actions > Inventory > Edit Device > Credentials选项卡。然后，使用新的用户名和/或密码以及启用密码更新“添加设备特定凭证”。此时，Cisco Catalyst Center将能够使用更新的凭证登录设备，设备资产状态将返回到“托管”。
3. 最后一步是在Global Credentials页面上更新这些相同的凭证。 这可确保新发现的设备或使用LAN自动化添加的设备使用更新的凭据。这些凭据来自“设计”页面>“网络设置”>“设备凭据”>“CLI凭据”>“编辑用户名”>“更新用户的密码和启用密码”。



注意：当可访问外部AAA服务器时，用户名和密码由外部AAA服务器进行身份验证，启用密码由受管设备在本地进行身份验证。

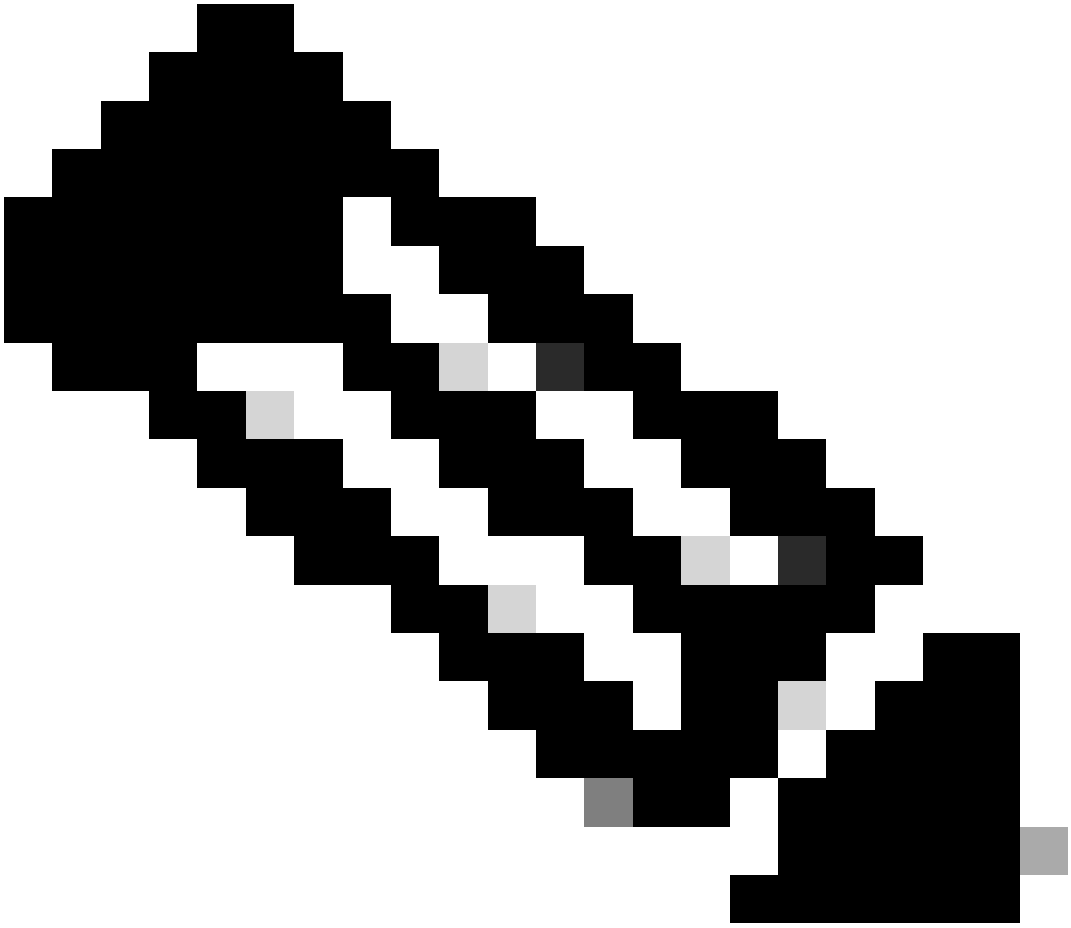


注意：在Cisco Catalyst Center的“设计”页面上为站点配置外部AAA服务器时，当您在“全局凭证”(Global Credentials)页面上更改或修改凭证时，Cisco Catalyst Center不会对设备或ISE执行任何操作。

具有Cisco Catalyst Center非托管AAA的站点

要求更改用户的密码（不更改使能密码）

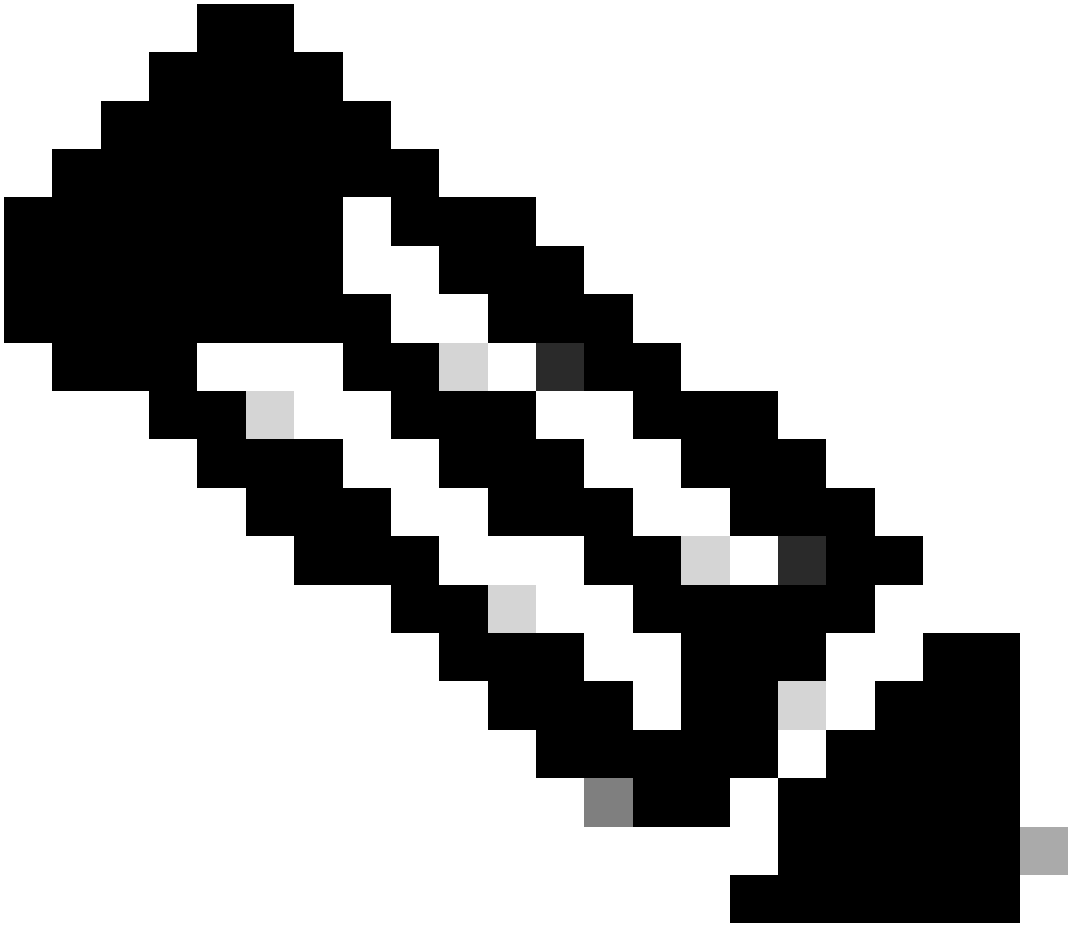
1. 在“全局凭证”(Global Credentials)页面上更新凭证，路径为：设计(Design) >网络设置(Network Settings) >设备凭证(Device Credentials) > CLI凭证(CLI Credentials) >编辑用户名(edit the username) >更新用户密码(update the user’s password)，而无需更改启用密码(enable password)。
2. 在Global Credentials页面上修改凭证后，Cisco Catalyst Center未管理AAA的站点的受管设备可以使用更新的凭证重新配置。 Cisco Catalyst Center可以推送临时EEM脚本以验证凭证。如果登录成功，则可保留配置。



注意：对于Cisco Catalyst Center未管理AAA配置的站点的受管设备，Cisco Catalyst Center对于是否使用外部AAA服务器手动配置受管设备或受管设备是否仅使用本地凭证没有任何了解，因此，如果在受管设备上配置了密码，请确保在继续执行以下步骤之前在外部AAA服务器上更新该密码。

要求是更改用户的口令和使能口令

1. 在“全局凭证”(Global Credentials)页面上更新凭证，该页面位于“设计”(Design) >“网络设置”(Network Settings) >“设备凭证”(Device Credentials) >“CLI凭证”(CLI Credentials) >“编辑用户名”(edit the username) >“更新用户的密码”(update the user’s password)以及“启用密码”(enable password)。
2. 在Global Credentials页面上修改凭证后，Cisco Catalyst Center未管理AAA的站点的受管设备可以使用更新的凭证重新配置。 Cisco Catalyst Center可以推送临时EEM脚本以验证凭证。如果登录成功，则可保留配置。



注意：对于Cisco Catalyst Center未管理AAA配置的站点的受管设备，Cisco Catalyst Center对于是否使用外部AAA服务器手动配置受管设备或受管设备是否仅使用本地凭证没有任何了解，因此，如果在受管设备上配置了密码，请确保在继续执行以下步骤之前在外部AAA服务器上更新该密码。

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）。