

從Cisco Catalyst Center為SDA和非SDA網路場景中的有線和無線裝置更改裝置憑證

目錄

[簡介](#)

[背景資訊](#)

[簡要說明](#)

[解決方案 \(最佳實踐\)](#)

[需求](#)

[前提條件](#)

[從Cisco Catalyst Center更改憑據的過程](#)

[具有Cisco Catalyst Center託管AAA的站點](#)

[要求更改使用者的密碼 \(不更改使能密碼\)](#)

[要求更改使用者的密碼和使能密碼](#)

[具有Cisco Catalyst Center未託管AAA的站點](#)

[要求更改使用者的密碼 \(不更改使能密碼\)](#)

[要求更改使用者的密碼和使能密碼](#)

簡介

本文檔介紹來自Cisco Catalyst Center (以前稱為Cisco DNA Center) 的憑證更改過程的步驟，適用於交換矩陣和非交換矩陣網路方案的有線和無線裝置。

背景資訊

本檔案也適用於具有動態網路存取控制(Cisco Catalyst Center)代管或非代管驗證、授權和計量(AAA)的站點。

簡要說明

本文討論更新Cisco Catalyst Center用於自動化的憑證時存在網路要求的情況。Cisco Catalyst Center使用使用者名稱和密碼發現受管裝置，Cisco Catalyst Center使用這些相同的憑證與受管裝置進行SSH連線 (用於自動化/資產收集等)。本文檔介紹在Cisco Catalyst Center發現受管裝置後更改其密碼的最佳實踐。

解決方案 (最佳實踐)

需求

1. 適用於使用Cisco Catalyst Center託管AAA的站點

- 要求更改使用者的密碼 (不更改使能密碼) 。
- 要求更改使用者的密碼和使能密碼。

2. 適用於具有Cisco Catalyst Center未託管AAA的站點

- 要求更改使用者的密碼 (不更改使能密碼) 。
- 要求更改使用者的密碼和使能密碼。

前提條件

- 確保未在Cisco Catalyst Center中為所有非SDA站點配置AAA。
- 使用Python指令碼驗證所有Catalyst 9k交換機 (SDA或非SDA) 是否使用RADIUS到ISE進行SSH登入到VTY線路。修復使用本地憑據的所有裝置。
- 對於擴展節點
 - 要更新線路vty 0到4，請使用這些配置命令 (這可能是擴展節點的第一步) 。

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

從Cisco Catalyst Center更改憑據的過程

具有Cisco Catalyst Center託管AAA的站點

要求更改使用者的密碼 (不更改使能密碼)

1. 首先更新ISE中的憑據 (相關使用者名稱的密碼) 。這將導致清單收集失敗，受管裝置清單狀態將更改為「無法訪問」、「部分收集失敗」或「錯誤憑據」。
2. 在Provision > Inventory頁面上，選擇一個或多個裝置，然後選擇Actions > Inventory > Edit Device > Credentials頁籤。接下來，使用新的使用者名稱和/或密碼 (保留相同的啟用密碼) 更新「新增裝置特定憑據」。此時，Cisco Catalyst Center將能夠使用更新的憑證登入裝置，裝置清單狀態將返回到「託管」。
3. 可以將裝置的本地憑證更新為回退，以確保Cisco Catalyst Center能夠在外部AAA伺服器無法訪問時登入到裝置。本地憑證可使用Cisco Catalyst Center的模板編輯器、自定義Python指令碼或手動進行更新。
4. 最後一步是在「全域性身份證明」頁上更新這些相同的身份證明。這可確保新發現的使用LAN Automation新增的裝置或裝置將使用Design (設計) 頁> Network Settings (網路設定) > Device Credentials (裝置憑證) > CLI Credentials (CLI憑證) >編輯使用者名稱>更新使用者密碼而不更改啟用密碼。



注意:SSH/Telnet登入由外部AAA伺服器進行身份驗證。 本地裝置憑據未更新。

注意：在Cisco Catalyst Center的「設計」頁面上為站點配置外部AAA伺服器時，當您更改/修改「全域性憑證」頁面上的憑證時，Cisco Catalyst Center不會對受管裝置或ISE採取任何操作。

要求更改使用者的密碼和使能密碼

1. 首先更新ISE中的憑據（相關使用者名稱的密碼）。這將導致清單收集失敗，受管裝置清單狀態將更改為「無法訪問」、「部分收集失敗」或「錯誤憑據」。
2. 在Provision > Inventory頁面上，選擇一個或多個裝置，然後選擇Actions > Inventory > Edit Device > Credentials頁籤。接下來，使用新的使用者名稱和/或密碼以及啟用密碼更新「新增裝置特定憑據」。此時，Cisco Catalyst Center將能夠使用更新的憑證登入裝置，裝置清單狀態將返回到「託管」。
3. 最後一步是在「全域性身份證明」頁上更新這些相同的身份證明。這可確保新發現的使用LAN Automation新增的裝置或裝置將使用Design（設計）頁> Network Settings（網路設定）> Device Credentials（裝置憑證）> CLI Credentials（CLI憑證）>編輯使用者名稱>更新使用者密碼和啟用密碼中的更新憑證。



注意：當外部AAA伺服器可訪問時，使用者名稱和密碼由外部AAA伺服器進行身份驗證，使能密碼由受管裝置在本地進行身份驗證。

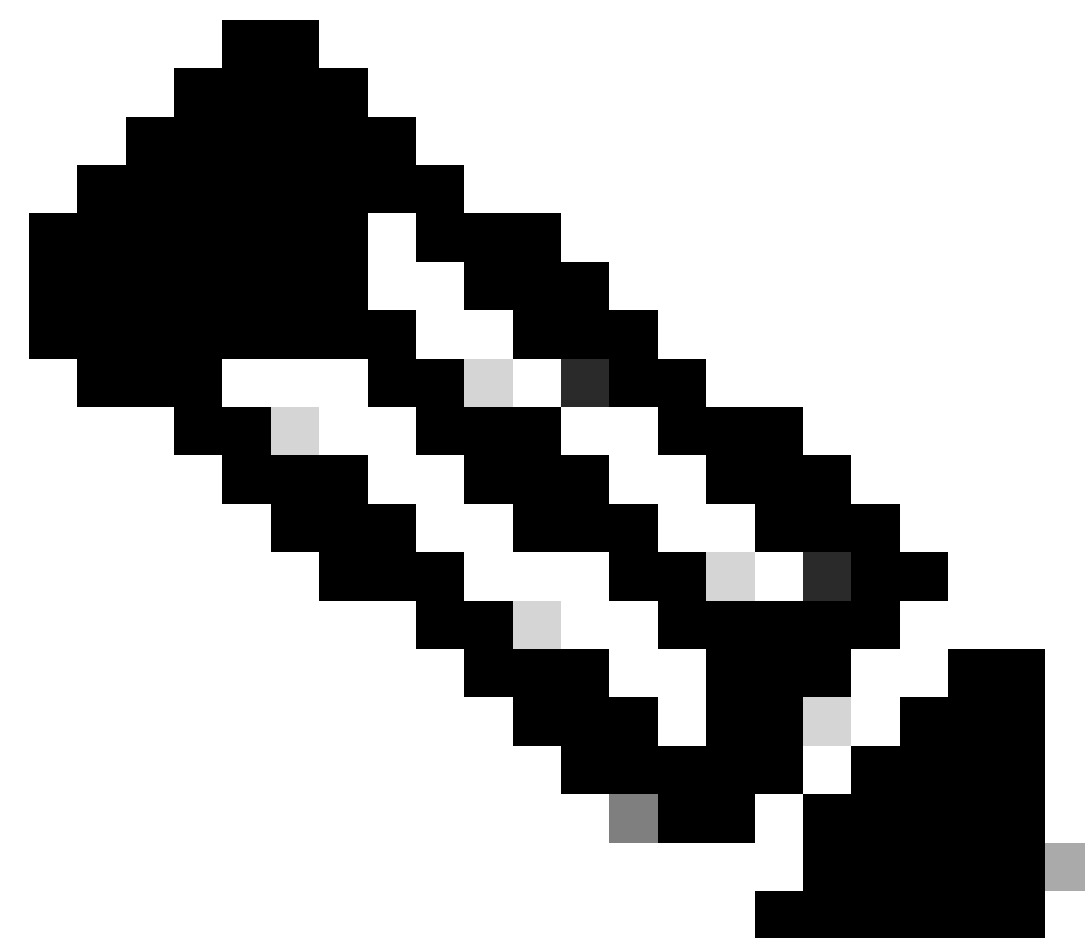


注意：在Cisco Catalyst Center的「設計」頁面上為站點配置外部AAA伺服器時，當您在「全域性憑證」頁面上更改或修改憑證時，Cisco Catalyst Center不會對裝置或ISE採取任何操作。

具有Cisco Catalyst Center未託管AAA的站點

要求更改使用者的密碼（不更改使能密碼）

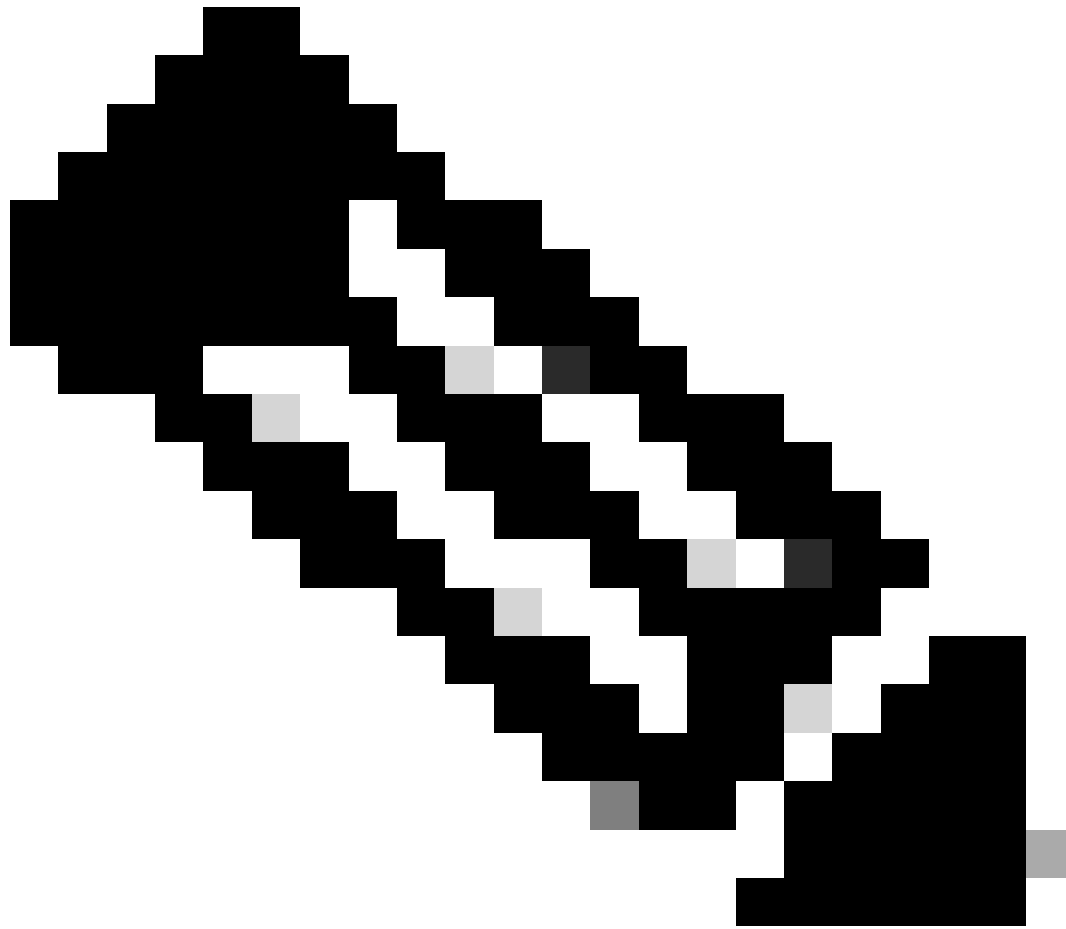
1. 在「全域性身份證明」頁面上更新身份證明，該頁面位於「設計」(Design)>「網路設定」(Network Settings)>「裝置身份證明」(Device Credentials)>「CLI身份證明」(CLI Credentials)>「編輯使用者名稱」(edit username)>「更新使用者密碼」(update the user's password)，而不更改啟用密碼。
2. 在Global Credentials頁面上修改憑證後，Cisco Catalyst Center未管理AAA的站點的受管裝置可以使用更新的憑證重新配置。Cisco Catalyst Center可以推送臨時EEM指令碼以驗證憑證。如果登入成功，則可保留配置。



註：對於Cisco Catalyst Center未管理AAA配置的站點上的受管裝置，Cisco Catalyst Center並不知道是否使用外部AAA伺服器手動配置受管裝置，或者受管裝置是否僅使用本地憑據，因此，如果在受管裝置上配置了密碼，請確保在外部AAA伺服器上更新密碼，然後繼續這些步驟。

要求更改使用者的密碼和使能密碼

1. 在「全域性身份證明」頁面上更新身份證明，該頁面位於「設計」(Design)>「網路設定」(Network Settings)>「裝置身份證明」(Device Credentials)>「CLI身份證明」(CLI Credentials)>編輯使用者名稱>更新使用者的密碼以及啟用密碼。
2. 在Global Credentials頁面上修改憑證後，Cisco Catalyst Center未管理AAA的站點的受管裝置可以使用更新的憑證重新配置。Cisco Catalyst Center可以推送臨時EEM指令碼以驗證憑證。如果登入成功，則可保留配置。



註：對於Cisco Catalyst Center未管理AAA配置的站點上的受管裝置，Cisco Catalyst Center並不知道是否使用外部AAA伺服器手動配置受管裝置，或者受管裝置是否僅使用本地憑據，因此，如果在受管裝置上配置了密碼，請確保在外部AAA伺服器上更新密碼，然後繼續這些步驟。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。