

使用ISE伺服器配置CIMC上的TACACS+身份驗證

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[用於許可權關聯的TACACS+伺服器端配置](#)

[ISE配置要求](#)

[CIMC上的TACACS+組態](#)

[驗證](#)

[在CIMC中從CLI驗證配置](#)

[疑難排解](#)

[ISE故障排除](#)

[相關資訊](#)

簡介

本檔案介紹在思科整合式管理控制器(CIMC)上設定終端存取控制器存取控制系統Plus(TACACS+)驗證。

TACACS+通常用於透過中央伺服器驗證網路裝置。自版本4.1(3b)起，Cisco IMC支援TACACS+身份驗證。CIMC上的TACACS+支援可簡化管理多個可存取裝置的使用者帳戶的工作。此功能有助於定期更改使用者憑據並遠端管理使用者帳戶。

必要條件

需求

思科建議您瞭解以下主題：

- 思科整合式管理控制器(CIMC)
- 終端存取控制器存取控制系統Plus(TACACS+)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- UCSC-C220-M4S
- CIMC版本：4.1(3b)
- 思科身份服務引擎(ISE)版本3.0.0.458

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

用於許可權關聯的TACACS+伺服器端配置

根據為該使用者配置的cisco-av-pair值來計算該使用者的許可權級別。需要在TACACS+伺服器上為建立cisco-av配對，使用者無法使用任何預設TACACS+屬性。cisco-av-pair屬性支援以下三個語法

admin許可權：

```
cisco-av-pair=shell:roles="admin"
```

對於使用者許可權：

```
cisco-av-pair=shell:roles="user"
```

對於只讀許可權：

```
cisco-av-pair=shell:roles="read-only"
```

要支援其他裝置，如果需要新增其他角色，則可以使用逗號作為分隔符來新增這些角色。例如，UCSM支援aaa，因此可以配置shell:roles="admin, aaa", CIMC接受此格式。

附註：如果沒有在TACACS+伺服器上設定cisco-av-pair，則具有該伺服器的使用者具有唯讀許可權。

ISE配置要求

必須在ISE網路裝置上允許伺服器的管理IP。

The screenshot shows the Cisco ISE Administration interface for Network Resources. The 'Network Devices' section is active, displaying a table of configured devices. The table has the following columns: Name, IP/Mask, Profile Name, Location, Type, and Description. The row for 'CIMC_4.1b' is highlighted with a red box, showing an IP of 10.31.123.2, Profile Name 'Cisco', Location 'All Locations', and Type 'All Device Types'.

| Name | IP/Mask | Profile Name | Location | Type | Description |
|------------------------------------|-------------|--------------|---------------|------------------|-------------|
| <input type="checkbox"/> CIMC_4.1b | 10.31.123.2 | Cisco | All Locations | All Device Types | |
| <input type="checkbox"/> Orma Test | 10.201.222 | Cisco | All Locations | All Device Types | |

要在CIMC上輸入的共用金鑰密碼。

- Network Devices
- Default Device
- Device Security Settings

Network Devices List > CIMC_4.1b

Network Devices

* Name

Description

IP Address /

* Device Profile

Model Name

Software Version

* Network Device Group

Location

IPSEC

Device Type

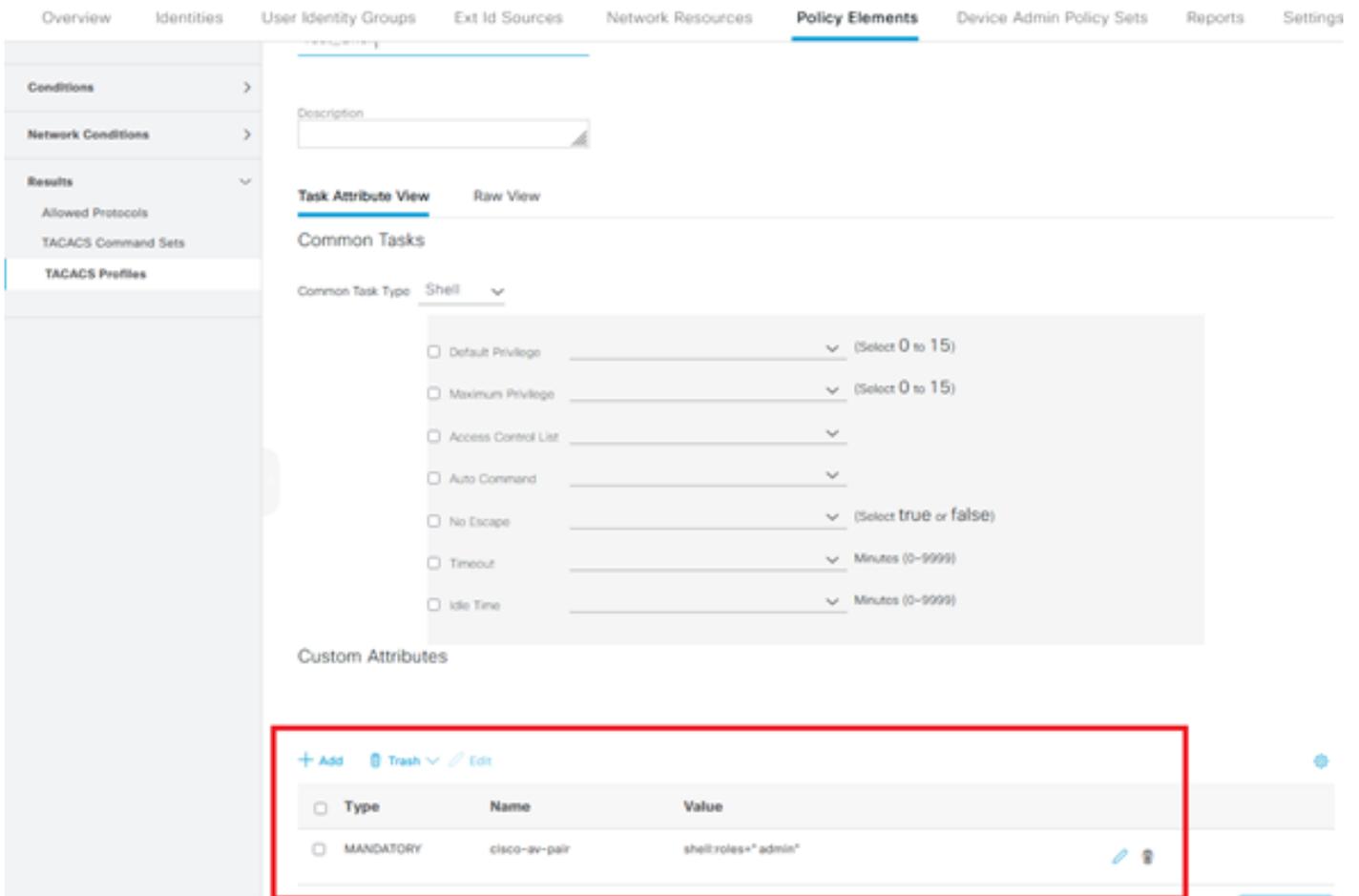
TEST

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

具有管理許可權的cisco-av-pair屬性的外殼配置檔案。



CIMC上的TACACS+組態

步驟1. 導覽至Admin > User Management > TACACS+

步驟2. 選中覈取方塊以啟用TACACS+

步驟3. 可以在表中指定的6行中的任意行中新增新伺服器。按一下該行或選擇該行並按一下表頂部的edit按鈕，如下圖所示。

TACACS+ Properties

Enabled: 1 ←

Fallback only on no connectivity:

Timeout (for each server): (5 - 30 Seconds)

Server List

Selected 0 / Total 6

| ID | IP Address or Host Name | Port | Server Key |
|-------------------------|-------------------------|------|------------|
| <input type="radio"/> 1 | | | |
| <input type="radio"/> 2 | | | |
| <input type="radio"/> 3 | | | |
| <input type="radio"/> 4 | | | |
| <input type="radio"/> 5 | | | |
| <input type="radio"/> 6 | | | |

附註： 在使用者啟用無連線選項的TACACS+回退時，CIMC會強制第一個身份驗證優先順序必須始終設定為TACACS+，否則回退配置可能變得無關。

步驟4. 填寫IP地址或主機名、埠和伺服器金鑰/共用金鑰並儲存配置。

Server List

Selected 0 / Total 6

| ID | IP Address or Host Name | Port | Server Key | Confirm Server Key |
|----|--|---------------------------------|------------------------------------|------------------------------------|
| 1 | <input type="text" value="10.31.126.220"/> | <input type="text" value="49"/> | <input type="text" value="*****"/> | <input type="text" value="*****"/> |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |

Save | Cancel

Cisco IMC最多支援六台TACACS+遠端伺服器。使用者成功通過驗證後，使用者名稱會附加上(TACACS+)。

🔔 0 tacacs_user (TACACS+)@10.24.92.202 - C220-WZP22460WCD ⚙️

Refresh | ? | i

這也會顯示在會話管理中

Sessions

Selected 0 / Total 1 ⚙

| Terminate Session | | | | |
|--------------------------|------------|-----------------------|--------------|--------------|
| | Session ID | User Name | IP Address | Session Type |
| <input type="checkbox"/> | 81 | tacacs_user (TACACS+) | 10.24.92.202 | webgui |

驗證

- CIMC上最多可以配置6台TACACS+伺服器。
- 與伺服器關聯的金鑰長度最多為64個字元。
- 超時可在5到30秒之間配置（計算最大為180秒以與LDAP一致）。
- 如果TACACS+伺服器需要使用服務名稱來建立cisco-av配對，則使用者需要使用Log in作為服務名稱。
- 不支援redfish修改配置。

在CIMC中從CLI驗證配置

- 確認TACACS+是否已啟用。

```
C220-WZP22460WCD# scope tacacs+
C220-WZP22460WCD /tacacs+ # show detail
TACACS+ Settings:
Enabled: yes
Fallback only on no connectivity: no
Timeout(for each server): 5
```

- 驗證每台伺服器的配置詳細資訊。

```
C220-WZP22460WCD /tacacs+ # scope tacacs-server 1
C220-WZP22460WCD /tacacs+/tacacs-server # show detail
Server Id 1:
Server IP address/Hostname: 10.31.126.220
Server Key: *****
Server Port: 49
```

疑難排解

- 確保可以從CIMC訪問TACACS+伺服器IP，並且埠配置正確。
- 確保TACACS+伺服器上的cisco-av-pair配置正確。
- 檢查TACACS+伺服器是否可連線（IP和連線埠）。
- 確保金鑰或憑據與TACACS+伺服器上配置的金鑰或憑據匹配。
- 如果您能使用TACACS+登入，但只有唯讀許可權，請確認cisco-av-pair在TACACS+伺服器上的語法是否正確。

ISE故障排除

- 檢驗Tacacs Live日誌，瞭解其中一次身份驗證嘗試。狀態必須為Pass。

Overview

| | |
|----------------------|--|
| Request Type | Authorization |
| Status | Pass |
| Session Key | ise30baaamex/408819883/155352 |
| Message Text | Device-Administration: Session Authorization succeeded |
| Username | tacacs_user |
| Authorization Policy | New Policy Set 1 >> Authorization Rule 1 |
| Shell Profile | Test_Shell |
| Matched Command Set | |
| Command From Device | |

- 驗證響應是否配置了正確的cisco-av-pair屬性。

Other Attributes

| | |
|---------------------------------|---|
| ConfigVersionId | 933 |
| DestinationIPAddress | 10.31.126.220 |
| DestinationPort | 49 |
| UserName | tacacs_user |
| Protocol | Tacacs |
| RequestLatency | 53 |
| Type | Authorization |
| Service-Argument | login |
| NetworkDeviceProfileId | b0699505-3150-4215-a80e-6753d45bf56c |
| AuthenticationIdentityStore | Internal Users |
| AuthenticationMethod | Lookup |
| SelectedAccessService | Default Device Admin |
| IdentityGroup | User Identity Groups:ALL_ACCOUNTS (default) |
| SelectedAuthenticationIdenti... | Internal Users |
| AuthenticationStatus | AuthenticationPassed |
| UserType | User |
| CPMSessionID | 50617983410.31.123.2734354Authorization506179834 |
| IdentitySelectionMatchedRule | Default |
| TEST | TEST#TEST |
| Network Device Profile | Cisco |
| IPSEC | IPSEC#Is IPSEC Device#No |
| EnableFlag | Enabled |
| Response | {Author-Reply-Status=PassAdd; AVPair=cisco-av-pair=shell:roles=" admin" ; } |

相關資訊

- [TACACS+驗證Cisco UCS-C](#)
- [技術支援與文件 - Cisco Systems](#)
- [配置ISE 2.0:基於AD組成員身份的IOS TACACS+驗證和命令授權](#)