

配置ISE 2.0 TACACS+身份驗證命令授權

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[配置ISE進行身份驗證和授權](#)

[將ISE 2.0加入Active Directory](#)

[新增網路裝置](#)

[啟用裝置管理服務](#)

[配置TACACS命令集](#)

[配置TACACS配置檔案](#)

[配置TACACS授權策略](#)

[配置Cisco IOS路由器以進行身份驗證和授權](#)

[驗證](#)

[Cisco IOS路由器驗證](#)

[ISE 2.0驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何根據Microsoft Active Directory(AD)群組成員身分設定TACACS+驗證和命令授權。

背景資訊

要根據身份服務引擎(ISE)2.0及更高版本的使用者的Microsoft Active Directory(AD)組成員身份配置TACACS+身份驗證和命令授權，ISE使用AD作為外部身份儲存來儲存資源，如使用者、電腦、組和屬性。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco IOS路由器完全可操作
- 路由器和ISE之間的連線。

- ISE伺服器已引導並且與Microsoft AD連線

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎2.0
- Cisco IOS[®]軟體版本15.4(3)M3
- Microsoft Windows Server 2012 R2

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。

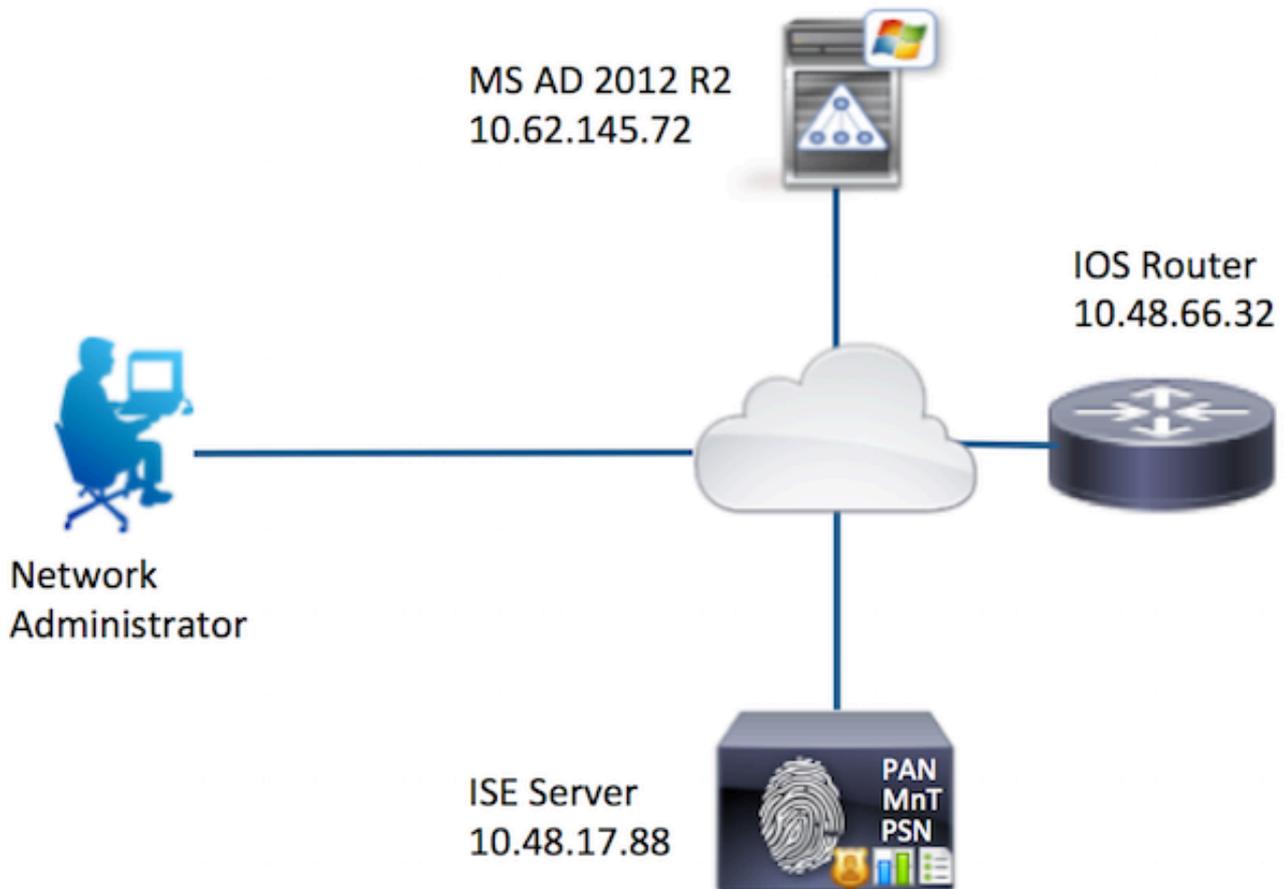
如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

設定

組態的目的是：

- 通過AD驗證telnet使用者
- 授權telnet使用者，使其在登入後進入特權執行模式
- 檢查並將每個執行的命令傳送到ISE進行驗證

網路圖表



組態

配置ISE進行身份驗證和授權

將ISE 2.0加入Active Directory

1. 導航到**管理>身份管理>外部身份庫> Active Directory >新增**。提供加入點名稱、Active Directory域並點選**提交**。

Operations Policy Guest Access Administration Work Centers

sources Device Portal Management pxGrid Services Feed Service pxGrid Identity Mapping

Identity Source Sequences Settings

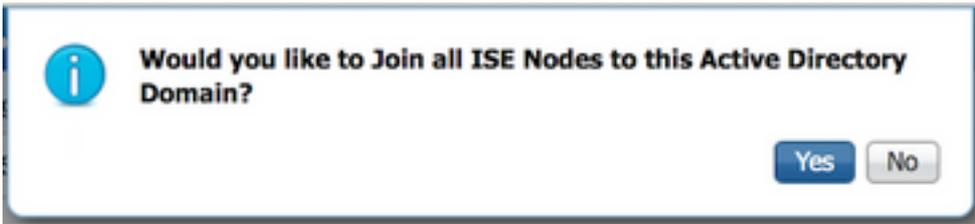
Connection

* Join Point Name AD

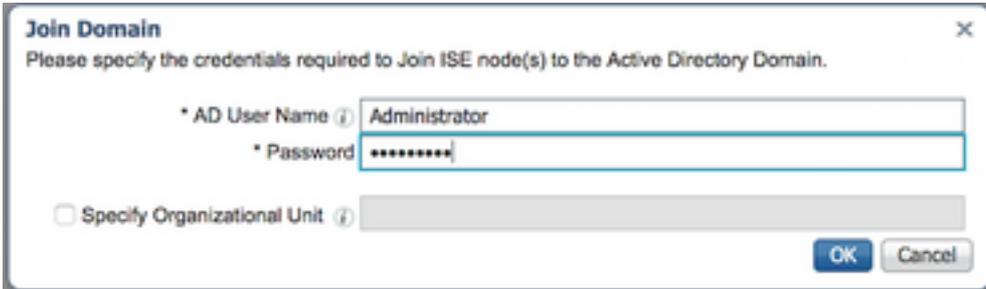
* Active Directory Domain example.com

Submit Cancel

2.當系統提示將所有ISE節點加入此Active Directory域時，按一下**是**。



3.提供AD使用者名稱和密碼，然後按一下**OK**。

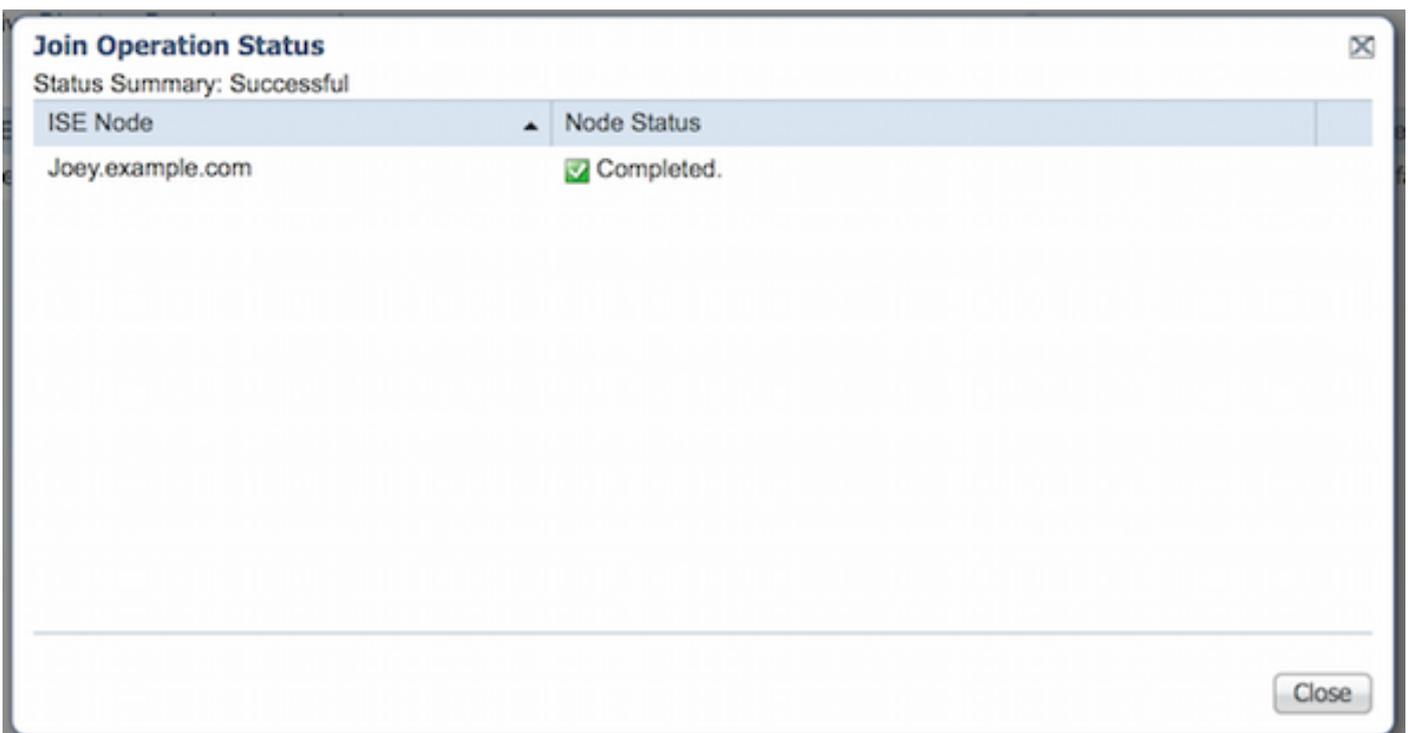


在ISE中訪問域所需的AD帳戶可以具有以下任一項：

- 將工作站新增到相應域中的域使用者許可權
- 在建立ISE電腦帳戶的ISE電腦加入ISE電腦到域之前，在相應的電腦容器上建立電腦對象或刪除電腦對象許可權

附註：思科建議禁用ISE帳戶的鎖定策略，並配置AD基礎設施，以便在為該帳戶使用錯誤密碼時向管理員傳送警報。輸入錯誤密碼時，ISE不會在必要時建立或修改其電腦帳戶，因此可能會拒絕所有身份驗證。

4.複查工序狀態。節點狀態必須顯示為已完成。按一下「**Close**」。



5. AD的狀態為運行。

Operations Policy Guest Access Administration Work Centers

Resources Device Portal Management pxGrid Services Feed Service pxGrid Identifier

entity Source Sequences Settings

Connection Authentication Domains Groups Attributes

* Join Point Name

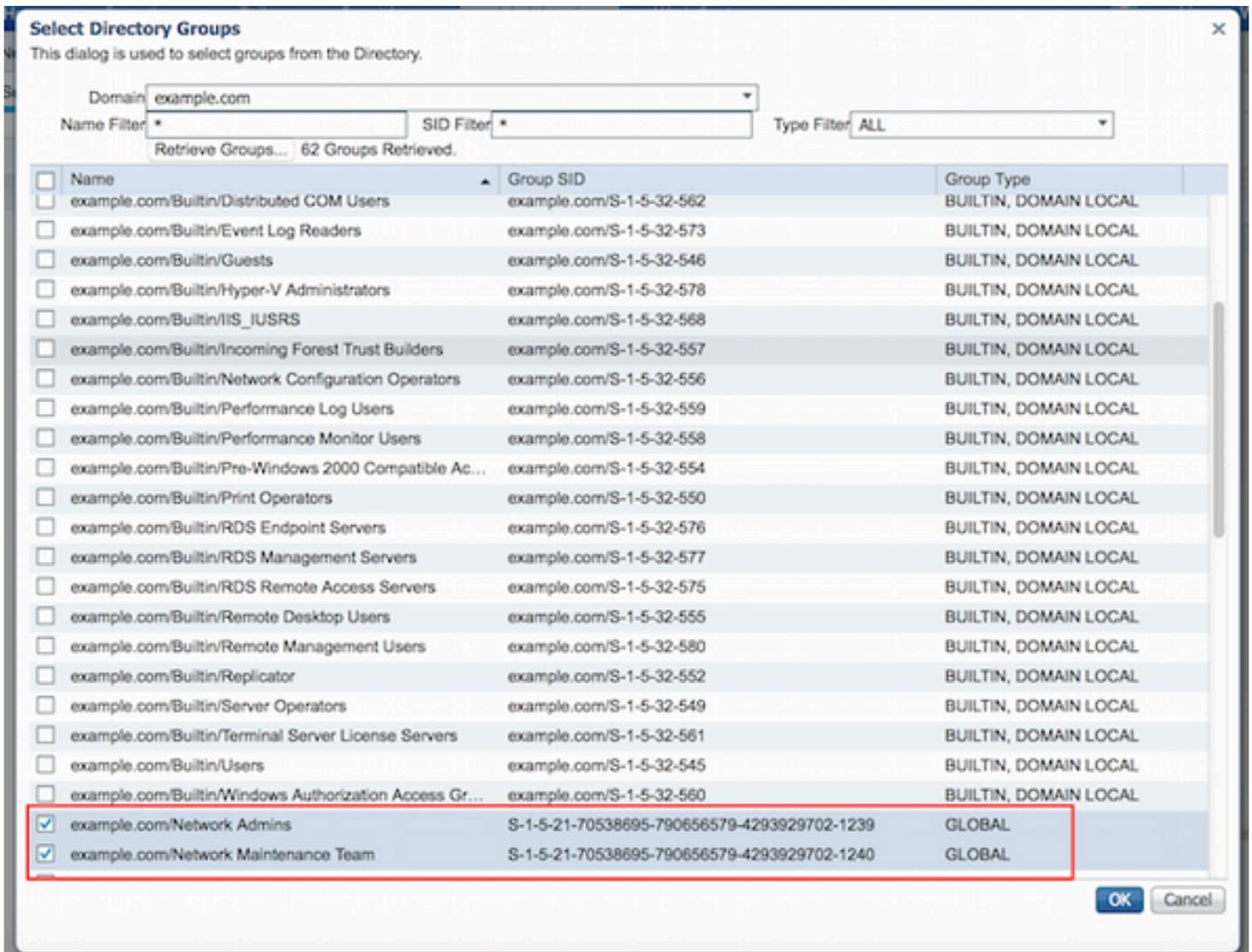
* Active Directory Domain **example.com**

Join Leave Test User Diagnostic Tool Refresh Table

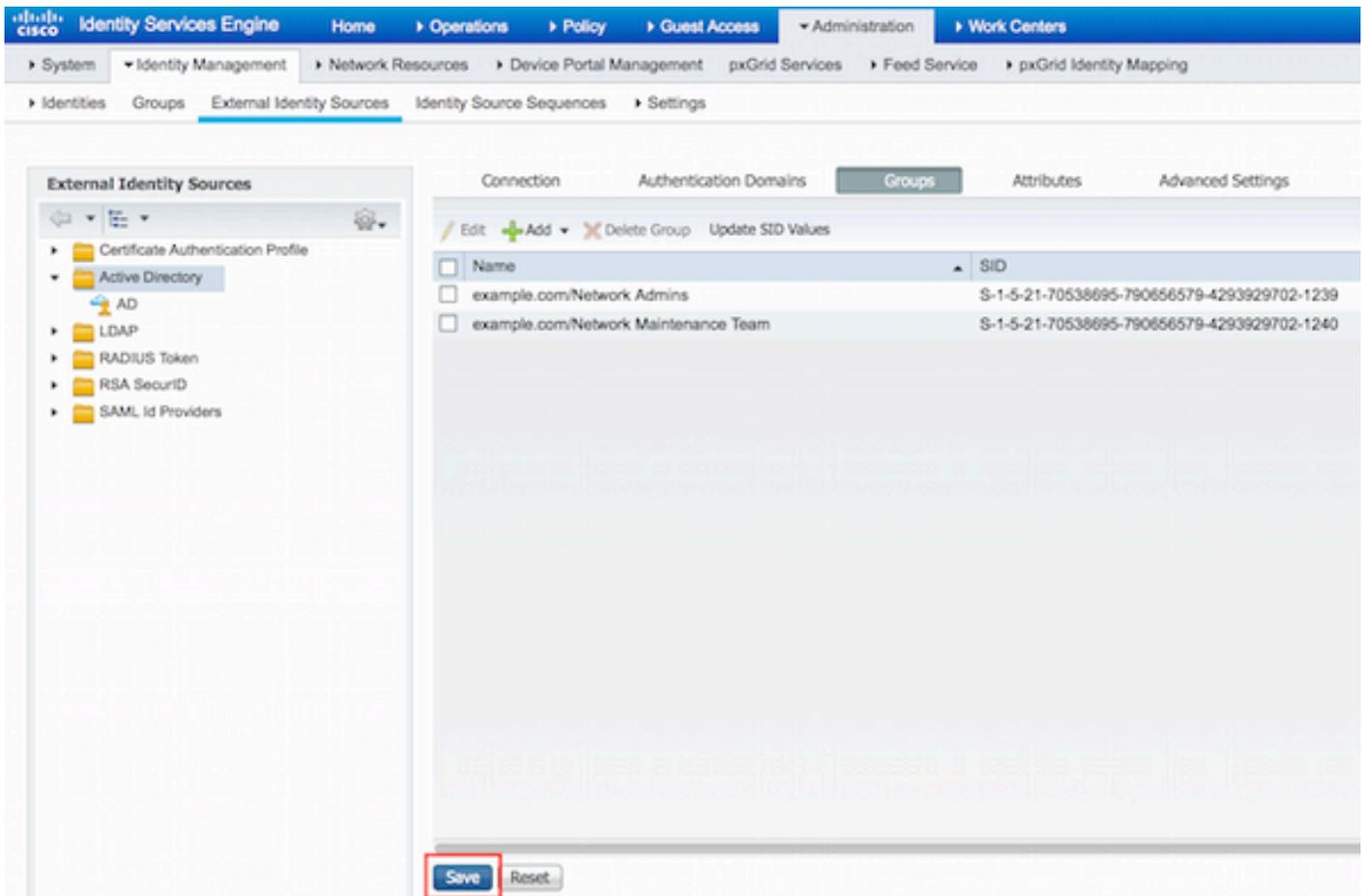
| <input type="checkbox"/> | ISE Node | ISE Node Role | Status |
|--------------------------|------------------|---------------|---|
| <input type="checkbox"/> | Joey.example.com | STANDALONE | <input checked="" type="checkbox"/> Operational |

6. 定位至「組」>「新增」>「從目錄選擇組」>「檢索組」。選中Network Admins AD Group和Network Maintenance Team AD Group覈取方塊，如下圖所示。

附註：使用者admin是網路管理員AD組的成員。此使用者具有完全訪問許可權。此使用者是網路維護團隊AD組的成員。此使用者只能執行show命令。



7. 按一下儲存以儲存檢索到的AD組。



新增網路裝置

導航至工作中心>裝置管理>網路資源>網路裝置。按一下「Add」。提供名稱、IP地址，選中TACACS+身份驗證設定覈取方塊並提供共用金鑰。

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions Policy Results Policy Sets Reports Settings

Network Devices List > New Network Device

Network Devices

Default Devices
TACACS External Servers
TACACS Server Sequence

1 * Name Router
Description

2 * IP Address: 10.48.66.32 / 32

* Device Profile Cisco
Model Name
Software Version

* Network Device Group
Location All Locations Set To Default
Device Type All Device Types Set To Default

RADIUS Authentication Settings

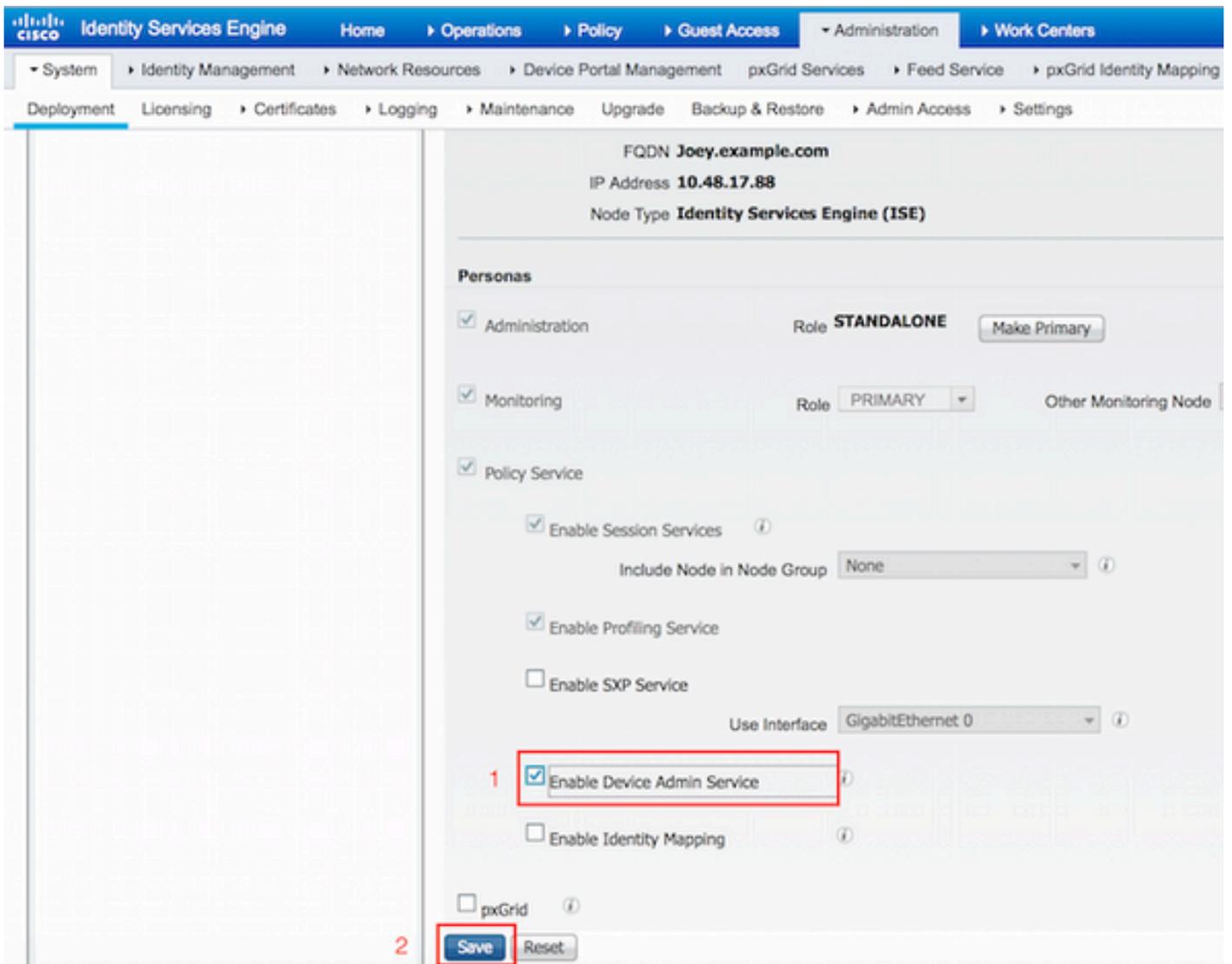
TACACS+ Authentication Settings

Shared Secret ***** Show

Enable Single Connect Mode

啟用裝置管理服務

導航到**管理>系統>部署**。選擇所需的節點。選中**Enable Device Admin Service**覆取方塊，然後按一下**Save**。



附註：對於TACACS，您需要安裝單獨的許可證。

配置TACACS命令集

配置了兩個命令集。第一個用於使用者admin的**PermitAllCommands**，它允許裝置上的所有命令。第二個使用者的**PermitShowCommands**，僅允許show命令。

1. 導航至工作中心>裝置管理>策略結果> TACACS命令集。按一下「Add」。提供名稱**PermitAllCommands**，選中**Permit any command**覈取方塊（未列出），然後按一下**Submit**。

TACACS Command Sets > New

Command Set

1

Name *

PermitAllCommands

Description

2

Permit any command that is not listed below

| <input type="checkbox"/> | Grant | Command | Arguments |
|--------------------------|-------|---------|-----------|
| No data found. | | | |

2. 導航到工作中心>裝置管理>策略結果> TACACS命令集。按一下「Add」。提供名稱 PermitShowCommands，按一下Add並允許show和退出命令。預設情況下，如果Arguments留空，則包含所有引數。按一下Submit (提交)。

Home ▶ Operations ▶ Policy ▶ Guest Access ▶ Administration ▶ Work Centers

Groups ▶ Network Resources ▶ Network Device Groups ▶ Policy Conditions ▶ Policy Results ▶ Policy Sets

TACACS Command Sets > New

Command Set

1 Name * PermitShowCommands

Description

Permit any command that is not listed below

0 Selected

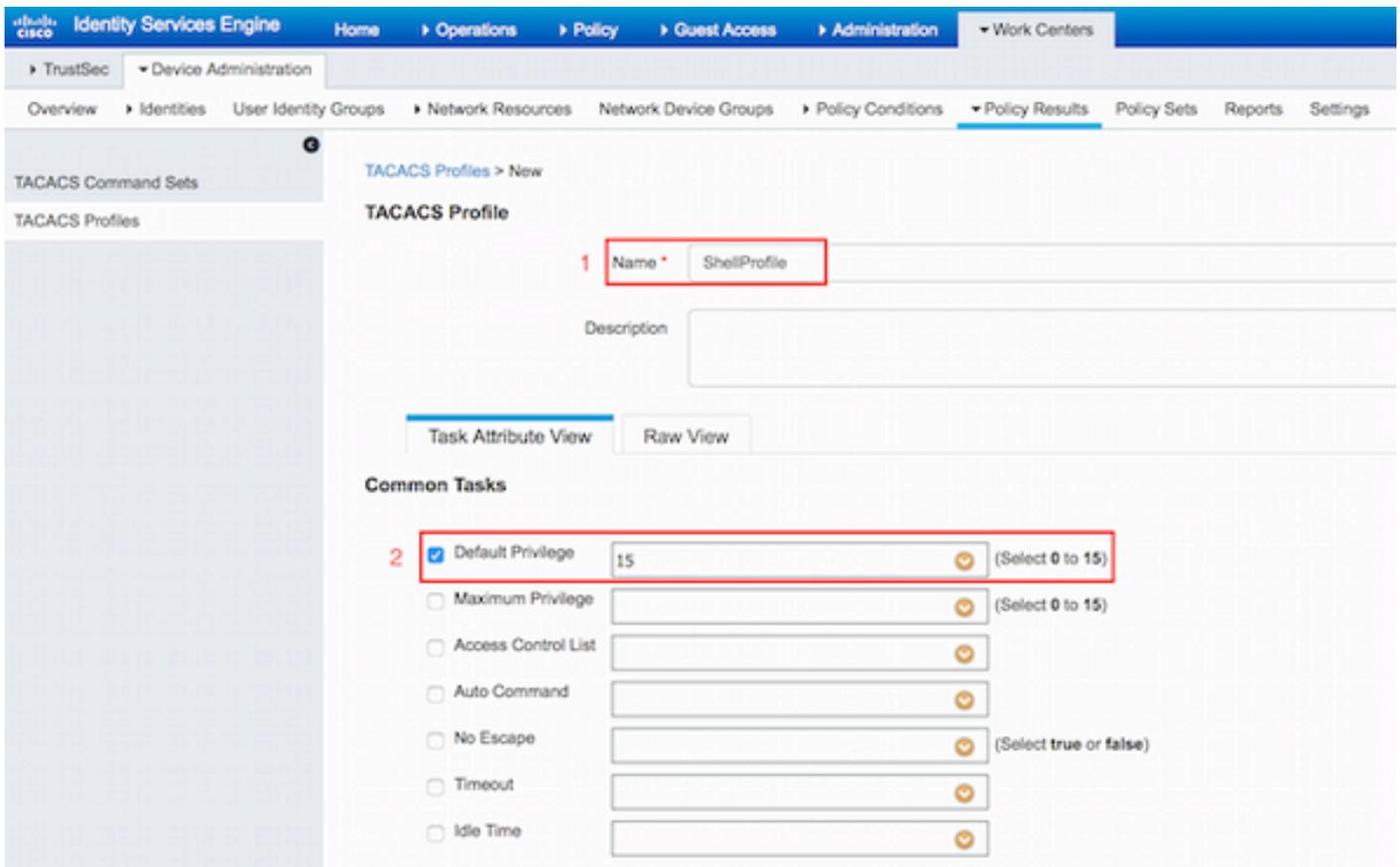
2 + Add Trash Edit Move Up Move Down

| Grant | Command | Arguments |
|--------------------------|---------|-----------|
| <input type="checkbox"/> | PERMIT | show |
| <input type="checkbox"/> | PERMIT | exit |

3

配置TACACS配置檔案

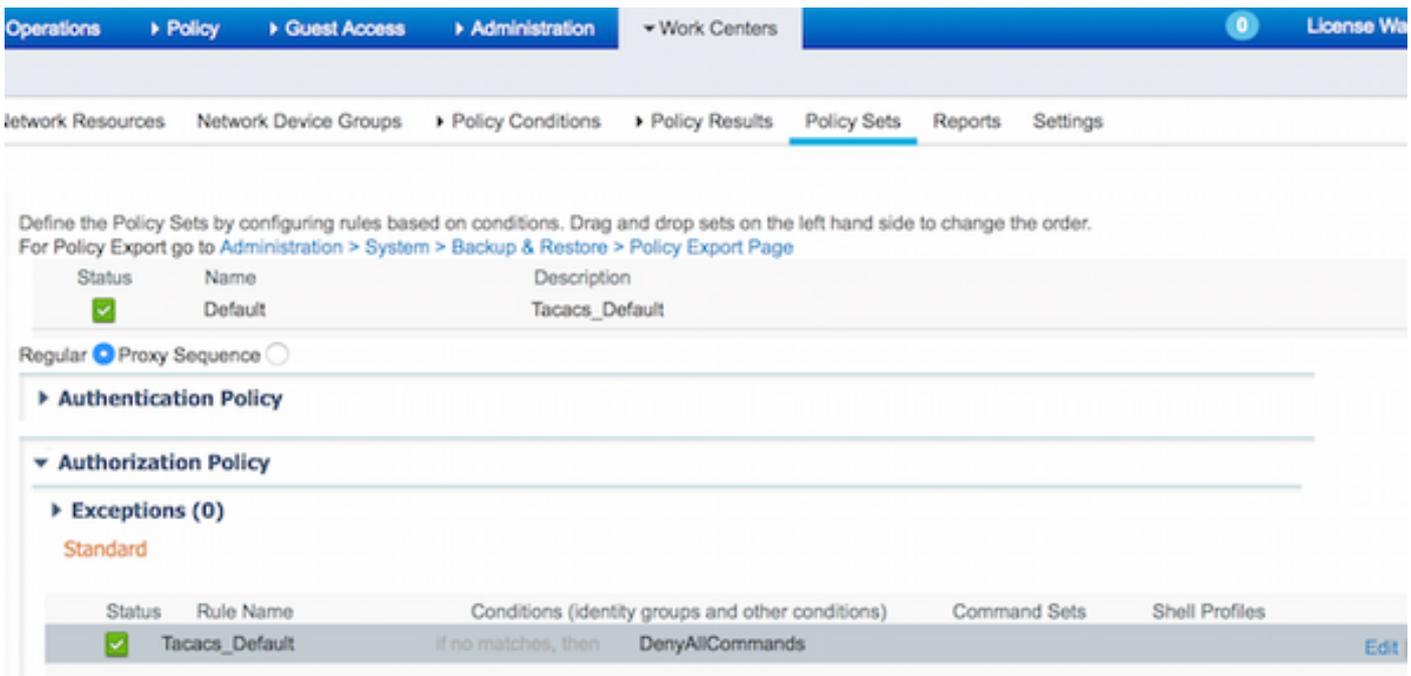
已配置單個TACACS配置檔案。TACACS配置檔案與ACS上的外殼配置檔案概念相同。實際的命令執行是通過命令集完成的。導航到工作中心(Work Centers)>裝置管理(Device Administration)>策略結果(Policy Results)> TACACS配置檔案(TACACS Profiles)。按一下「Add」。提供名稱ShellProfile，選中Default Privilege覈取方塊，然後輸入值15。按一下提交。



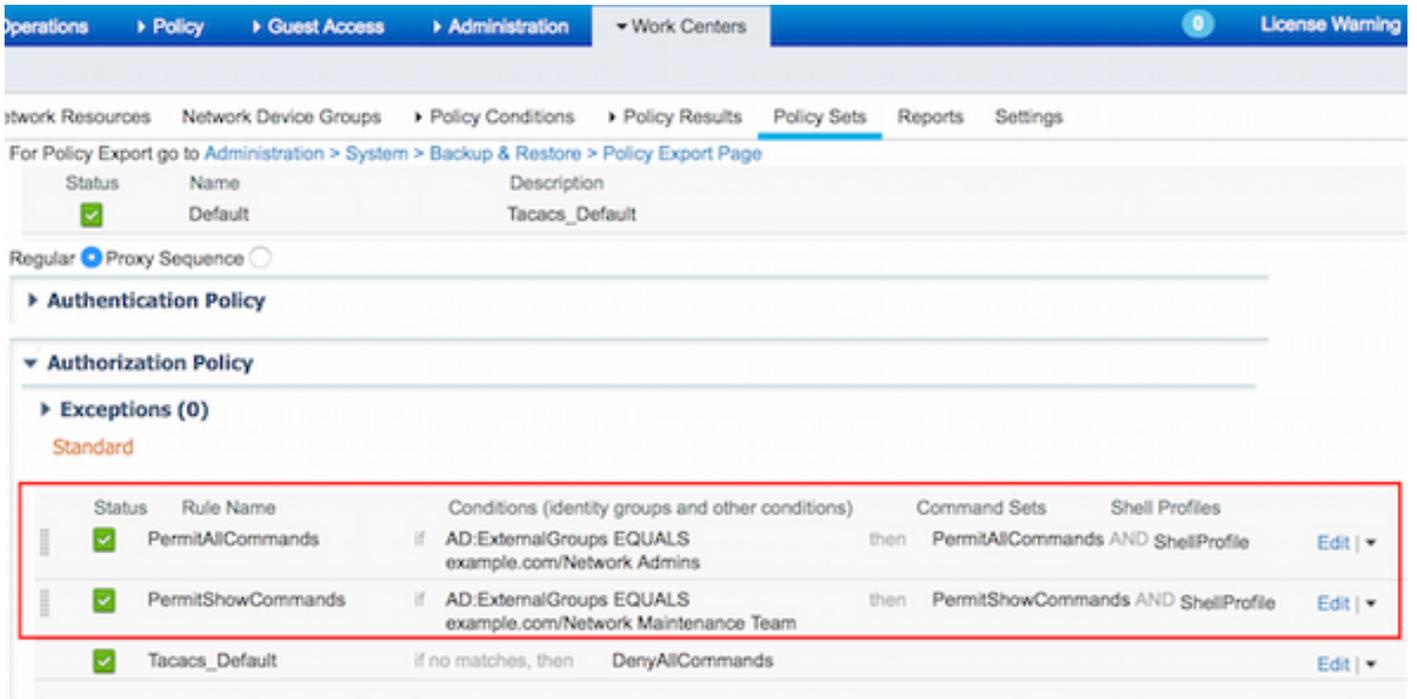
配置TACACS授權策略

預設情況下，「身份驗證策略」指向All_User_ID_Stores（包括AD），因此它保持不變。

導航到Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule above。



配置了兩個授權規則；第一個規則根據網路管理員AD組成員身份分配TACACS配置檔案ShellProfile和命令Set PermitAllCommands。第二個規則基於網路維護團隊AD組成員身份分配TACACS配置檔案ShellProfile和命令Set PermitShowCommands。



配置Cisco IOS路由器以進行身份驗證和授權

完成這些步驟，設定用於驗證和授權的Cisco IOS路由器。

1.使用**username**命令建立具有完全回退許可權的本地使用者，如下所示。

```
username cisco privilege 15 password cisco
```

2.啟用**aaa new-model**。定義TACACS伺服器ISE，並將其放入組ISE_GROUP。

```
aaa new-model
```

```
tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
```

```
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

附註： 伺服器金鑰與之前在ISE伺服器上定義的金鑰匹配。

3.使用**test aaa**命令測試TACACS伺服器的可達性，如下所示。

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

上一個命令的輸出顯示TACACS伺服器可訪問且使用者已成功通過身份驗證。

4.配置登入並啟用身份驗證，然後使用**exec**和命令授權，如下所示。

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
```

```
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

附註：建立的方法清單名為AAA，稍後在將其分配給行vty時使用。

5.將方法清單分配給行vty 0 4。

```
line vty 0 4
  authorization commands 0 AAA
  authorization commands 1 AAA
  authorization commands 15 AAA
  authorization exec AAA
  login authentication AAA
```

驗證

Cisco IOS路由器驗證

1.以admin身份telnet至Cisco IOS路由器，該管理員屬於AD中的完全訪問組。Network Admins組是AD中對映到ISE上設定的ShellProfile和PermitAllCommands命令的組。嘗試運行任何命令以確保完全訪問。

```
Username:admin
Password:
```

```
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

2. Telnet至Cisco IOS路由器，使其成為屬於AD中有限訪問組的使用者。網路維護組是AD中對映到ISE上設定的ShellProfile和PermitShowCommands命令的組。嘗試運行任何命令以確保只能發出show命令。

```
Username:user
Password:
```

```
Router#show ip interface brief | exclude unassigned
Interface          IP-Address      OK? Method Status          Protocol
GigabitEthernet0/0 10.48.66.32     YES NVRAM  up              up
```

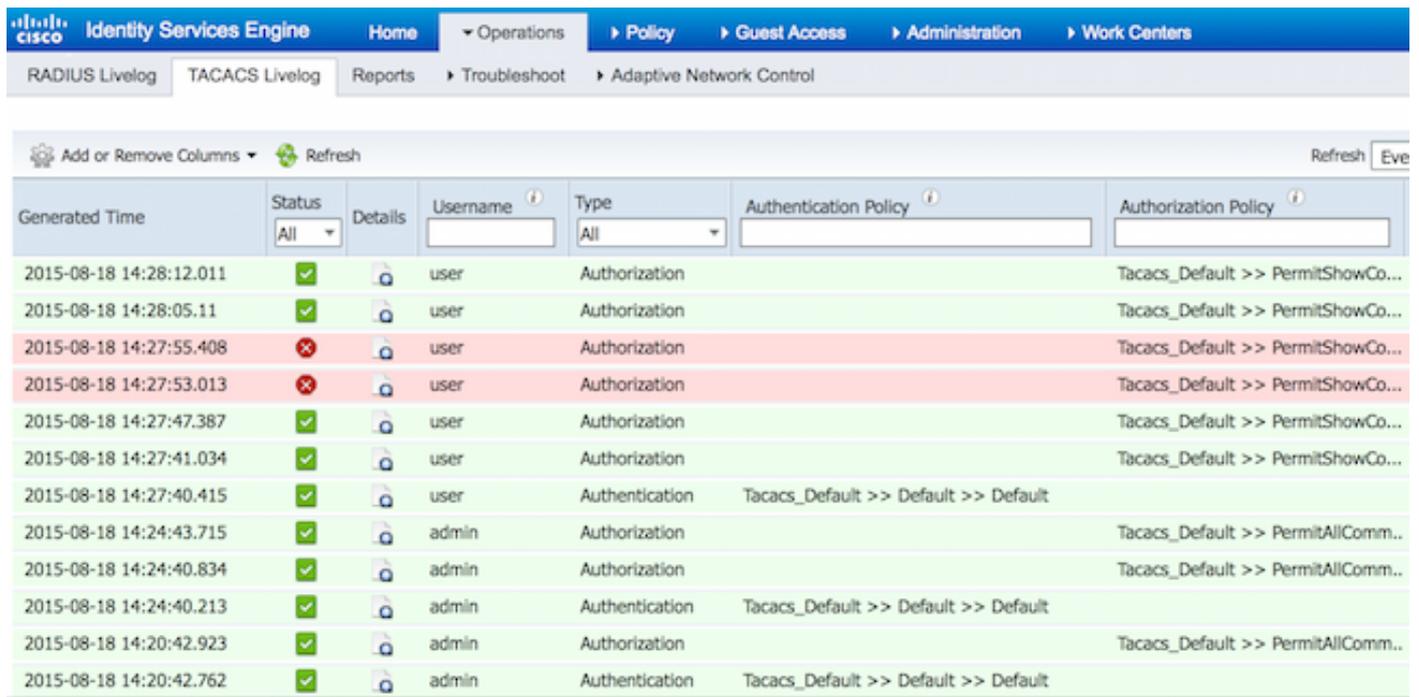
```
Router#ping 8.8.8.8
Command authorization failed.
```

```
Router#configure terminal
Command authorization failed.
```

```
Router#show running-config | include hostname
hostname Router
Router#
```

ISE 2.0驗證

1. 導覽至 Operations > TACACS Livelog。確保看到已完成的嘗試。



| Generated Time | Status | Details | Username | Type | Authentication Policy | Authorization Policy |
|-------------------------|--------|---------|----------|----------------|--------------------------------------|------------------------------------|
| 2015-08-18 14:28:12.011 | ✓ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:28:05.11 | ✓ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:27:55.408 | ✗ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:27:53.013 | ✗ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:27:47.387 | ✓ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:27:41.034 | ✓ | | user | Authorization | | Tacacs_Default >> PermitShowCo... |
| 2015-08-18 14:27:40.415 | ✓ | | user | Authentication | Tacacs_Default >> Default >> Default | |
| 2015-08-18 14:24:43.715 | ✓ | | admin | Authorization | | Tacacs_Default >> PermitAllComm... |
| 2015-08-18 14:24:40.834 | ✓ | | admin | Authorization | | Tacacs_Default >> PermitAllComm... |
| 2015-08-18 14:24:40.213 | ✓ | | admin | Authentication | Tacacs_Default >> Default >> Default | |
| 2015-08-18 14:20:42.923 | ✓ | | admin | Authorization | | Tacacs_Default >> PermitAllComm... |
| 2015-08-18 14:20:42.762 | ✓ | | admin | Authentication | Tacacs_Default >> Default >> Default | |

2. 按一下其中一個紅色報表的詳細資訊。以前執行的失敗命令可見。

Overview

| | |
|----------------------|--|
| Request Type | Authorization |
| Status | Fail |
| Session Key | Joey/229259639/49 |
| Message Text | Failed-Attempt: Command Authorization failed |
| Username | user |
| Authorization Policy | Tacacs_Default >> PermitShowCommands |
| Shell Profile | |
| Matched Command Set | |
| Command From Device | configure terminal |

Authorization Details

| | |
|----------------|--|
| Generated Time | 2015-08-18 14:27:55.408 |
| Logged Time | 2015-08-18 14:27:55.409 |
| ISE Node | Joey |
| Message Text | Failed-Attempt: Command Authorization failed |
| Failure Reason | 13025 Command failed to match a Permit rule |

疑難排解

錯誤：13025命令無法匹配Permit規則

檢查SelectedCommandSet屬性以驗證預期的Command Sets是否由授權策略選擇。

相關資訊

[技術支援與文件 - Cisco Systems](#)

[ISE 2.0版本說明](#)

[ISE 2.0硬體安裝指南](#)

[ISE 2.0升級指南](#)

[ACS到ISE遷移工具指南](#)

[ISE 2.0 Active Directory整合指南](#)

[ISE 2.0引擎管理員指南](#)

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）。