

將RADIUS用於身份服務引擎的裝置管理

目錄

[簡介](#)

[背景資訊](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[建立存取接受設定檔](#)

[建立訪問拒絕配置檔案](#)

[裝置清單](#)

[聚合服務路由器\(ASR\)](#)

[Cisco交換機IOS®和Cisco IOS® XE](#)

[BlueCoat資料包整形器](#)

[BlueCoat Proxy伺服器\(AV/SG\)](#)

[Brocade交換機](#)

[Infoblox](#)

[Cisco Firepower管理中心](#)

[Nexus交換機](#)

[無線LAN控制器\(WLC\)](#)

[資料中心網路管理員\(DCNM\)](#)

[音訊碼](#)

簡介

本文檔介紹各種思科和非思科產品預期從AAA伺服器（如思科ISE）接收的屬性集合。

背景資訊

思科和非思科產品期望從身份驗證、授權和記帳(AAA)伺服器接收屬性編譯。在這種情況下，伺服器是思科ISE，ISE會返回這些屬性以及作為授權配置檔案(RADIUS)一部分的Access-Accept。

本文檔提供有關如何增加自定義屬性授權配置檔案的分步說明，還包含裝置清單和裝置預期從AAA伺服器返回的RADIUS屬性。所有主題都包含示例。

本檔案所提供的屬性清單既不詳盡，也不具權威性，且不需更新本檔案即可隨時變更。

網路裝置的裝置管理通常使用TACACS+協定實現，但如果網路裝置不支援TACACS+或ISE沒有裝置管理許可證，也可以使用RADIUS實現，如果網路裝置支援RADIUS裝置管理。某些裝置支援這兩種通訊協定，且需由使用者決定使用哪一種通訊協定，但TACACS+可能是有益的，因為它擁有例如命令授權和命令計費等功能。

必要條件

需求

思科建議您瞭解以下內容：

- 思科ISE作為感興趣網路上的RADIUS伺服器
- Radius協定的工作流程- RFC2865

採用元件

本文檔中的資訊基於Cisco身份服務引擎(ISE) 3.x及更高版本的ISE。

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


步驟 1.建立供應商特定屬性(VSA)

可以為每個供應商建立各種詞典，並且可以在這些詞典中增加屬性。每個詞典可以有多個可在授權配置檔案中使用的屬性。一般而言，每個屬性都會定義使用者在登入網路裝置時，可以獲得的不同裝置管理角色。但是，此屬性可用於網路裝置上的不同操作或配置目的。

ISE為一些供應商提供預定義屬性。如果未列出供應商，則可以將其增加為具有屬性的詞典。對於某些網路裝置，這些屬性是可配置的，並且可針對各種型別的訪問進行更改，在這種情況下，ISE必須使用網路裝置期望用於不同型別訪問的屬性進行配置。

預期透過Radius Access-Accept傳送的屬性定義如下：

1. 導航到策略>策略元素>詞典>系統> Radius > Radius供應商>增加。
2. 輸入並儲存名稱和供應商ID。
3. 按一下儲存的Radius Vendor，然後導航到Dictionary Attributes。
4. 按一下Add並填寫區分大小寫的屬性名稱、資料型別、方向和ID。
5. 儲存屬性。
6. 如果要將多個「屬性」新增至同一個「詞典」，請在同一頁面上新增其他「屬性」。

 註：在此部分中作為值輸入的每個欄位均由供應商自己提供。如果不知道供應商網站，可以訪問供應商網站或聯絡供應商支援。

Cisco ISE Policy · Policy Elements

Dictionaries Conditions Results

System Dictionaries

EQ

< [List Icon] [Settings Icon]

- > System
- > User

View

Name	Description
<input type="checkbox"/> ACIDEX	Profiler ACIDEX dictionary
<input type="checkbox"/> ACTIVEDIRECTORY_PROBE	Profiler ACTIVEDIRECTORY_PROBE dictionary
<input type="checkbox"/> APIC	Dictionary for APIC
<input type="checkbox"/> CDP	Profiler CDP dictionary

Cisco ISE Policy · Policy Elements

Dictionaries Conditions Results

RADIUS Vendors

EQ

< [List Icon] [Settings Icon]

- > PassiveID
- > Posture
- > PROFILER
- Radius
 - > IETF
 - RADIUS Vendors
 - > Airespace
 - > Alcatel-Lucent
 - > Aruba

Edit Add Delete Import Export

Name	Vendor ID	Description
<input type="checkbox"/> Airespace	14179	Dictionary for Vendor Airespace
<input type="checkbox"/> Alcatel-Lucent	800	Dictionary for Vendor Alcatel-Lucent
<input type="checkbox"/> Aruba	14823	Dictionary for Vendor Aruba
<input type="checkbox"/> Brocade	1588	Dictionary for Vendor Brocade
<input type="checkbox"/> Cisco	9	Dictionary for Vendor Cisco
<input type="checkbox"/> Cisco-BBSM	5263	Dictionary for Vendor Cisco-BBSM
<input type="checkbox"/> Cisco-VPN3000	3076	Dictionary for Vendor Cisco-VPN3000

Dictionarys Conditions Results

Dictionarys

EQ



- Radius
- IETF
- RADIUS Vendors
 - Airespace
 - Alcatel-Lucent
 - Aruba
 - Brocade

RADIUS Vendors List > New RADIUS Vendor

* Dictionary Name Packeteer
Description Disctionary for BlueCoat Packet Shaper

* Vendor ID 2334
Vendor Attribute Type Field Length 1
Vendor Attribute Size Field Length 1

Submit Cancel

Dictionarys Conditions Results

Dictionarys

EQ



- RADIUS Vendors
 - Airespace
 - Alcatel-Lucent
 - Aruba
 - Brocade
 - Cisco
 - Cisco-BBSM
 - Cisco-VPN3000
 - H3C
 - HP
 - Juniper
 - Microsoft
 - Motorola-Symbol
 - Packeteer
 - Ruckus

Dictionarys > ... > RADIUS Vendors > Packeteer

Dictionary Dictionary Attributes

Dictionary Attributes


+ Add Edit Delete

<input type="checkbox"/>	Name	Number	Type	Direction	Description	Predefi...
No data available						

The screenshot shows the Cisco ISE Policy Elements configuration page for a Dictionary Attribute. The breadcrumb navigation is "Dictionaries > ... > RADIUS Vendors > Packeteer". The "Dictionary Attributes" tab is active. The configuration fields are as follows:

- Attribute Name:** Packeteer-AVPair
- Description:** Used in order to specify Access Level
- Data Type:** STRING (dropdown menu)
- Enable MAC option:**
- Direction:** OUT (dropdown menu)
- ID:** 1 (0-255)
- Allow Tagging:**
- Allow multiple instances of this attribute in a profile:**

A "Submit" button is located at the bottom right of the configuration area.

 **注意：**並非所有供應商都要求增加特定詞典。如果供應商可以使用IETF定義的RADIUS屬性（已存在於ISE上），則可以跳過此步驟。

步驟 2. 建立網路裝置配置檔案

此部分不是必需的。網路裝置配置檔案可幫助隔離所增加的網路裝置的型別，並為其建立相應的授權配置檔案。與RADIUS詞典一樣，ISE有一些預定義的可使用的配置檔案。如果尚未存在，則可以建立新的裝置配置檔案。

以下為新增網路設定檔的程式：

1. 導航到管理>網路資源>網路裝置配置檔案>增加。
2. 指定名稱並選中RADIUS所對應的框。
3. 在RADIUS Dictionaries 下，選擇上一部分中建立的詞典。
4. 如果為相同型別的裝置建立了多個詞典，則可以在RADIUS詞典下選擇所有這些詞典。
5. 儲存設定檔。

Cisco ISE Administration - Network Resources

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences NAC Managers

Network Device Profiles

[Edit](#) [+ Add](#) [Duplicate](#) [Import](#) [Cisco Communities Import](#) [Export Selected](#) [Delete Selected](#)

<input type="checkbox"/>	Name	Description	Vendor	Source
<input type="checkbox"/>	AlcatelWired	Profile for Alcatel switches	Alcatel	Cisco Provided
<input type="checkbox"/>	ArubaWireless	Profile for Aruba wireless network access devices	Aruba	Cisco Provided
<input type="checkbox"/>	BrocadeWired	Profile for Brocade switches	Brocade	Cisco Provided
<input type="checkbox"/>	Cisco	Generic profile for Cisco network access devices	Cisco	Cisco Provided

Cisco ISE Administration - Network Resources

Network Devices Network Device Groups **Network Device Profiles** External RADIUS Servers RADIUS Server Sequences

Network Device Profile List > New Network Device Profile

Network Device Profiles

[Submit](#) [Cancel](#)

* Name

Description

Icon [Change icon...](#) [Set To Default](#) ⓘ

Vendor

Supported Protocols

RADIUS
 TACACS+
 TrustSec

RADIUS Dictionaries ×

步驟 3. 在ISE上增加網路裝置

裝置管理所在的網路裝置必須隨在網路裝置上定義的金鑰一起增加到ISE中。在網路裝置上，使用此金鑰將ISE增加為RADIUS AAA伺服器。

以下是在ISE上增加裝置的過程：

1. 導航到管理>網路資源>網路裝置>增加。
2. 提供名稱和IP地址。
3. 您可以從下拉式清單中選擇「裝置設定檔」，做為上一節中定義的設定檔。如果未建立配置檔

案，則可以使用預設的Cisco。

4. 檢查Radius身份驗證設定。

5. 輸入共用金鑰並儲存裝置。

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration · Network Resources'. Below it, a secondary navigation bar lists 'Network Devices', 'Network Device Groups', 'Network Device Profiles', 'External RADIUS Servers', 'RADIUS Server Sequences', and 'NAC Managers'. The 'Network Devices' section is active, showing a sidebar with 'Network Devices', 'Default Device', and 'Device Security Settings'. The main content area is titled 'Network Devices' and features a toolbar with 'Edit', '+ Add', 'Duplicate', 'Import', 'Export', 'Generate PAC', and 'Delete' buttons. Below the toolbar is a table with the following data:

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	SPRT	172.18.228...	Cisco	All Locations	All Device Types	
<input type="checkbox"/>	posturelinux	10.106.36.9...	Cisco	All Locations	All Device Types	

Network Devices

Default Device

Device Security Settings

[Network Devices List](#) > [New Network Device](#)

Network Devices

Name

Description

IP Address /

Device Profile

Model Name

Software Version

Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret

Cisco ISE Administration · Network Resources

Network Devices | Network Device Groups | Network Device Profiles | External RADIUS Servers | RADIUS Server Sequences | NAC Man

Network Devices List > New Network Device

Network Devices

Name

Description

IP Address /

Device Profile

Model Name

Software Version

Network Device Group

Location [Set To Default](#)

IPSEC [Set To Default](#)

Device Type [Set To Default](#)

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret [Show](#)

步驟 4. 建立授權配置檔案

從ISE推送為Access-Accept或Access-Reject的最終結果在授權配置檔案中定義。每個授權配置檔案都可以推送網路裝置期望的其他屬性。

以下是建立授權配置檔案的過程：

1. 導航到策略>策略元素>結果>授權>授權配置檔案。
2. 在Standard Authorization Profiles下，按一下Add。

The screenshot shows the Cisco ISE interface. At the top, there is a navigation bar with the Cisco ISE logo and a breadcrumb trail: Policy > Policy Elements. Below this, there are tabs for Dictionaries, Conditions, and Results (which is selected). On the left side, there is a sidebar menu with categories: Authentication, Authorization (selected), Downloadable ACLs, Profiling, Posture, and Client Provisioning. Under the Authorization category, 'Authorization Profiles' is selected. The main content area is titled 'Standard Authorization Profiles'. It includes a sub-header: 'For Policy Export go to Administration > System > Backup & Restore > Policy Export Page'. Below this, there are action buttons: Edit, Add (highlighted), Duplicate, and Delete. A table lists the profiles:

<input type="checkbox"/>	Name	Profile
<input type="checkbox"/>	Bidirectional_posture_profile	Cisco ⓘ
<input type="checkbox"/>	Blackhole_Wireless_Access	Cisco ⓘ
<input type="checkbox"/>	Cisco_IP_Phones	Cisco ⓘ
<input type="checkbox"/>	Cisco_Temporal_Onboard	Cisco ⓘ


可以增加的配置檔案型別為Access-Accept和Access-Reject。

建立存取接受設定檔

此設定檔用於以某種方式存取網路裝置。此設定檔可同時傳遞多個屬性。以下是步驟：

1. 請指定一個合理的名稱，然後選擇Access Type作為Access-Accept。
2. 選擇在前面部分之一建立的網路裝置配置檔案。如果未建立配置檔案，則可以使用預設的Cisco。
3. 選擇不同型別の設定檔時，此處的頁面會限制組態選項。
4. 在Advanced Attributes Settings下，選擇詞典和適用的屬性(LHS)。
5. 從下拉式清單中為屬性指派值(RHS)（如果有的話）或鍵入預期的值。
6. 如果作為同一結果的一部分要傳送其他屬性，請按一下+圖示並重複步驟4和步驟5。

為ISE預期傳送的每個結果/角色/授權建立多個授權配置檔案。

 附註：合併的屬性可在「屬性明細」欄位下驗證。

Dictionaries Conditions **Results**

- Authentication >
- Authorization ▾
 - Authorization Profiles**
 - Downloadable ACLs
- Profiling >
- Posture >
- Client Provisioning >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Common Tasks

ACL ⓘ

Security Group

Advanced Attributes Settings

Attributes Details

Access Type = ACCESS_ACCEPT

Packeteer-AVPair = access=touch

Cisco ISE Policy · Policy Elements

Dictionarys Conditions **Results**

Authentication >

Authorization >

Authorization Profiles

Downloadable ACLs

Profiling >

Posture >

Client Provisioning >

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

> Common Tasks

Advanced Attributes Settings

=

Attributes Details

Access Type = ACCESS_ACCEPT

cisco-av-pair = shell:priv-lvl=15

建立訪問拒絕配置檔案

此設定檔用於傳送拒絕裝置管理的訊息，但仍可用來傳送屬性。這用於傳送RADIUS Access-Reject資料包。除必須選擇Access-Reject而非Access-Accept作為Access Type的步驟外，這些步驟保持不變。

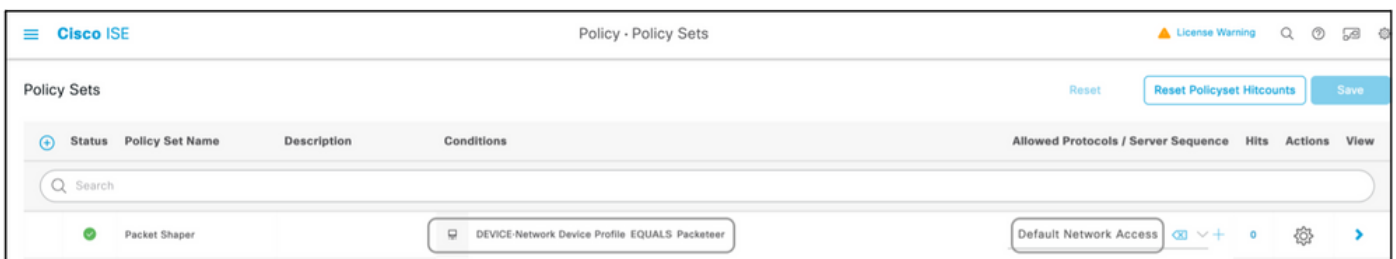
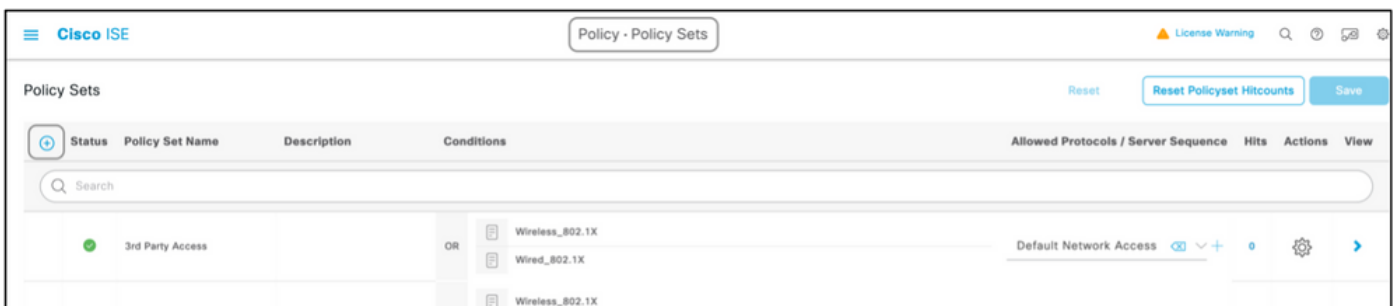
步驟 5. 建立策略集

ISE上的策略集由上到下進行評估，第一個滿足策略集中條件集的策略集負責ISE對網路裝置傳送的

RADIUS訪問請求資料包的響應。Cisco建議為每種型別的裝置設定唯一的策略。評估使用者身份驗證和授權的條件發生在評估階段。如果ISE具有外部身份源，則可用於授權型別。

典型的策略集建立方式如下：

1. 導航到策略>策略集> +。
2. 重新命名新策略集1。
3. 將此條件設定為此裝置的唯一條件。
4. 展開Policy Set。
5. 展開Authentication Policy以設定身份驗證規則。外部源或內部使用者是示例，可用作身份源序列，ISE將根據該序列檢查使用者。
6. 身份驗證策略已全部設定。此時可以儲存策略。
7. 展開Authorization Policy為使用者增加授權條件。例如，檢查特定AD組或ISE內部身份組。同樣命名規則。
8. 可從下拉選單中選擇授權規則的結果。
9. 為供應商支援的不同訪問型別建立多個授權規則。



Cisco ISE Policy - Policy Sets License Warning

Packet Shaper DEVICE-Network Device Profile EQUALS Packeteer Default Network Access

Authentication Policy (1)

Status	Rule Name	Conditions	Use
✓	Any authentication condition	DEVICE-Network Device Profile EQUALS Packeteer	All_User_ID_Stores ⌵ Options
✓	Default		All_User_ID_Stores ⌵ Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

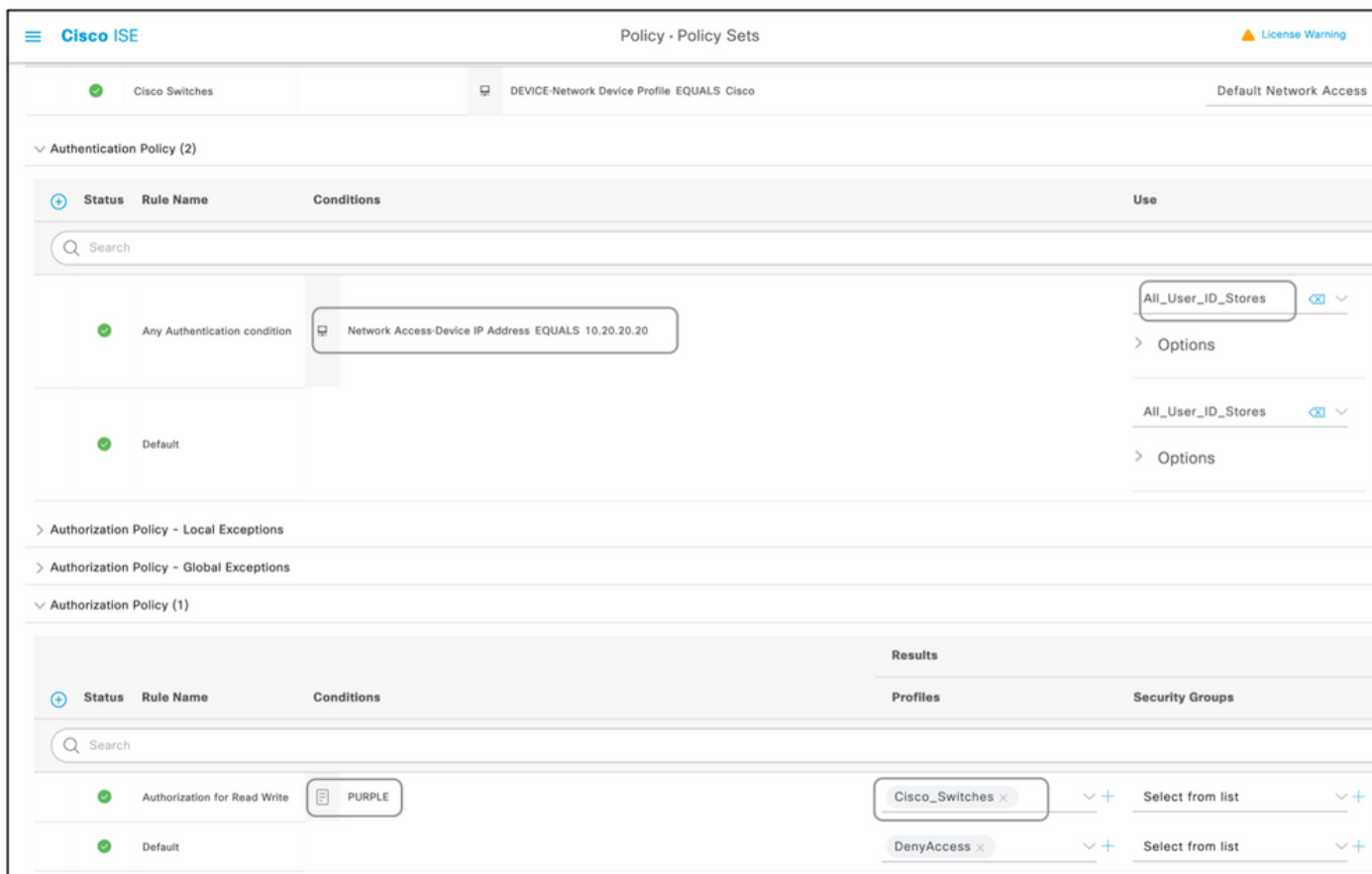
Authorization Policy (1)

Status	Rule Name	Conditions	Results	
			Profiles	Security Groups
✓	Authorization for Read Write	Admins	BlueCoat_PS_ReadWri... ⌵ +	Select from list ⌵ +
✓	Default		DenyAccess ⌵ +	Select from list ⌵ +

Cisco ISE Policy - Policy Sets License Warning

Policy Sets Reset Reset Policyset Hitcounts Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Cisco Switches		DEVICE-Network Device Profile EQUALS Cisco	Default Network Access ⌵ +	0	⚙️	➔



裝置清單

任何支援使用Radius進行裝置管理的裝置都可以增加到ISE上，只需對前面部分提到的所有步驟進行一些修改。因此，本文檔列出了使用本節所提供資訊的裝置。本檔案所提供的屬性與值清單既不詳盡，也不具權威性，且不需更新本檔案即可隨時變更。請查閱供應商網站和供應商支援以進行驗證。

聚合服務路由器(ASR)

無需為此建立單獨的詞典和VSA，因為它使用ISE上已存在的思科AV對。

屬性：cisco-av-pair

值：shell : tasks="#<role-name> , <permission> : <process>"

用法：將<role-name>的值設定為路由器上本地定義的角色名稱。角色階層可以樹狀結構來描述，其中role#roots位於樹狀結構頂端，而role#leaf會新增其他命令。這兩個角色可以合併並傳回if : shell : tasks="#root , #leaf"。

許可權也可以以個別程式為基礎傳回，這樣使用者就可以被授與特定程式的讀取、寫入和執行許可權。例如，若要授與使用者對BGP程式的讀寫許可權，請將值設為

: shell : tasks="#root , rw : bgp"。屬性的順序並不重要；無論值是設定為 toshell : tasks="#root , rw : bgp"還是 toshell : tasks="rw : bgp , #root"，結果相同。

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	cisco-av-pair	字串	shell : tasks="#root , #leaf , rwx : bgp , r : ospf"

Cisco交換機IOS®和Cisco IOS® XE

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：cisco-av-pair

值：shell : priv-lvl=<level>

使用方式：將<level>的值設定為基本上是要傳送的許可權數目。通常，如果傳送15，則表示讀寫；如果傳送7，則表示只讀。

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	cisco-av-pair	字串	shell : priv-lvl=15

BlueCoat資料包整形器

屬性：Packeteer-AVPair

值：access=<level>

使用方式：<level>是要授與的存取層級。觸控存取相當於讀寫，而瀏覽存取相當於唯讀。

使用下列值建立詞典（如本檔案所示）：

- 名稱：Packeteer
- 供應商ID：2334
- 供應商長度欄位大小：1
- 供應商型別欄位大小：1

輸入屬性的詳細資訊：

- 屬性：Packeteer-AVPair
- 描述：用於指定存取層次
- 供應商屬性ID：1
- 方向：輸出
- 允許多個：False
- 允許標籤：未選中
- 屬性型別：字串

示例：將屬性增加到授權配置檔案（用於只讀訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
------	----------	------	-----

RADIUS打包程式	打包-AVPair	字串	access=look
------------	-----------	----	-------------

示例：將屬性增加到授權配置檔案（用於讀寫訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS打包程式	打包-AVPair	字串	access=touch

BlueCoat Proxy伺服器(AV/SG)

屬性：Blue-Coat-Authorization

值：<level>

使用方式：<level>是要授與的存取層級。0表示沒有存取權，1表示唯讀存取權，而2表示讀寫存取權。Blue-Coat-Authorization屬性是負責訪問級別的屬性。

使用下列值建立詞典（如本檔案所示）：

- 名稱：BlueCoat
- 供應商ID：14501
- 供應商長度欄位大小：1
- 供應商型別欄位大小：1

輸入屬性的詳細資訊：

- 屬性：Blue-Coat-Group
- 供應商屬性ID：1
- 方向：兩者
- 允許多個：False
- 允許標籤：未選中
- 屬性型別：無符號整數32 (UINT32)

輸入第二個屬性的詳細資訊：

- 屬性：Blue-Coat-Authorization
- 描述：用於指定存取層次
- 供應商屬性ID：2
- 方向：兩者
- 允許多個：False
- 允許標籤：未選中
- 屬性型別：無符號整數32 (UINT32)

示例：將屬性增加到授權配置檔案（用於禁止訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-BlueCoat	Blue-Coat組	UINT32	0

示例：將屬性增加到授權配置檔案（用於只讀訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-BlueCoat	Blue-Coat組	UINT32	1

示例：將屬性增加到授權配置檔案（用於讀寫訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-BlueCoat	Blue-Coat組	UINT32	2

Brocade交換機

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：Tunnel-Private-Group-ID

值：U：<VLAN1>；T：<VLAN2>

用法：將<VLAN1>設定為資料VLAN的值。將<VLAN2>設定為語音VLAN的值。在本示例中，資料VLAN是VLAN 10，語音VLAN是VLAN 21。

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	Tunnel-Private-Group-ID	標籤字串	U：10；T：21

Infoblox

屬性：Infoblox-Group-Info

值：<group-name>

使用方式：<group-name>是具有授予使用者之許可權的群組的名稱。必須在Infoblox裝置上配置此組。在此配置示例中，組名稱為MyGroup。

使用下列值建立詞典（如本檔案所示）：

- 姓名：Infoblox
- 供應商ID：7779
- 供應商長度欄位大小：1
- 供應商型別欄位大小：1

輸入屬性的詳細資訊：

- 屬性：Infoblox-Group-Info
- 供應商屬性ID：009
- 方向：輸出
- 允許多個：False
- 允許標籤：未選中

- 屬性型別：字串

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Infoblox	Infoblox-Group-Info	字串	我的群組

Cisco Firepower管理中心

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：cisco-av-pair

值：Class-[25]=<role>

使用方式：將<role>的值設定為FMC上本機定義的角色名稱。在FMC上建立多個角色，例如管理員和只讀使用者，並將值分配給ISE上的屬性以同樣由FMC接收。

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	cisco-av-pair	字串	Class-[25]=NetAdmins

Nexus交換機

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：cisco-av-pair

值：shell : roles="<角色1> <角色2>"

用法：將<role1>和<role2>的值設定為交換機本地定義的角色名稱。建立多個角色時，請使用空格字元分隔角色。當多個角色從AAA伺服器傳遞回Nexus交換機時，結果使用者能夠訪問由所有三個角色的並集定義的命令。

內建角色在[配置使用者帳戶和RBAC](#)中進行定義。

示例：將屬性增加到授權配置檔案。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	cisco-av-pair	字串	shell : 角色="network-admin vdc-admin vdc-operator"

無線LAN控制器(WLC)

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：Service-Type

值：管理(6)/NAS提示(7)

使用方式：若要授與使用者對無線LAN控制器(WLC)的讀取/寫入存取權，其值必須為「管理」；若為唯讀存取權，其值必須為「NAS提示」。

有關詳細資訊，請參閱[無線LAN控制器\(WLC\)上的RADIUS伺服器管理使用者身份驗證配置示例](#)

示例：將屬性增加到授權配置檔案（用於只讀訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	服務型別	列舉	NAS提示

示例：將屬性增加到授權配置檔案（用於讀寫訪問）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	服務型別	列舉	管理

資料中心網路管理員(DCNM)

更改身份驗證方法後，必須重新啟動DCNM。否則，它可分配網路操作員許可權而不是網路管理員。

無需為此建立單獨的詞典和VSA，因為它使用ISE上已經存在的RADIUS屬性。

屬性：cisco-av-pair

值：shell：roles=<role>

DCNM角色	RADIUS Cisco-AV-Pair
使用者	shell：角色= "network-operator"
管理員	shell：角色= "network-admin"

音訊碼

屬性：ACL-Auth-Level

值：ACL-Auth-Level = 「<integer>」

使用方式：<integer>是要授與的存取層級。使用者之名稱為ACL-Auth-UserLevel的ACL-Auth-Level屬性值50，名稱為ACL-Auth-AdminLevel的ACL-Auth-Level屬性值100，名稱為ACL-Auth-SecurityAdminLevel的ACL-Auth-Level值200。可以跳過這些名稱，並且可直接將屬性的值作為授權配置檔案高級AV對的值。

使用下列值建立詞典（如本檔案所示）：

- 名稱：AudioCode

- 供應商ID : 5003
- 供應商長度欄位大小 : 1
- 供應商型別欄位大小 : 1

輸入屬性的詳細資訊：

- 屬性 : ACL-Auth-Level
- 描述 : 用於指定存取層次
- 供應商屬性ID : 35
- 方向 : 輸出
- 允許多個 : False
- 允許標籤 : 未選中
- 屬性型別 : 整數

示例：將屬性增加到授權配置檔案（針對使用者）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-AudioCode	ACL身份驗證級別	整數	50

示例：將屬性增加到授權配置檔案（針對管理員）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-AudioCode	ACL身份驗證級別	整數	100

示例：將屬性增加到授權配置檔案（用於安全管理員）。

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-AudioCode	ACL身份驗證級別	整數	200

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）。