適用於各種思科和非思科裝置的TACACS+和RADIUS屬性組態範例

目錄

簡介

本檔案將整合各種思科和非思科產品預期從驗證、授權和計量(AAA)伺服器接收的屬性；在這種情況下，AAA伺服器是存取控制伺服器(ACS)。 ACS可將這些屬性連同Access-Accept一起作為外殼配置檔案(TACACS+)或授權配置檔案(RADIUS)的一部分。

本文分步介紹了如何將自定義屬性新增到外殼配置檔案和授權配置檔案。本檔案還包含裝置清單以及裝置預期從AAA伺服器傳回的TACACS+和RADIUS屬性。所有主題均包含示例。

本文提供的屬性清單並非詳盡無遺或具有權威性，無需更新本文即可隨時更改。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據ACS版本5.2/5.3。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

建立外殼設定檔(TACACS+)

外殼配置檔案是基於TACACS+的訪問的基本許可權容器。除Cisco® IOS許可權級別、會話超時和其他引數外，您還可以指定哪些應使用Access-Accept返回的TACACS+屬性和屬性值。

完成以下步驟，將自定義屬性新增到新的外殼配置檔案：

1. 登入到ACS介面。
2. 導覽至**Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**。
3. 按一下**Create**按鈕。
4. 命名外殼配置檔案。
5. 按一下**Custom Attributes**頁籤。
6. 在「屬性」欄位中輸入**屬性名**稱。
7. 從「需求」下拉選單中選擇需求是**必備**還是**可選**。
8. 將屬性值的下拉選單設定為**Static**。如果該值為靜態，則可以在下一個欄位中輸入該值。如果該值是動態的，則不能手動輸入該屬性；而是將屬性對映到身份儲存之一中的屬性。
9. 在最後一個欄位中輸入屬性值。
10. 按一下**Add**按鈕將條目新增到表中。
11. 重複配置所需的所有屬性。
12. 按一下螢幕底部的**Submit**按鈕。

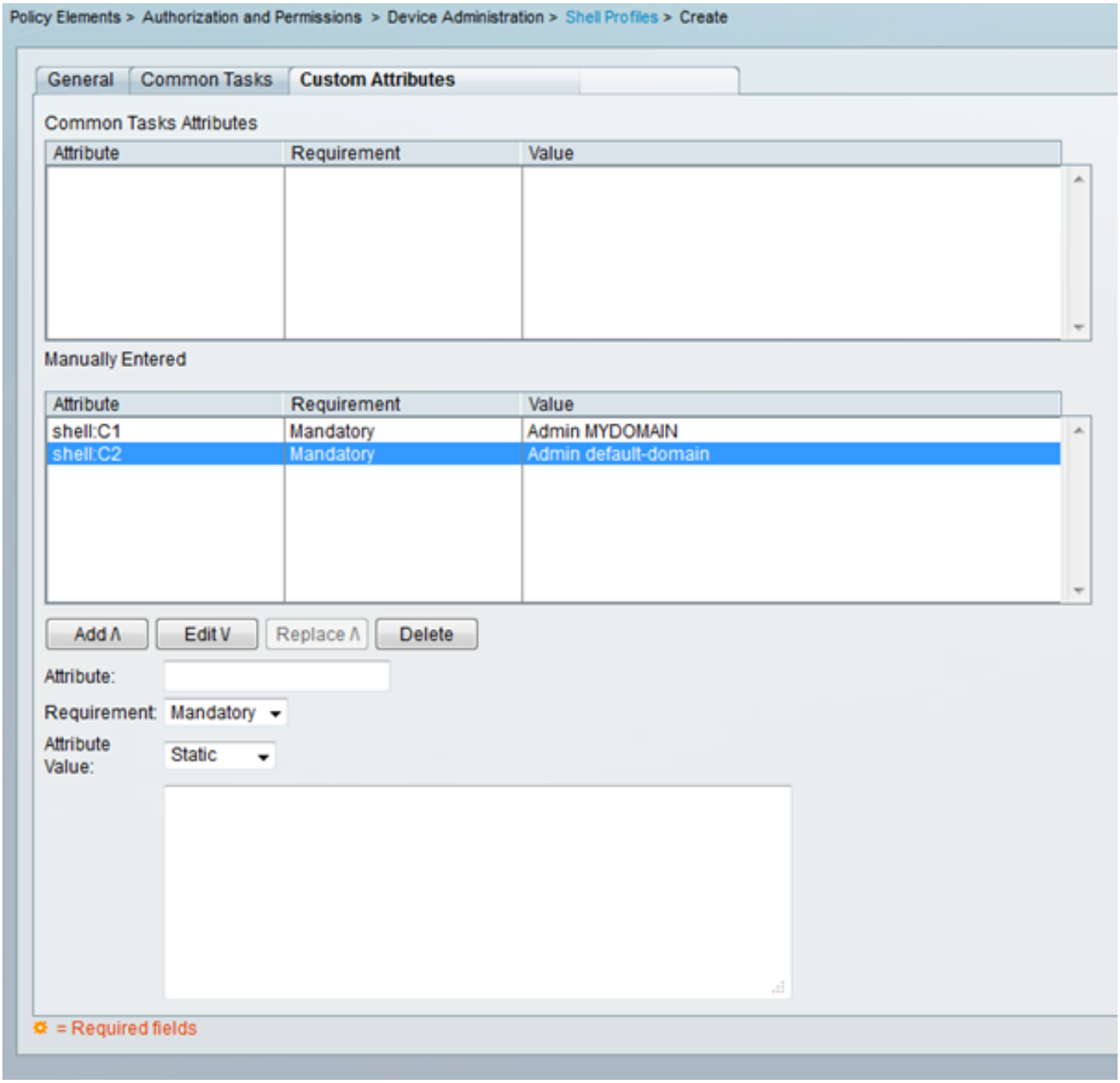
組態範例

裝置:應用程式控制引擎(ACE)

屬性： `shell:<context-name>`

值： `<role-name> <domain-name1>`

用法：角色和域由空格字元分隔。您可以配置使用者（例如USER1），使其在使用者登入到上下文（例如C1）時分配角色（例如ADMIN）和域（例如MYDOMAIN）。



建立授權設定檔(RADIUS)

授權配置檔案是基於RADIUS訪問的基本許可權容器。除了VLAN、存取控制清單(ACL)和其他引數之外，您還可以指定哪些應使用Access-Accept返回的RADIUS屬性和屬性值。

完成以下步驟，將自定義屬性新增到新的授權配置檔案：

1. 登入到ACS介面。
2. 導覽至**Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**。
3. 按一下**Create**按鈕。
4. 命名授權配置檔案。
5. 按一下**RADIUS Attributes**頁籤。
6. 從**Dictionary Type**下拉選單中選擇詞典。
7. 若要為「RADIUS屬性」欄位設定選擇屬性，請按一下**選擇**按鈕。出現一個新視窗。

8. 檢視可用的屬性，進行選擇，然後按一下**確定**。**Attribute Type**值根據您剛才選擇的屬性預設進行設定。
9. 將屬性值的下拉選單設定為**Static**。如果該值為靜態，則可以在下一個欄位中輸入該值。如果該值是動態的，則不能手動輸入該屬性；而是將屬性對映到身份儲存之一中的屬性。
10. 在最後一個欄位中輸入屬性值。
11. 按一下**Add**按鈕將條目新增到表中。
12. 重複配置所需的所有屬性。
13. 按一下螢幕底部的**Submit**按鈕。

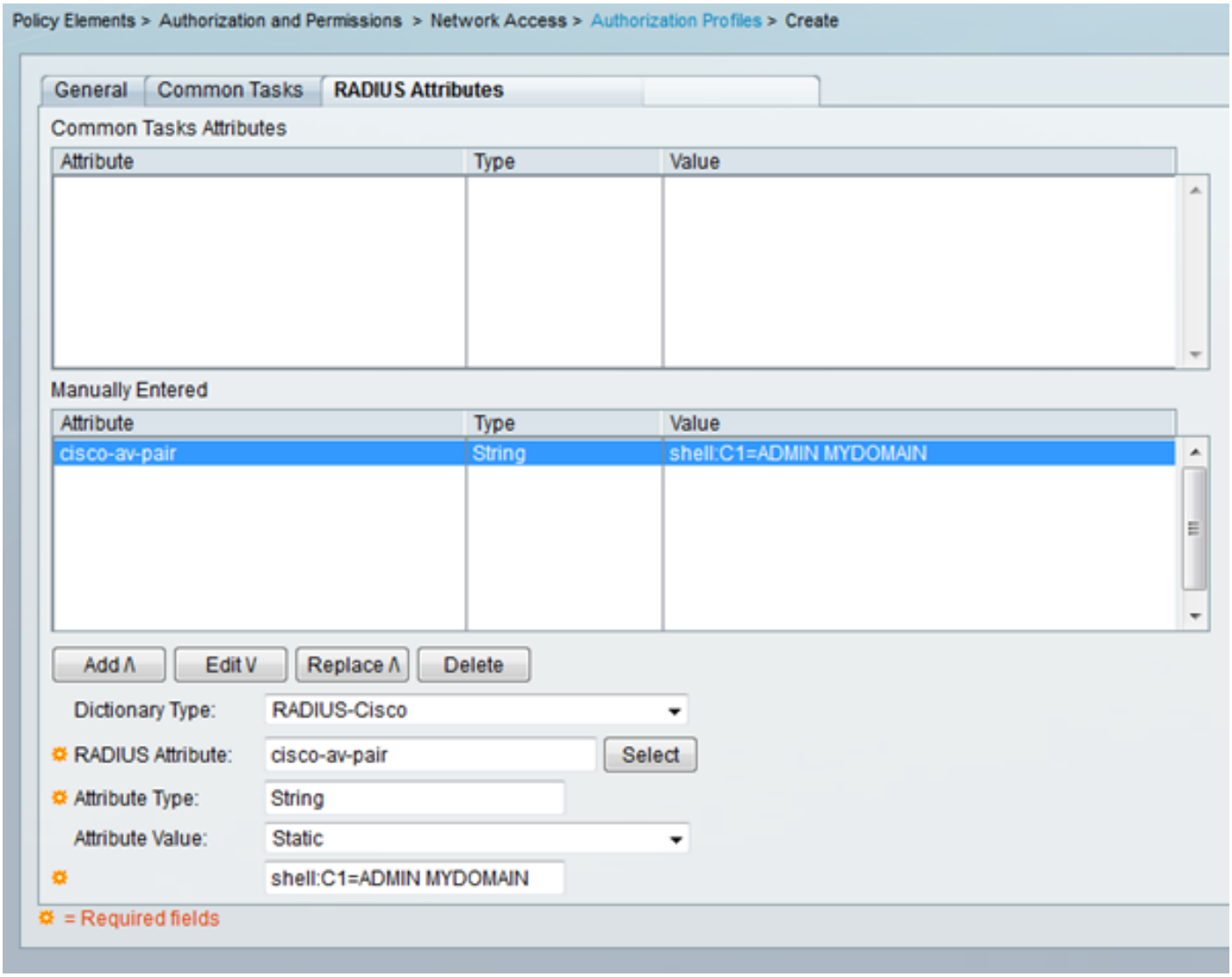
組態範例

裝置:ACE

屬性： `cisco-av-pair`

值： `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

用法：等號之後的每個值都用空格字元分隔。您可以配置使用者（例如USER1），使其在使用者登入到上下文（例如C1）時分配角色（例如ADMIN）和域（例如MYDOMAIN）。



裝置清單

聚合服務路由器(ASR)

RADIUS（授權設定檔）

屬性： `cisco-av-pair`

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

用法：將<role-name>為在路由器上本地定義的角色的名稱。角色層次結構可以用樹來描述，其中角色#root位於樹頂部，角色#leaf會新增其命令。如果出現以下情況，則可以將這兩個角色組合在一起並傳回：`shell:tasks="#root,#leaf"`。

許可權也可以基於單個進程傳回，以便授予使用者某些進程的讀取、寫入和執行許可權。例如，要授予使用者對bgp進程的讀寫許可權，請將該值設定為：`shell:tasks="#root,rw:bgp"`。 屬性的順序並不重要；無論將該值設定為`shell:tasks="#root,rw:bgp"`還是ro `shell:tasks="rw:bgp#root"`，結果都相同。

示例 — *將屬性新增到授權配置檔案*

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"`

應用程式控制引擎(ACE)

TACACS+（外殼配置檔案）

屬性： `shell:<context-name>`

值： `<role-name> <domain-name1>`

用法：角色和域由空格字元分隔。您可以配置使用者（例如USER1），使其在使用者登入到上下文（例如C1）時分配角色（例如ADMIN）和域（例如MYDOMAIN）。

示例 — *將屬性新增到外殼配置檔案*

屬性	需求	屬性值
`shell:C1`	必填	`Admin MYDOMAIN`

如果USER1通過C1情景登入，則會自動為該使用者分配ADMIN角色和MYDOMAIN域（前提是已配置授權規則，其中USER1登入後，將為其分配此授權配置檔案）。

如果USER1通過不同的上下文登入（在ACS傳送回的屬性值中未返回），則會自動為該使用者分配預設角色(Network-Monitor)和預設域(default-domain)。

RADIUS（授權設定檔）

屬性： `cisco-av-pair`

值： `shell:<context-name>=<Role-name> <domain-name1> <domain-name2>`

用法：等號之後的每個值都用空格字元分隔。您可以配置使用者（例如USER1），在使用者登入到上下文（例如C1）時為其分配角色（例如ADMIN）和域（例如MYDOMAIN）。

示例 — *將屬性新增到授權配置檔案*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	`cisco-av-pair`	字串	`shell:C1=ADMIN MYDOMAIN`

如果USER1通過C1情景登入，則會自動為該使用者分配ADMIN角色和MYDOMAIN域（前提是配置了授權規則，其中USER1登入後，將為使用者分配此授權配置檔案）。

如果USER1通過不同的上下文登入（在ACS傳送回的屬性值中未返回），則會自動為該使用者分配預設角色(Network-Monitor)和預設域(default-domain)。

BlueCoat封包成型器

RADIUS（授權設定檔）

屬性： `– AVPair`

值： `access=<level>`

用法： `<level>`是授予的訪問許可權級別。觸控訪問等效於讀寫，而檢視訪問等效於只讀。

預設情況下，ACS詞典中不存在BlueCoat VSA。要在授權配置檔案中使用BlueCoat屬性，您必須建立一個BlueCoat字典並將BlueCoat屬性新增到該字典中。

建立字典：

1. 導覽至System Administration > Configuration > Dictionaries > **Protocols** > **RADIUS** > **RADIUS VSA**。
2. 按一下「**Create**」。
3. 輸入詞典的詳細資訊：名稱:藍衣供應商ID:2334屬性字首：打包程式 —
4. 按一下「**Submit**」。

在新字典中建立屬性：

1. 導航至System Administration > Configuration > Dictionaries > Protocols > RADIUSS > **RADIUS VSA** > **BlueCoat**。
2. 按一下「**Create**」。
3. 輸入屬性的詳細資訊：屬性： `– AVPair`說明:用於指定訪問級別供應商屬性ID:1Direction:出站允許多個：假在日誌中包括屬性：已檢查屬性型別：字串
4. 按一下「**Submit**」。

範例 — *將屬性新增到授權配置檔案（用於只讀訪問）*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-BlueCoat	`Packeteer-AVPair`	字串	`access=look`

範例 — *將屬性新增到授權配置檔案（用於讀寫訪問）*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-BlueCoat	`Packeteer-AVPair`	字串	`access=touch`

Brocade交換機

RADIUS（授權設定檔）

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。在本例中，資料VLAN是VLAN 10，語音VLAN是VLAN 21。

示例 — *將屬性新增到授權配置檔案*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	`Tunnel-Private-Group-ID`	標籤的字串	`U:10,T:21`

Cisco Unity Express(CUE)

RADIUS（授權設定檔）

屬性： `cisco-av-pair`

值： `fndn:groups=<group-name>`

用法：`<group-name>`是要授予使用者許可權的組的名稱。必須在Cisco Unity Express(CUE)上配置此組。

示例 — *將屬性新增到授權配置檔案*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	`cisco-av-pair`	字串	`fndn:groups=Administrators`

Infoblox

RADIUS（授權設定檔）

屬性： `Infoblox-Group-Info`

值： `<group-name>`

用法： <group-name>是要授予使用者許可權的組的名稱。必須在Infoblox裝置上配置此組。在此配置示例中，組名稱為MyGroup。

預設情況下，Infoblox VSA在ACS詞典中不存在。為了在授權配置檔案中使用Infoblox屬性，您必須建立一個Infoblox字典並將Infoblox屬性新增到該字典中。

建立字典：

1. 導覽至System Administration > Configuration > Dictionaries > **Protocols** > **RADIUSS** > **RADIUS VSA。**
2. 按一下「**Create**」。
3. 按一下**使用高級供應商選項**旁邊的小箭頭。
4. 輸入詞典的詳細資訊：名稱: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
5. 按一下「**Submit**」。

在新字典中建立屬性：

1. 導航至System Administration > Configuration > Dictionaries > Protocols > RADIUSS > **RADIUS VSA** > **Infoblox。**
2. 按一下「**Create**」。
3. 輸入屬性的詳細資訊：屬性：`Infoblox-Group-Info`供應商屬性ID:009Direction:出站允許多個：假在日誌中包括屬性：已檢查屬性型別：字串
4. 按一下「**Submit**」。

示例 — 將屬性新增到授權配置檔案

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Infoblox	`Infoblox-Group-Info`	字串	`MyGroup`

入侵防禦系統(IPS)

RADIUS（授權設定檔）

屬性： `ips-role`

值： <>

用法：值<role name>四個入侵防禦系統(IPS)使用者角色中的任意一個：viewer、operator、administrator或service。有關授予每種使用者角色型別的許可權的詳細資訊，請參閱您的IPS版本的配置指南。

- 適用於IPS 7.0的Cisco入侵防禦系統裝置管理器配置指南
- 適用於IPS的Cisco入侵防禦系統裝置管理器配置指南7.1

示例 — 將屬性新增到授權配置檔案

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-Cisco	`cisco-av-pair`	字串	`ips-role:administrator`

Juniper

TACACS+（外殼配置檔案）

屬性： `allow-commands ;allow-configuration;local-user-name ;deny-commands ;deny-configuration;user-permissions`

值： `<allow-commands-regex>;<allow-configuration-regex>;<local-username>;<deny-commands-regex>;<deny-configuration-regex>`

用法：將`<local-username>`的值（即local-user-name屬性的值）設定為Juniper裝置上本地存在的使用者名稱。例如，當您將local-user-name屬性的值設定為JUSER時，可以將使用者（例如USER1）配置為分配給Juniper裝置上本地存在的使用者（例如JUSER）相同的使用者模板。allow-commands、allow-configuration、deny-commands和deny-configuration屬性的值可以按regex格式輸入。這些屬性被設定為的值是使用者登入類許可權位授權的操作/配置模式命令之外的值。

示例 — 向殼配置檔案1新增屬性

屬性	需求	屬性值
`allow-commands`	可選	`"(request system) | (show rip neighbor)"`
`allow-configuration`	可選	
`local-user-name`	可選	`sales`
`deny-commands`	可選	`"<^clear"`
`deny-configuration`	可選	

示例 — 向殼配置檔案2新增屬性

屬性	需求	屬性值
`allow-commands`	可選	`"monitor | help | show | ping | traceroute"`
`allow-configuration`	可選	
`local-user-name`	可選	`engineering`
`deny-commands`	可選	`"configure"`
`deny-configuration`	可選	

Nexus交換器

RADIUS（授權設定檔）

屬性： `cisco-av-pair`

值： `shell:roles="<role1> <role2>"`

用法：將<role1><role2>的值交換機本地定義的角色名稱。新增多個角色時，請使用空格字元分隔它們。當多個角色從AAA伺服器傳遞回Nexus交換機時，結果使用者有權訪問由所有三個角色聯合定義的命令。

內建角色在配置使用者帳戶和RBAC中定義。

示例 — *將屬性新增到授權配置檔案*

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

河床

TACACS+（外殼配置檔案）

屬性：;local-user-name

值：rbt-exec ;<>

用法：若要授予使用者只讀訪問許可權，必須將<username>值設定為monitor。若要授予使用者讀寫訪問許可權，<username>值必須設定為admin。如果除admin和monitor之外還定義了其他帳戶，請配置要返回的名稱。

示例 — *向外殼配置檔案新增屬性（用於只讀訪問）*

屬性	需求	屬性值
service	必填	rbt-exec
local-user-name	必填	monitor

示例 — *向外殼配置檔案新增屬性（用於讀寫訪問）*

屬性	需求	屬性值
service	必填	rbt-exec
local-user-name	必填	admin

無線區域網路控制器(WLC)

RADIUS（授權設定檔）

屬性： Service-Type

值：(6)/ NAS-Prompt(7)

用法：若要授予使用者對無線LAN控制器(WLC)的讀取/寫入存取許可權，值必須為Administrative;對於只讀訪問，該值必須為NAS-Prompt。

如需詳細資訊，請參閱無線LAN控制器(WLC)上管理使用者的RADIUS伺服器驗證組態範例

範例 — *將屬性新增到授權配置檔案（用於只讀訪問）*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	`Service-Type`	列舉	`NAS-Prompt`

範例 — *將屬性新增到授權配置檔案（用於讀寫訪問）*

詞典型別	RADIUS屬性	屬性型別	屬性值
RADIUS-IETF	`Service-Type`	列舉	`Administrative`

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，它可能分配network-operator許可權而不是network-admin。

DCNM角色	RADIUS Cisco-AV配對	Tacacs Cisco-AV配對
使用者	`shell:roles = "network-operator"`	`cisco-av-pair=shell:roles="network-operator"`
管理員	`shell:roles = "network-admin"`	`cisco-av-pair=shell:roles="network-admin"`

相關資訊

- 技術支援與文件 - Cisco Systems
- 終端存取控制器存取控制系統(TACACS+)
- 遠端驗證撥入使用者服務(RADIUS)
- 要求建議 (RFC)