

根據ISE上的vlan-id屬性配置授權策略

目錄

[簡介](#)

[使用案例](#)

[配置步驟](#)

[NAD側](#)

[ISE端](#)

[測試](#)

[NAD側](#)

[ISE端](#)

簡介

本文描述根據從NAD傳送的VLAN id屬性配置ISE授權策略的步驟。此功能僅適用於IBNS 2.0。

使用案例

客戶希望填充在訪問介面上配置的VLAN ID，並在以後使用它來提供ISE上的訪問。

配置步驟

NAD側

1.將交換機配置為在訪問請求中傳送VLAN radius屬性。

```
Device# configure terminal Device(config)# access-session attributes filter-list list TEST
Device(config-com-filter-list)# vlan-id Device(config-com-filter-list)# exit Device(config)#
access-session accounting attributes filter-spec include list TEST Device(config)# access-
session authentication attributes filter-spec include list TEST Device(config)# end
```

附註：輸入「*access-session accounting attributes filter-spec include list TEST*」命令接受遷移到IBNS 2時可能會收到警告。

```
Switch(config)#access-session accounting attributes filter-spec include list TEST This operation
will permanently convert all relevant authentication commands to their CPL control-policy
equivalents. As this conversion is irreversible and will disable the conversion CLI
'authentication display [legacy|new-style]', you are strongly advised to back up your current
configuration before proceeding. Do you wish to continue? [yes]:
```

有關詳細資訊，請檢視以下指南：[Vlan-id radius attributes config guide](#)

ISE端

1.根據需要建立身份驗證策略(MAB/DOT1X)。

2.授權策略將包含下一個條件型別，請確保與確切語法匹配

Radius-Tunnel-Private-Group-ID EQUALS (tag=1)

範例：

對於VLAN-ID = 77

Authorization Policy (21)

Status	Rule Name	Conditions	Results	Profiles
+	Vlan-Id test	Radius-Tunnel-Private-Group-ID EQUALS (tag=1) 77	PermitAccess	

測試

NAD側

```
Switch#sh run interface Tw1/0/3 Building configuration... Current configuration : 336 bytes !
interface TwoGigabitEthernet1/0/3 switchport access vlan 77 switchport mode access device-
tracking attach-policy DT_POLICY access-session host-mode multi-host access-session closed
access-session port-control auto mab dot1x pae authenticator spanning-tree portfast service-
policy type control subscriber POLICY_Tw1/0/3 end Switch#
```

```
Switch#sh auth sess inter Tw1/0/3 details Interface: TwoGigabitEthernet1/0/3 IIF-ID: 0x1FA6B281
MAC Address: c85b.768f.51b4 IPv6 Address: Unknown IPv4 Address: 10.4.18.167 User-Name: C8-5B-76-
8F-51-B4 Status: Authorized Domain: DATA Oper host mode: multi-host Oper control dir: both
Session timeout: N/A Common Session ID: 33781F0A00000AE958E57C9D Acct Session ID: 0x0000000e
Handle: 0x43000019 Current Policy: POLICY_Tw1/0/3 Local Policies: Service Template:
DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Security Policy: Should Secure Server
Policies: Method status list: Method State mab Authc Success Switch#
```

ISE端

Overview

Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
Endpoint Id	C8:5B:76:8F:51:B4 ⓘ
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Vlan-id test
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2021-11-25 21:06:55.187
Received Timestamp	2021-11-25 21:06:55.187
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
User Type	Host

Steps

11001 Received RADIUS Access-Request
11017 RADIUS created a new session
11027 Detected Host Lookup UseCase (Service-Type = Call Check (10)) **System Scan**
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15041 Evaluating Identity Policy
15048 Queried PIP - Normalised Radius.RadiusFlowType
15013 Selected Identity Source - Internal Endpoints
24209 Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4
24211 Found Endpoint in Internal Endpoints IDStore
22037 Authentication Passed
24715 ISE has not confirmed locally previous successful machine authentication for user in Active Directory
15036 Evaluating Authorization Policy
15048 Queried PIP - Radius.Tunnel-Private-Group-ID
15016 Selected Authorization Profile - PermitAccess
24209 Looking up Endpoint in Internal Endpoints IDStore - C8:5B:76:8F:51:B4
24211 Found Endpoint in Internal Endpoints IDStore
11002 Returned RADIUS Access-Accept

CiscoAVPair

```
cts-pac-opaque=****,  
service-type=Call Check,  
audit-session-id=33781F0A00000AEA58E88DB4,  
method=mab,  
client-iif-id=491113166,  
vlan-id=77
```