ISEのvlan-id属性に基づいて認可ポリシーを設定します

内容

概要
使用例
設定手順
NAD側
ISE側
テスト
NAD側
ISE側

概要

この記事では、NADから送信されるVLAN id属性に基づいてISE認可ポリシーを設定する手順について説明します。この機能は、IBNS 2.0でのみ使用できます。

使用例

お客様は、アクセスインターフェイスに設定されているVLAN IDを入力し、後でISEにアクセスを提供するためにそれを使用したいと考えています。

設定手順

NAD側

1.アクセス要求でVLAN RADIUS属性を送信するようにスイッチを設定します。

```
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
```

注：*access-session accounting attributes filter-spec include list TEST*コマンドを入力すると、*IBNS 2への移行を受け入れる際に警告が表示される場合があります。*

```
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]:
```

詳細については、次のガイドを参照してください：Vlan-id radius attributes設定ガイド

ISE側

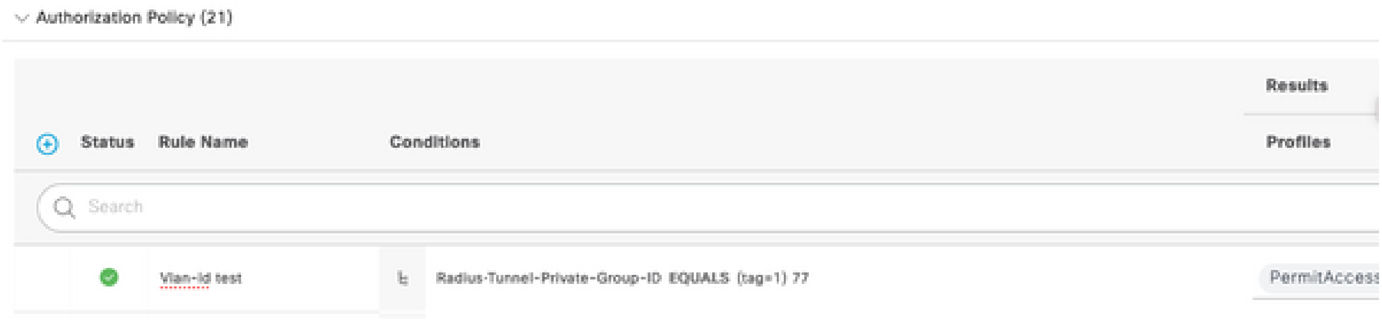
1.ニーズ(MAB/DOT1X)に基づいて認証ポリシーを作成します。

2.認可ポリシーには次の条件タイプが含まれます。正確な構文に一致することを確認してください

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

例：

VLAN-ID = 77の場合



Authorization Policy (21)

Status	Rule Name	Conditions	Results Profiles
Search			
✓	Vlan-id test	Radius·Tunnel-Private-Group-ID EQUALS (tag=1) 77	PermitAccess

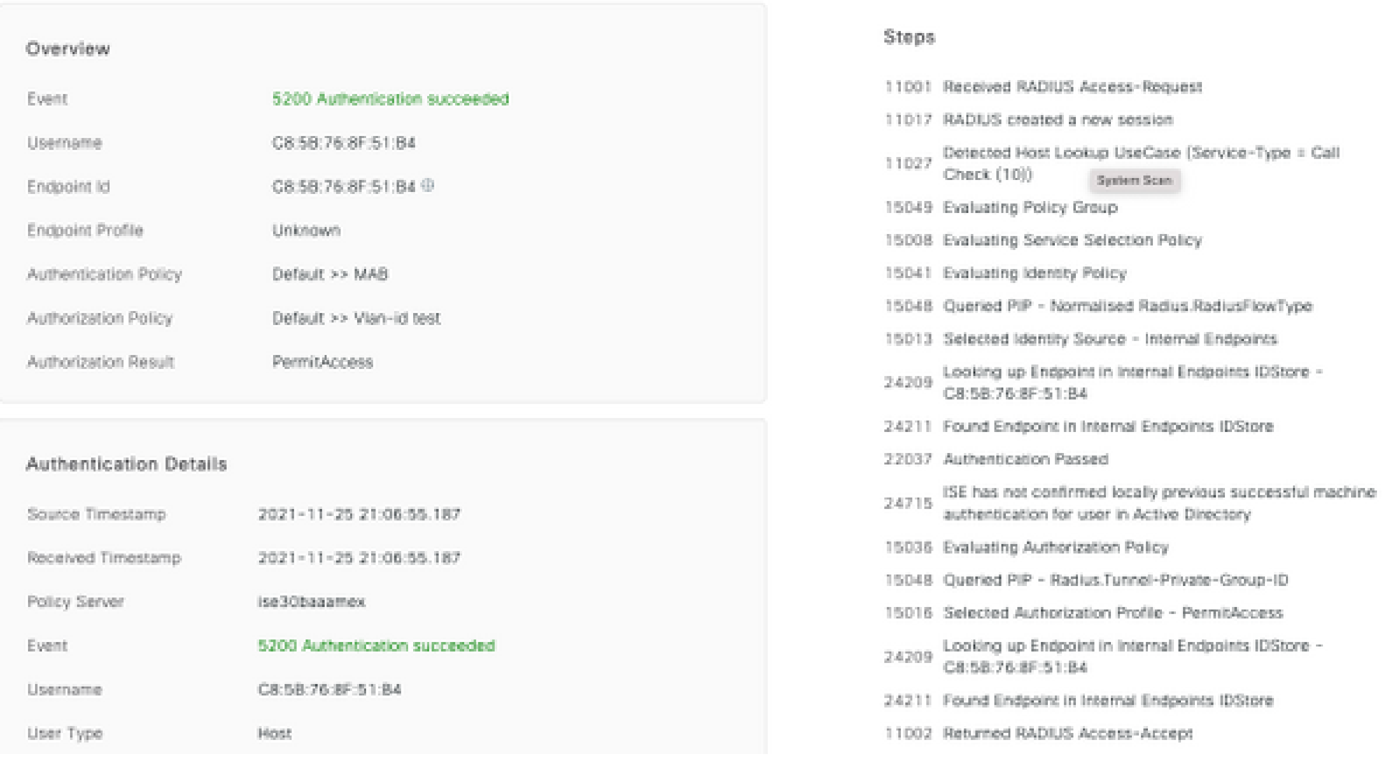
テスト

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側



Overview

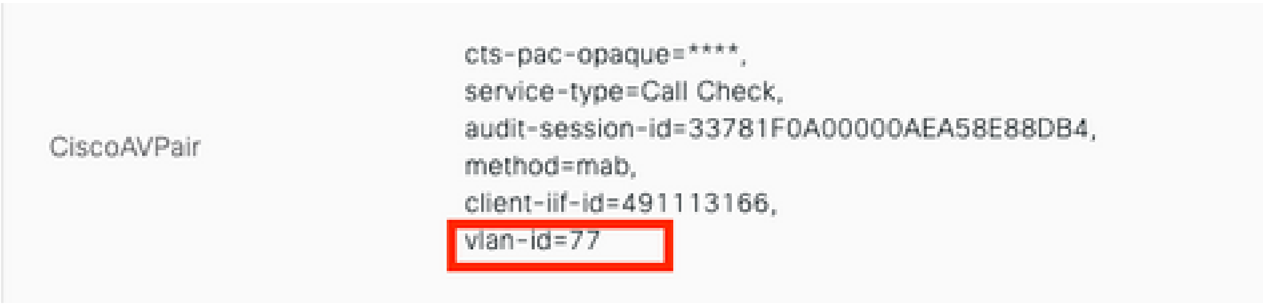
Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
Endpoint Id	C8:5B:76:8F:51:B4
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Vlan-id test
Authorization Result	PermitAccess

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