ISE의 vlan-id 특성을 기반으로 권한 부여 정책 구성

목차

소개

이 문서에서는 NAD에서 전송된 VLAN ID 특성을 기반으로 ISE 권한 부여 정책을 구성하는 단계에 대해 설명합니다. 이 기능은 IBNS 2.0에서만 사용할 수 있습니다.

활용 사례

고객은 액세스 인터페이스에 구성된 VLAN ID를 채우고 나중에 이를 사용하여 ISE에 대한 액세스를 제공하고자 합니다.

구성 단계

NAD 측

1. 액세스 요청에서 VLAN 반경 특성을 전송하도록 스위치를 구성합니다.

```
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
```

참고: *"access-session accounting attributes filter-spec include list TEST"* 명령을 입력하면 *IBNS 2로의 마이그레이션을* 수락하는 경고가 표시될 수 있습니다.

```
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]:
```

자세한 내용은 다음 설명서를 참조하십시오. Vlan-id radius attributes config guide

ISE 측

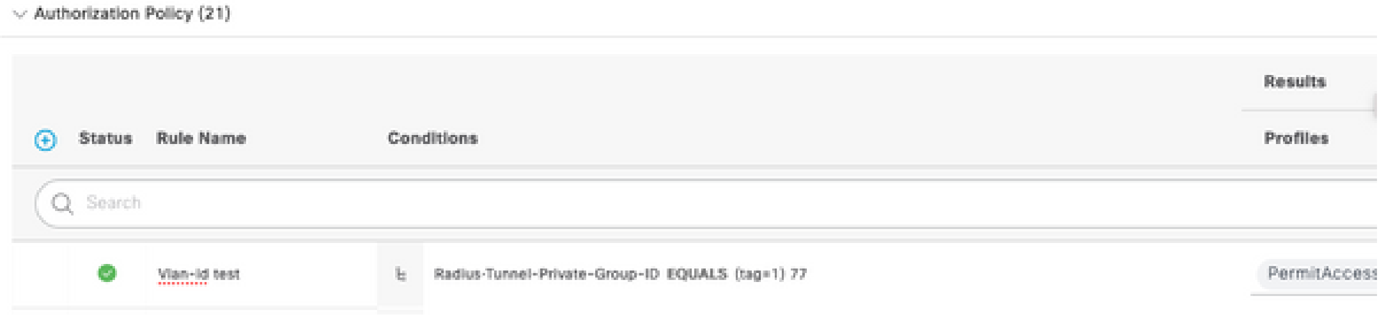
1. 필요에 따라 인증 정책을 생성합니다(MAB/DOT1X).

2. 권한 부여 정책에는 다음 조건 유형이 포함되며 정확한 구문과 일치해야 합니다.

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

예:

VLAN-ID의 경우 = 77



Authorization Policy (21)

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

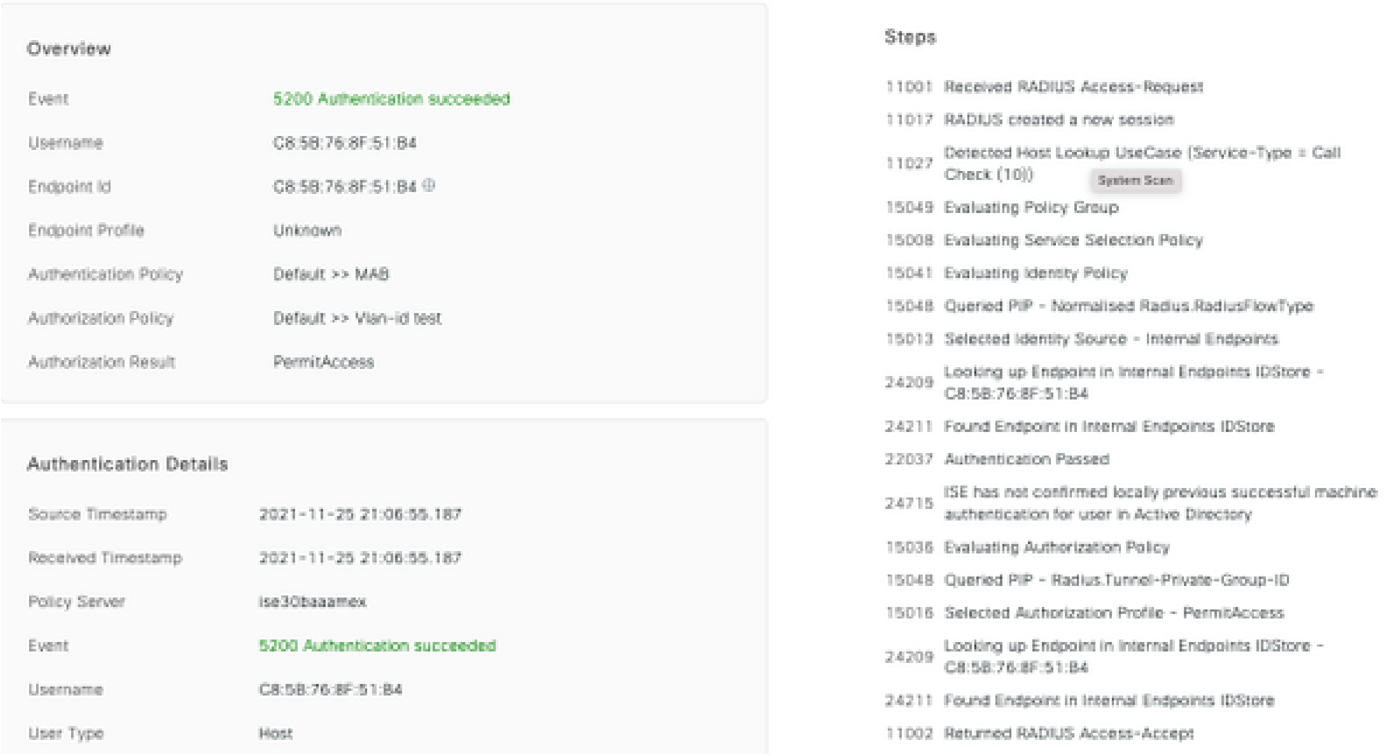
테스트

NAD 측

```
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 측



Overview

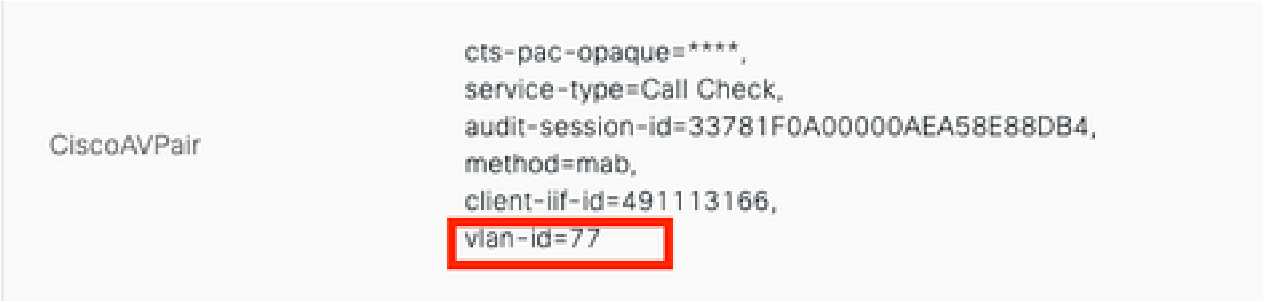
Event	5200 Authentication succeeded
Username	C8:5B:76:8F:51:B4
Endpoint Id	C8:5B:76:8F:51:B4
Endpoint Profile	Unknown
Authentication Policy	Default >> MAB
Authorization Policy	Default >> Vlan-id test
Authorization Result	PermitAccess

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