在ISE上根据vlan-id属性配置授权策略

目录

简介

本文介绍根据从NAD发送的VLAN id属性配置ISE授权策略的步骤。此功能仅适用于IBNS 2.0。

使用案例

客户希望填充在接入接口上配置的VLAN ID，然后使用它在ISE上提供访问。

配置步骤

NAD侧

1.配置交换机以在访问请求中发送VLAN RADIUS属性。

```
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
```

NOTE:输入“access-session accounting attributes filter-spec include list TEST”*命令以接受迁移到IBNS 2时*，您可能会收到警告。

```
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]:
```

有关详细信息，请参阅以下指南：Vlan-id radius属性配置指南

ISE端

1.根据您的需求创建身份验证策略(MAB/DOT1X)。

2.授权策略将包括下一种条件类型，确保与确切的语法匹配

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

示例：

对于VLAN-ID = 77

测试

NAD侧

```
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	ise30baamex
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