UCS在交换机上实施MAB/802.1x身份验证

目录

简介

本文档介绍如何在思科交换机上实施UCS C系列和MAB/802.1x身份验证。

背景

思科提供的一种访问控制技术是MAC身份验证绕行(MAB)。MAB使用设备的MAC地址来确定要提供哪种网络访问。

在包含支持IEEE 802.1X的设备和不支持IEEE 802.1X的设备的网络中，MAB可以部署为IEEE 802.1X的回退或补充机制。如果网络没有支持IEEE 802.1X的设备，MAB可以部署为独立身份验证机制。

要了解有关解决方案级使用案例、设计和分阶段部署方法的详细信息，请参阅 [MAC身份验证绕行部署指南](#)。

问题

拓扑

```
UCS (C220)mgnt interface —— gig 1/0/1[3750-X]  ——— ISE (configured for MAB)
```

不同的UCS和不同的交换机上都会发生这种情况。4500交换机上也出现了相同情况。

UCS设备(UCS-C210-M2:观察到问题)不能与MAB配合使用**access-session closed**或**no authentication** open**命令。**

工作场景

UCS管理接口连接在交换机端口上。以下是配置（工作）：

```
interface GigabitEthernet1/0/1
description DVR-UCS-dot1x-issue
switchport access vlan 300
switchport mode access
```

```
switchport voice vlan 400
ip arp inspection trust
ipv6 nd raguard
dot1x timeout quiet-period 300
dot1x timeout tx-period 5
dot1x timeout supp-timeout 5
dot1x timeout ratelimit-period 300
no mdix auto
source template ENT-TEMPLATE
spanning-tree portfast
spanning-tree guard root
end
3750# show access-sess int g1/0/1 details

Interface: GigabitEthernet1/0/1
IIF-ID: 0x102AEC0000003D7
MAC Address: 30f7.0d08.7ace
IPv6 Address: Unknown
IPv4 Address: 10.141.49.205
User-Name: 30-F7-0D-08-7A-CE
Status: Authorized
Domain: DATA
Oper host mode: multi-auth
Oper control dir: both
Session timeout: 65535s (local), Remaining: 11282s
Timeout action: Reauthenticate
Common Session ID: 0A8D31C7000017BD723AF6C2
Acct Session ID: 0x0000287D
Handle: 0x980002D5
Current Policy: ENT-IDENTITY-POL Server Policies:
ACS ACL: xACSACLx-IP-PERMIT_ALL_TRAFFIC-51134bb2
SGT Value: 12 Method status list:
Method State
dot1x Stopped
mab Authc Success
```

非工作场景

但是，当**access-session关闭时**，您无法ping通它，也无法看到access-session信息。

```
3750(config)#int g1/0/1
3750(config-if)#access-session closed
3750(config-if)#shutdown
3750(config-if)#no shutdown

May 11 16:33:14.311 JST: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to down
May 11 16:33:15.312 JST: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to down
May 11 16:33:17.891 JST: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
May 11 16:33:18.891 JST: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up


Sending 5, 100-byte ICMP Echos to 10.141.49.205, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
3750#do sh access-sess int g1/0/1 details
No sessions match supplied criteria.
```

解决方案

Debug(**debug MAB all命令**)显示交换机上未获知的UCS的MAC条目，这是向后端进行身份验证所必需的。

```
3750  (config)#  interface GigabitEthernet1/0/37
3750(config-if)#access-session control-direction in
```

输入**access-session control-direction in**命令(以前是**authentication control-direction in** 命令)，以使交换机能够将出口流量发送到主机，而不是以相反的方式发送流量。该命令通常用于不连续发送流量以发起通信的客户端（如打印机/设备）（也用于LAN唤醒）。 实际上，交换机会发送数据包，客户端会做出响应。响应将包含MAC地址，然后用于MAB。在已建立的设置中，未收到来自客户端的MAC地址。