스위치에서 MAB/802.1x 인증을 사용하는 UCS 구현

목차

소개

이 문서에서는 Cisco 스위치에 MAB/802.1x 인증을 사용하여 UCS C-Series를 구현하는 방법에 대해 설명합니다.

배경

Cisco에서 제공하는 액세스 제어 기법 중 하나는 MAB(MAC Authentication Bypass)입니다.MAB는 어떤 종류의 네트워크 액세스를 제공할 것인지 결정하기 위해 디바이스의 MAC 주소를 사용합니다.

지원하는 장치와 IEEE 802.1X를 지원하지 않는 장치를 모두 포함하는 네트워크에서 MAB를 IEEE 802.1X에 대한 대체 또는 보완적 메커니즘으로 구축할 수 있습니다.네트워크에 IEEE 802.1X 지원 디바이스가 없는 경우 MAB를 독립형 인증 메커니즘으로 구축할 수 있습니다.

솔루션 레벨 사용 사례, 설계 및 단계별 배포 방법론에 대한 자세한 내용은 [MAC Authentication Bypass 구축 가이드를 참조하십시오](#).

문제

토폴로지

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

이는 서로 다른 UCS와 다른 스위치에서 발생합니다.4500 스위치에서도 마찬가지입니다.

UCS 디바이스(UCS-C210-M2:problem observed)는 MAB에서 **access-session closed** 또는 **no authentication open** 명령을 사용하지 않습니다.

작업 시나리오

UCS 관리 인터페이스는 스위치 포트에 연결됩니다.구성(작동 중)입니다.

```
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
```

비작동 시나리오

그러나 **access-session이 닫혀** 있으면 ping할 수 없으며 access-session 정보를 볼 수 없습니다.

```
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.
```

솔루션

Debug(**debug MAB all** 명령)는 백엔드를 인증하는 데 필요한 스위치에서 학습되지 않은 UCS의 MAC 항목을 표시합니다.

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

스위치가 이그레스(egress)로 트래픽을 전송하지만 다른 방법은 허용하지 않도록 하려면 **access-session control-direction in** 명령(이전에 **authentication control-direction in** 명령)을 입력합니다.이 명령은 일반적으로 통신을 시작하는 방법으로 트래픽을 지속적으로 전송하지 않는 프린터/디바이스 등의 클라이언트에서 사용됩니다(Wake on Lan에도 사용됨). 기본적으로 패킷은 스위치에서 전송되고 클라이언트는 응답합니다.응답에는 MAB에 사용되는 MAC 주소가 포함됩니다.이미 설정된 설정에서 클라이언트의 MAC 주소를 받지 못했습니다.