UCS Implementatie met MAB/802.1x verificatie op switches

Inhoud

Inleiding

Dit document beschrijft hoe u UCS C-Series kunt implementeren met MAB/802.1x verificatie op Cisco-switches.

Achtergrond

Een van de technologie voor toegangscontrole die Cisco biedt, is MAC Verificatie Bypass (MAB). MAB gebruikt het MAC-adres van een apparaat om te bepalen welk soort netwerktoegang moet worden verleend.

In een netwerk dat zowel apparaten omvat die ondersteuning bieden als apparaten die IEEE 802.1X niet ondersteunen, kan MAB als reserve, of complementair, aan IEEE 802.1X worden ingezet. Als het netwerk geen IEEE 802.1X-compatibele apparaten heeft, kan MAB als standalone authenticatiemechanisme worden ingezet.

Om meer te weten te komen over het gebruik van een oplossing, ontwerp, en een gefaseerde implementatiemethode, zie de implementatiegids van de MAC-verificatie Bypass Deployment.

Probleem

Topologie

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

Dit gebeurt met verschillende UCS en op verschillende switches. Hetzelfde wordt waargenomen op de 4500-schakelaar.

UCS-apparaten (UCS-C210-M2: probleem waargenomen) werkt niet met MAB met **gesloten toegangssessie** of **geen authenticatie open** opdracht.

Werkscenario

De UCS Management-interface is aangesloten op switchpoort. Dit is de configuratie (in bedrijf):

```
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
```

Niet-functionerend scenario

Maar als de **toegangssessie is gesloten**, kunt u deze niet pingelen en kunt u geen informatie over de toegangssessie zien.

```
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.
```

Oplossing

Debug (**debug MAB all** opdracht) toont de MAC-ingang van UCS die niet op de schakelaar is geleerd, die vereist is om met de backend voor authentiek te verklaren.

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

Voer de **controle-richting in** de **toegangssessie in** opdracht (voorheen de **authenticatie controle-richting in** opdracht) om de schakelaar in staat te stellen om verkeer in stress naar de host te verzenden, maar niet andersom. Deze opdracht wordt meestal gebruikt op klanten zoals printers/apparaten die niet voortdurend verkeer verzenden als manier om communicatie te initiëren (ook gebruikt voor Wake on LAN). Een pakje wordt verzonden van de switch en de client reageert. Het antwoord bevat het MAC-adres dat vervolgens voor MAB wordt gebruikt. In de reeds vastgestelde instelling werd het MAC-adres van de client niet ontvangen.