Implementación de UCS con autenticación MAB/802.1x en switches

Contenido

Introducción

Este documento describe cómo implementar UCS C-Series con autenticación MAB/802.1x en switches Cisco.

Background

Una de las técnicas de control de acceso que proporciona Cisco es la derivación de autenticación MAC (MAB). MAB utiliza la dirección MAC de un dispositivo para determinar qué tipo de acceso a la red se debe proporcionar.

En una red que incluye tanto dispositivos que admiten como dispositivos que no admiten IEEE 802.1X, MAB se puede implementar como mecanismo de reserva o complementario a IEEE 802.1X. Si la red no tiene dispositivos compatibles con IEEE 802.1X, MAB se puede implementar como un mecanismo de autenticación independiente.

Para obtener más información sobre los casos prácticos de nivel de solución, el diseño y una metodología de implementación por fases, consulte Guía de implementación de omisión de autenticación MAC.

Problema

Topología

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

Esto sucede con diferentes UCS y en diferentes switches. Lo mismo se observa en el switch 4500.

Dispositivos UCS (UCS-C210-M2: problema observado) no funciona con MAB con el comando **access-session Closed** o **no authentication open**.

Escenario de trabajo

La interfaz de administración de UCS está conectada en el puerto de switch. Esta es la configuración (en funcionamiento):

```
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
```

Escenario que no funciona

Sin embargo, con **sesión de acceso cerrada**, no puede hacer ping y no puede ver información de sesión de acceso.

```
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.
```

Solución

Debug (**debug MAB all** command) muestra la entrada MAC de UCS no aprendida en el switch, que es necesaria para autenticarse con el motor.

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

Ingrese el comando **access-session control-direction in** (anteriormente el **comando authentication control-direction in**) para permitir que el switch envíe tráfico de salida al host, pero no al revés. El comando se suele utilizar en clientes como impresoras/dispositivos que no envían tráfico continuamente como una manera de iniciar la comunicación (también se utiliza para Wake on Lan). Esencialmente, se envía un paquete desde el switch y el cliente responde. La respuesta contendrá la dirección MAC que luego se utiliza para MAB. En la configuración ya establecida, la dirección MAC del cliente no estaba siendo recibida.