Implementação do UCS com autenticação MAB/802.1x em switches

Contents

Introduction

Este documento descreve como implementar o UCS C-Series com autenticação MAB/802.1x em switches Cisco.

Background

Uma das técnicas de controle de acesso fornecidas pela Cisco é o MAC Authentication Bypass (MAB). O MAB usa o endereço MAC de um dispositivo para determinar que tipo de acesso à rede deve ser fornecido.

Em uma rede que inclui dispositivos que suportam e dispositivos que não suportam IEEE 802.1X, o MAB pode ser implantado como mecanismo de fallback ou complementar para o IEEE 802.1X. Se a rede não tiver nenhum dispositivo compatível com IEEE 802.1X, o MAB pode ser implantado como um mecanismo de autenticação independente.

Para saber mais sobre casos de uso, design e uma metodologia de implantação em fases no nível da solução, consulte Guia de implantação de desvio de autenticação MAC.

Problema

Topologia

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

Isso acontece com o UCS diferente e em switches diferentes. O mesmo se observa no switch 4500.

Dispositivos UCS (UCS-C210-M2: problema observado) não funciona com MAB com **access-session closed** ou **nenhum** comando **de autenticação aberta**.

Cenário de trabalho

A interface de gerenciamento do UCS é conectada na porta do switch. Esta é a configuração (em funcionamento):

```
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
```

Cenário inoperante

No entanto, com **sessão de acesso fechada**, você não pode fazer ping e não pode ver informações da sessão de acesso.

```
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.
```

Solução

Debug (**debug MAB all** command) mostra a entrada MAC do UCS não aprendido no switch, que é necessário para autenticar com o backend.

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

Insira o **comando access-session control-direction in** (anteriormente o **comando authentication control-direction in**) para permitir que o switch envie o tráfego de saída para o host, mas não o contrário. O comando geralmente é usado em clientes como impressoras/dispositivos que não enviam tráfego continuamente como uma forma de iniciar a comunicação (também usada para Wake on Lan). Essencialmente, um pacote é enviado do switch e o cliente responde. A resposta conterá o endereço MAC que é usado para MAB. Na configuração já estabelecida, o endereço MAC do cliente não estava sendo recebido.