UCS-Implementierung mit MAB/802.1x-Authentifizierung auf Switches

Inhalt

Einführung

Dieses Dokument beschreibt die Implementierung der UCS C-Serie mit MAB/802.1x-Authentifizierung auf Cisco Switches.

Hintergrund

Eine der von Cisco bereitgestellten Methoden zur Zugriffskontrolle ist MAB (MAC Authentication Bypass). MAB verwendet die MAC-Adresse eines Geräts, um die Art des Netzwerkzugriffs zu bestimmen.

In einem Netzwerk, das sowohl Geräte unterstützt als auch Geräte, die IEEE 802.1X nicht unterstützen, kann MAB als Fallback- oder ergänzender Mechanismus für IEEE 802.1X bereitgestellt werden. Wenn das Netzwerk über keine IEEE 802.1X-fähigen Geräte verfügt, kann MAB als eigenständiger Authentifizierungsmechanismus bereitgestellt werden.

Weitere Informationen zu Anwendungsfällen, Designs und einer schrittweisen Bereitstellungsmethode auf Lösungsebene finden Sie im [Bereitstellungsleitfaden zur MAC Authentication Bypass-Authentifizierung](#).

Problem

Topologie

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

Dies geschieht mit unterschiedlichen UCS- und Switches. Dies gilt auch für den Switch 4500.

UCS-Geräte (UCS-C210-M2: Problem beobachtet) funktioniert nicht mit MAB bei **geschlossener Zugriffssitzung** oder **ohne** Befehl **zur offenen Authentifizierung**.

Arbeitsszenario

Die UCS-Verwaltungsschnittstelle ist über den Switch-Port verbunden. Dies ist die Konfiguration (funktioniert):

```
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
```

Nichterwerbstätiges Szenario

Wenn die **Zugriffssitzung geschlossen** ist, können Sie jedoch keinen Ping senden und keine Informationen zu Zugriffssitzungen anzeigen.

```
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.
```

Lösung

Debug (**debug MAB all** Befehl) zeigt den MAC-Eintrag des UCS an, der auf dem Switch nicht erfasst wurde. Dieser muss mit dem Backend authentifiziert werden.

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

Geben Sie den Befehl **access-session control-direction in** (zuvor den Befehl **authentication control-direction in**) ein, damit der Switch Datenverkehr an den Host senden kann, jedoch nicht umgekehrt. Der Befehl wird in der Regel auf Clients wie Druckern/Geräten verwendet, die nicht ständig Datenverkehr senden, um die Kommunikation zu initiieren (wird auch für Wake on Lan verwendet). Im Wesentlichen wird ein Paket vom Switch gesendet, und der Client antwortet. Die Antwort enthält die MAC-Adresse, die dann für MAB verwendet wird. In der bereits eingerichteten Konfiguration wurde die MAC-Adresse vom Client nicht empfangen.