Implementazione UCS con autenticazione MAB/802.1x sugli switch

Sommario

Introduzione

In questo documento viene descritto come implementare la serie C UCS con autenticazione MAB/802.1x sugli switch Cisco.

Sfondo

Una delle tecniche di controllo dell'accesso fornite da Cisco è MAC Authentication Bypass (MAB). MAB utilizza l'indirizzo MAC di un dispositivo per determinare il tipo di accesso alla rete da fornire.

In una rete che include sia dispositivi che supportano sia dispositivi che non supportano IEEE 802.1X, MAB può essere distribuito come meccanismo di fallback o complementare a IEEE 802.1X. Se la rete non dispone di dispositivi compatibili con IEEE 802.1X, è possibile distribuire MAB come meccanismo di autenticazione standalone.

Per ulteriori informazioni sui casi di utilizzo a livello di soluzione, sulla progettazione e sulla metodologia di distribuzione per fasi, vedere MAC Authentication Bypass Deployment Guide.

Problema

Topologia

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

Ciò accade con UCS diversi e su switch diversi. Lo stesso avviene sullo switch 4500.

Dispositivi UCS (UCS-C210-M2: (problema rilevato) non funziona con MAB con il comando **access-session closed** o **no authentication open**.

Scenario di lavoro

L'interfaccia di gestione UCS è connessa a switchport. Questa è la configurazione (funzionante):

```
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
```

Scenario non lavorativo

Tuttavia, quando la sessione di **accesso è chiusa**, non è possibile eseguirne il ping e non è possibile visualizzare le informazioni sulla sessione di accesso.

```
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.
```

Soluzione

Il comando debug (**debug MAB all**) visualizza la voce MAC dell'UCS non appresa sullo switch, necessaria per l'autenticazione sul back-end.

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

Immettere il comando **access-session control-direction** (in precedenza **authentication control-direction**) per consentire allo switch di inviare il traffico in uscita all'host, ma non il contrario. Il comando viene in genere utilizzato su client quali stampanti/dispositivi che non inviano continuamente traffico come metodo per avviare la comunicazione (utilizzato anche per Wake on Lan). Essenzialmente, un pacchetto viene inviato dallo switch e il client risponde. La risposta conterrà l'indirizzo MAC che verrà utilizzato per MAB. Nella configurazione già stabilita, l'indirizzo MAC del client non è stato ricevuto.