Implémentation UCS avec authentification MAB/802.1x sur les commutateurs

Contenu

Introduction

Ce document décrit comment mettre en oeuvre UCS série C avec l'authentification MAB/802.1x sur les commutateurs Cisco.

Fond

L'une des techniques de contrôle d'accès fournies par Cisco est le contournement de l'authentification MAC (MAB). MAB utilise l'adresse MAC d'un périphérique afin de déterminer le type d'accès réseau à fournir.

Dans un réseau qui comprend à la fois des périphériques qui prennent en charge et des périphériques qui ne prennent pas en charge la norme IEEE 802.1X, la MAB peut être déployée comme mécanisme de secours ou complémentaire à la norme IEEE 802.1X. Si le réseau ne comporte aucun périphérique compatible IEEE 802.1X, le MAB peut être déployé comme mécanisme d'authentification autonome.

Afin d'en savoir plus sur les utilisations au niveau de la solution, la conception et une méthodologie de déploiement échelonné, consultez Guide de déploiement de contournement d'authentification MAC.

Problème

Topologie

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

Cela se produit avec différents UCS et sur différents commutateurs. Il en est de même sur le commutateur 4500.

Périphériques UCS (UCS-C210-M2 : problème observé) ne fonctionne pas avec MAB avec la commande **access-session close** ou **no authentication open**.

Scénario de travail

L'interface de gestion UCS est connectée au port de commutation. Voici la configuration (qui fonctionne) :

```
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
```

Scénario de non-travail

Cependant, lorsque **la session d'accès est fermée**, vous ne pouvez pas lui envoyer de requête ping et ne pouvez pas voir les informations de session d'accès.

```
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.
```

Solution

Debug (**debug MAB all** command) affiche l'entrée MAC d'UCS non apprise sur le commutateur, qui est nécessaire pour s'authentifier avec le serveur principal.

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

Entrez la commande **access-session control-direction in** (précédemment la commande **authentication control-direction in**) afin de permettre au commutateur d'envoyer le trafic en sortie à l'hôte, mais pas l'inverse. La commande est généralement utilisée sur les clients tels que les imprimantes/périphériques qui n'envoient pas continuellement le trafic comme moyen d'initier la communication (également utilisé pour Wake on Lan). Essentiellement, un paquet est envoyé à partir du commutateur et le client répond. La réponse contient l'adresse MAC qui est ensuite utilisée pour MAB. Dans la configuration déjà établie, l'adresse MAC du client n'a pas été reçue.