Dépanner le CPU élevé sur les commutateurs avec dot1x/Mab en raison de EAP Framework et AAA Manager

Contenu

Introduction

Ce document décrit comment dépanner le CPU/la mémoire élevée en raison du cadre EAP (Extensible Authentication Protocol) et du gestionnaire AAA (Authentication, Authorization, and Accounting). Ceci est visible sur les commutateurs qui utilisent l'authentification dot1x/mab.

Informations générales

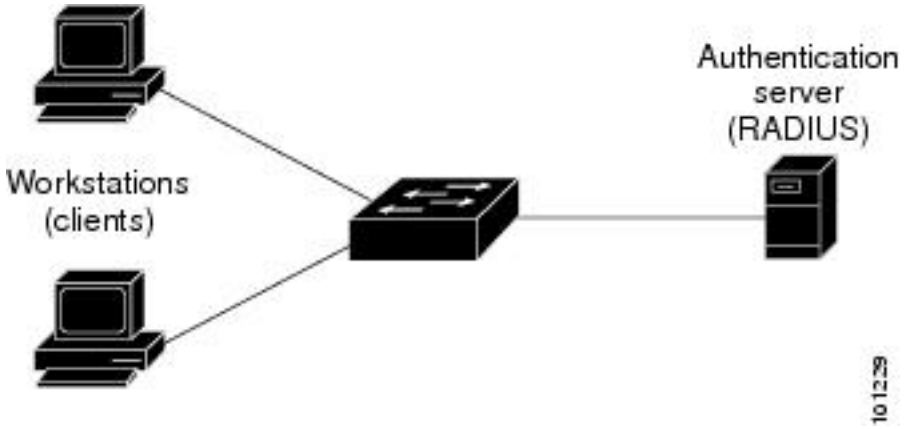
Cisco IOS Auth Manager gère les demandes d'authentification réseau et applique les stratégies d'autorisation quelle que soit la méthode d'authentification. Le gestionnaire d'authentification gère les données opérationnelles pour toutes les tentatives de connexion réseau basées sur les ports, les authentifications, les autorisations et les déconnexions et fait office de gestionnaire de session.

Le commutateur agit comme un intermédiaire (proxy) entre le client et le serveur d'authentification, il demande des informations d'identité au client, vérifie ces informations avec le serveur d'authentification et relaie une réponse au client. Le commutateur inclut le client RADIUS, qui encapsule et décapsule les trames EAP et interagit avec le serveur d'authentification.

Configuration

Cette section présente un commutateur Cisco qui effectue l'authentification MAB/DOT1X (MAC AuthenticationBypass).

Vous devez comprendre les concepts du contrôle d'accès réseau basé sur les ports et comprendre comment configurer le contrôle d'accès réseau basé sur les ports sur votre plate-forme Cisco. Cette image illustre les stations de travail qui ont une authentification dot1x/MAB.



Voici un exemple de configuration :

```
interface FastEthernet0/8
 switchport access vlan 23
 switchport mode access
 switchport voice vlan 42
 authentication host-mode multi-domain
 authentication order mab dot1x
 authentication priority mab dot1x---> Priority order
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate <value in sec>---->(Time after which the client auth would
be re-negotiated)
authentication violation protect mab mls qos trust dscp dot1x pae authenticator dot1x timeout
tx-period 3 storm-control broadcast level 2.00 no cdp enable spanning-tree portfast spanning-
tree bpduguard enable service-policy input Marking end
```

Dépannage

Les commutateurs qui utilisent l'authentification dot1x/MAB ont parfois des pics élevés de CPU/mémoire en raison du cadre EAP et du gestionnaire AAA. Cela peut avoir un impact sur la production puisque les demandes d'authentification sont abandonnées.

Pour résoudre ce problème, il est recommandé de procéder comme suit :

Étape 1. Entrez la commande **show proc cpu sort** afin de vérifier l'utilisation élevée du CPU sur le commutateur et assurez-vous que les processus EAP Framework et Auth Manager ont l'utilisation la plus élevée comme indiqué dans cet exemple :

```
PU utilization for five seconds:

97%

/2%; one minute: 90%; five minutes: 89%
PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
149   178566915 140683416       1269

64.04% 47.11% 45.63%   0 EAP Framework


141   130564594  55418491       2355

21.61% 29.05% 29.59%   0 Auth Manager
```

```
121   305295906 487695245        519  1.74%  1.84%  1.78%   0 Hulc LED Process
144    12070918  31365536        384  0.63%  0.43%  0.49%   0 MAB Framework
258   117344878 885817567        132  0.47%  0.79%  0.86%   0 RADIUS
```

Étape 2. Vérifiez l'utilisation de la mémoire sur le commutateur pour des processus tels que Auth Manager et RADIUS à l'aide de la commande **show process cpu memory**, comme indiqué dans cet exemple.

```
Processor Pool Total:   22559064 Used:   16485936 Free:    6073128
      I/O Pool Total:    4194304 Used:    2439944 Free:    1754360
Driver te Pool Total:    1048576 Used:         40 Free:    1048536

PID TTY  Allocated      Freed    Holding    Getbufs    Retbufs Process
   0   0   29936164   13273256   13856236          0          0 *Init*
   0   0   34797632   32603736    1091560    2481468     263240 *Dead*
  59   0     366860       6760     317940          0          0 Stack Mgr Notifi
141   0

 569580564 3357129696

174176    2986956

          0

Auth Manager


258   0

1212276148 2456764884     140684   21066696

          0

RADIUS


131   0  552345134 541235441      90736      20304          0 HRPC qos reque
```

Étape 3. Si vous faites face à une utilisation élevée des ressources sur le commutateur, vous pouvez voir les journaux suivants pour les échecs d'authentification comme indiqué :

Entrez la commande **show logging**.

```
%DOT1X-5-FAIL: Authentication failed for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A733402000000224870C28AA
%AUTHMGR-7-RESULT:

Authentication result 'no-response'

 from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17 AuditSessionID
0A733402000000224870C28AA
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A733402000000224870C28AA
```

Étape 4. Définissez le compteur de réauthentification sur une valeur supérieure (par exemple, 3 600 secondes) afin de vous assurer que vous ne vous authentifiez pas fréquemment pour les clients, ce qui augmente la charge sur le commutateur.

Afin de valider la configuration, entrez la commande **show run interface <interface-name>** :

```
interface FastEthernet0/8
switchport access vlan 23
switchport mode access
switchport voice vlan 42
authentication host-mode multi-domain
authentication order mab dot1x
authentication priority mab dot1x
authentication port-control auto
authentication periodic


authentication timer reauthenticate 60---------->Make sure we do not have any

 aggressive timers set
authentication violation protect
```

Étape 5. Déterminez le nombre de sessions vues pour les processus MAB/dot1x, car parfois un nombre élevé de sessions authentifiées peut également conduire à un CPU élevé. Afin de vérifier le nombre de sessions actives, entrez ces commandes :

```
SW#

show authentication registrations


Auth Methods registered with the Auth Manager:
  Handle  Priority  Name
    100       0      dot1x
    3         1      mab
    1         2      webauth



SW#Show authentication method dot1x


SW#Show authentication method mab

SW#Show authentication sessions
```

Étape 6. Afin de vérifier la version et les bogues potentiels, entrez la commande **show version**.

Si le bogue n'est pas répertorié dans la section « Bugs », ouvrez un dossier auprès du Centre d'assistance technique (TAC) et joignez tous les journaux des étapes 1 à 5.

Bugs

CSCus46997 Fuite de mémoire et UC élevée dans IP Host Track et Auth Manager

CSCtz06177 Un catalyseur 2960 peut manquer de mémoire.

CSCty49762 EAP Framework et AAA AttrL sous-utilisent toute la mémoire de processus

Astuce : Pour plus de détails, référez-vous aux ID de bogue Cisco CSCus46997, CSCtz06177 et CSCty49762.