Risoluzione dei problemi di CPU alta sugli switch con dot1x/Mab a causa di EAP Framework e AAA Manager

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a CPU/memoria elevata dovuta al framework EAP (Extensible Authentication Protocol) e al gestore di autenticazione, autorizzazione e accounting (AAA). Questa condizione viene rilevata sugli switch che usano l'autenticazione dot1x/mab.

Premesse

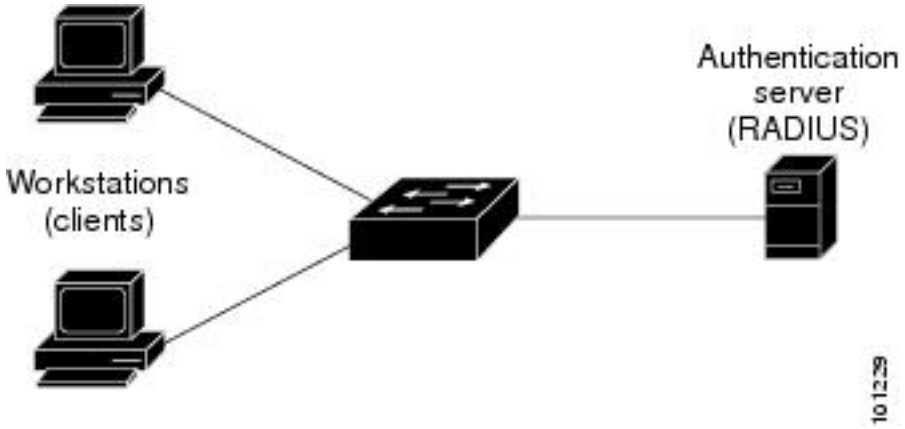
Cisco IOS Auth Manager gestisce le richieste di autenticazione di rete e applica i criteri di autorizzazione indipendentemente dal metodo di autenticazione. Auth Manager gestisce i dati operativi per tutti i tentativi di connessione alla rete basati su porta, le autenticazioni, le autorizzazioni e le disconnessioni e funge da gestore della sessione.

Lo switch funge da intermediario (proxy) tra il client e il server di autenticazione, richiede informazioni sull'identità al client, verifica tali informazioni con il server di autenticazione e invia una risposta al client. Lo switch include il client RADIUS, che incapsula e decapsula i frame EAP e interagisce con il server di autenticazione.

Configurazione

In questa sezione viene mostrato uno switch Cisco con autenticazione MAB/DOT1X (MAC AuthenticationBypass).

Ènecessario comprendere i concetti di controllo degli accessi alla rete basato sulle porte e configurare il controllo degli accessi alla rete basato sulle porte sulla piattaforma Cisco in uso. Nell'immagine sono illustrate le workstation con autenticazione dot1x/MAB.



Di seguito è riportata una configurazione di esempio:

```
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
```

Risoluzione dei problemi

Gli switch che usano l'autenticazione dot1x/MAB a volte hanno picchi elevati di CPU/memoria a causa del framework EAP e del manager AAA. Questo può influire sulla produzione poiché le richieste di autenticazione vengono eliminate.

Per risolvere questo problema, si consiglia di effettuare le seguenti operazioni:

Passaggio 1. Immettere il comando **show proc cpu sort** per controllare l'utilizzo elevato della CPU sullo switch e assicurarsi che i processi EAP Framework e Auth Manager abbiano l'utilizzo più elevato, come mostrato nell'esempio:

```
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
```

Passaggio 2. Controllare l'utilizzo della memoria sullo switch per individuare processi quali Auth Manager e RADIUS con il comando **show process cpu memory**, come mostrato nell'esempio.

```
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
```

Passaggio 3. Se si verifica un elevato utilizzo delle risorse sullo switch, è possibile che vengano visualizzati i seguenti log per gli errori di autenticazione, come mostrato:

Immettere il comando **show logging**.

```
%DOT1X-5-FAIL: Authentication failed for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A73340200000224870C28AA
%AUTHMGR-7-RESULT:

Authentication result 'no-response'

 from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17 AuditSessionID
0A73340200000224870C28AA
%AUTHMGR-7-FAILOVER: Failing over from 'dot1x' for client (7446.a04b.1495) on Interface Fa0/17
AuditSessionID 0A73340200000224870C28AA
```

Passaggio 4. Impostare il timer di riautenticazione su un valore più alto (ad esempio, 3600 secondi) per garantire che non si esegua frequentemente l'autenticazione per i client, con conseguente aumento del carico sullo switch.

Per convalidare la configurazione, immettere il comando **show run interface <nome-interfaccia>**:

```
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
```

Passaggio 5. Determinare il numero di sessioni visualizzate per i processi MAB/dot1x, in quanto a volte un numero elevato di sessioni autenticate può portare a un CPU elevato. Per controllare il numero di sessioni attive, immettere i seguenti comandi:

```
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
```

Passaggio 6. Per controllare la versione e i potenziali bug, immettere il comando **show version**.

Se il bug non è elencato nella sezione "Bug", aprire una richiesta con il Technical Assistance Center (TAC) e allegare tutti i registri dai passaggi da 1 a 5.

Bug

Perdita di memoria e CPU elevata in CSCus46997 IP Host Track e Auth Manager

CSCtz06177 La memoria di un Catalyst 2960 potrebbe essere insufficiente.

CSCty49762 EAP Framework e AAA AttrL Sub utilizzano tutta la memoria di processo

Suggerimento: Per ulteriori informazioni, fare riferimento agli ID bug Cisco CSCus46997, CSCtz06177 e CSCty49762.