Fehlerbehebung bei hoher CPU auf Switches mit dot1x/mab aufgrund von EAP-Framework und AAA-Manager

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie eine Fehlerbehebung bei hoher CPU/Speicher aufgrund des Extensible Authentication Protocol (EAP)-Frameworks und des Authentication, Authorization, and Accounting (AAA)-Managers durchführen. Dies zeigt sich bei Switches, die die 802.1x/mab-Authentifizierung verwenden.

Hintergrundinformationen

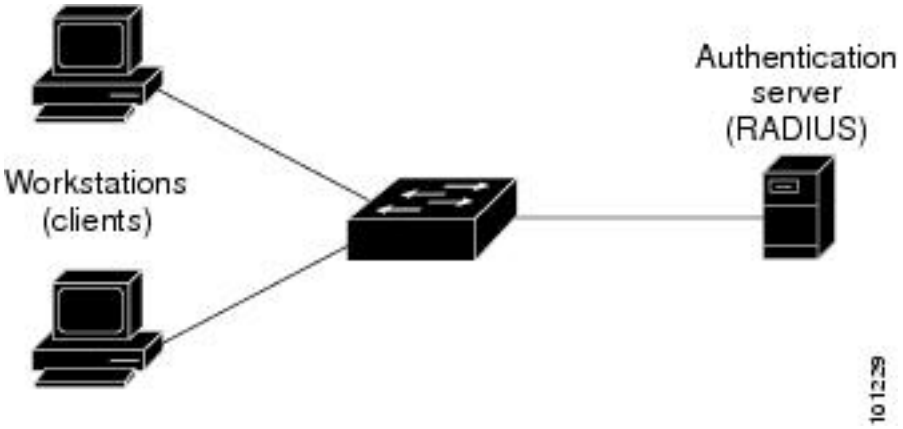
Der Cisco IOS Auth Manager verarbeitet Authentifizierungsanfragen im Netzwerk und setzt Autorisierungsrichtlinien unabhängig von der Authentifizierungsmethode durch. Der Auth Manager verwaltet Betriebsdaten für alle Port-basierten Netzwerkverbindungsversuche, -authentifizierungen, -autorisierungen und -trennungen und fungiert als Sitzungsmanager.

Der Switch agiert als Vermittler (Proxy) zwischen dem Client und dem Authentifizierungsserver, er fordert Identitätsinformationen vom Client an, verifiziert diese Informationen mit dem Authentifizierungsserver und leitet eine Antwort an den Client weiter. Der Switch umfasst den RADIUS-Client, der die EAP-Frames kapselt und entkapselt und mit dem Authentifizierungsserver interagiert.

Konfiguration

Dieser Abschnitt zeigt einen Cisco Switch, der die MAB/DOT1X-Authentifizierung (MAC AuthenticationBypass) durchführt.

Sie sollten die Konzepte der portbasierten Netzwerkzugriffskontrolle verstehen und wissen, wie Sie die portbasierte Netzwerkzugriffskontrolle auf Ihrer Cisco Plattform konfigurieren. Dieses Bild zeigt Workstations mit dot1x/MAB-Authentifizierung.



Dies ist eine Beispielkonfiguration:

```
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
```

Fehlerbehebung

Switches, die die 802.1x/MAB-Authentifizierung verwenden, weisen aufgrund des EAP-Framework- und AAA-Managers manchmal hohe CPU-/Speicherspitzen auf. Dies kann sich auf die Produktion auswirken, da Authentifizierungsanforderungen verworfen werden.

Zur Lösung dieses Problems werden folgende Schritte empfohlen:

Schritt 1: Geben Sie den Befehl **show proc cpu sort** ein, um die hohe CPU-Auslastung auf dem Switch zu überprüfen und sicherzustellen, dass die EAP Framework- und Auth-Verwaltungsprozesse die höchste Auslastung aufweisen, wie in diesem Beispiel gezeigt:

```
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
```

Schritt 2: Überprüfen Sie die Speichernutzung auf dem Switch auf Prozesse wie Auth Manager und RADIUS mit dem Befehl **show process cpu memory** wie in diesem Beispiel gezeigt.

```
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
```

Schritt 3: Wenn der Switch eine hohe Ressourcenauslastung aufweist, werden möglicherweise die folgenden Protokolle für die Authentifizierungsfehler angezeigt, wie gezeigt:

Geben Sie den Befehl **show logging ein**.

```
%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
```

Schritt 4: Stellen Sie den Timer für die erneute Authentifizierung auf einen höheren Wert ein (z. B. 3600 Sekunden), um sicherzustellen, dass Sie sich nicht häufig für die Clients authentifizieren, was die Last für den Switch erhöht.

Um die Konfiguration zu validieren, geben Sie den Befehl **show run interface <interface-name>** ein:

```
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
```

Schritt 5: Stellen Sie fest, wie viele Sitzungen für MAB-/dot1x-Prozesse sichtbar sind, da manchmal eine hohe Anzahl authentifizierter Sitzungen zu einer hohen CPU führen kann. Geben Sie folgende Befehle ein, um die Anzahl der aktiven Sitzungen zu überprüfen:

```
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
```

Schritt 6: Um die Version und mögliche Fehler zu überprüfen, geben Sie den Befehl **show version ein**.

Wenn der Fehler nicht im Abschnitt "Bugs" aufgeführt ist, erstellen Sie ein Ticket beim Technical Assistance Center (TAC) und hängen alle Protokolle von den Schritten 1 bis 5 an.

Bug

CSCus46997 Speicherverlust und hohe CPU im IP-Host-Track- und Auth-Manager

CSCtz06177 Ein Catalyst 2960 kann wenig Arbeitsspeicher beanspruchen.

CSCty49762 EAP-Framework und AAA AttrL-Subversion verwenden alle Prozessspeicher.

Tipp: Weitere Informationen finden Sie unter Cisco Bug IDs CSCus46997, CSCtz06177 und CSCty49762.