Vermeiden Sie große Wireless RADIUS-Netzwerk-Engpässe

Inhalt

Einführung

Dieses Dokument bietet eine kurze Übersicht über die grundlegenden Konfigurationsrichtlinien für umfangreiche Wireless-Bereitstellungen, wie den AireOS Wireless LAN Controller (WLC) mit RADIUS mit der Cisco Identity Services Engine (ISE) oder dem Cisco Secure Access Control Server (ACS). Dieses Dokument enthält weitere technische Informationen.

Beobachtete Symptome

In Universitätsumgebungen kommt es in der Regel zu einem solchen Meltdown-Status (Authentication, Authorization, Accounting - AAA). In diesem Abschnitt werden die üblichen Symptome/Protokolle beschrieben, die in dieser Umgebung auftreten.

1. Überwachung der RADIUS-Leistung

Der Dotx-Client ist mit zahlreichen erneuten Authentifizierungsversuchen sehr verzögert.

Verwenden Sie den Befehl **show radius auth statistics** (GUI: **Monitor > Statistics > RADIUS Servers**), um nach Problemen zu suchen. Achten Sie insbesondere auf eine große Anzahl von Retries, Rejects und Timeouts. Hier ein Beispiel:

```
Server Index..................................... 2
Server Address................................... 192.168.88.1
Msg Round Trip Time.............................. 3 (msec)
First Requests................................... 1256
Retry Requests................................... 5688
Accept Responses................................. 22
Reject Responses................................. 1
```

```
Challenge Responses..... 96
Malformed Msgs..... 0
Bad Authenticator Msgs..... 0
Pending Requests..... 1
Timeout Requests..... 6824
Unknowntype Msgs..... 0
Other Drops..... 0
```

Suchen Sie nach:

- Hohe Wiederholung: Quote für erste Anforderung (darf nicht mehr als 10 % sein)
- Hohe Ablehnung: Akzeptanzrate
- Hoher Timeout: Quote für erste Anforderung (darf nicht mehr als 5 % sein)

Wenn Probleme auftreten, prüfen Sie, ob:

- Nicht konfigurierte Clients
- Probleme bei der Netzwerkerreichbarkeit zwischen dem WLC und dem RADIUS-Server
- Probleme zwischen dem RADIUS-Server und der Backend-Datenbank, wenn diese verwendet wird, z. B. mit Active Directory (AD)

2. Der WLC sieht, dass die RADIUS-Warteschlange voll in den Msglogs ist.

Der WLC empfängt diese Meldung über die RADIUS-Warteschlange:

```
Univ-WISM2-02: *aaa QueueReader: Dec 02 14:25:31.565: #AAA-3-3TXQUEUE_ADD_FAILED:
radius_db.c:889 Transmission queue full. Que name: Radius queue. Dropping
sessionpackets.
host = x.x.x.x.
```

3. AAA-Debuggen

Bei einem AAA-Debuggen wird folgende Meldung angezeigt:

```
*aaaQueueReader: Dec 02 21 09:19:52.198: xx:xx:xx:xx:xx:xx Returning AAA Error
'Out of Memory' (-2) for mobile xx:xx:xx:xx:xx:xx
```

Beim Debuggen von AAA wird das AAA Error **Timeout (-5)** für Mobilgeräte zurückgegeben. Der AAA-Server ist nicht erreichbar, gefolgt von der Client-Deautorisierung.

4. Der RADIUS-Server ist zu voll und reagiert nicht.

Dies ist die Trap System Time (Protokollsystemzeit):

```
0 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
1 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 available
2 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
3 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
4 Wed Aug 20 15:30:40 2014 RADIUS auth-server x.x.x.x:1812 unavailable
5 Wed Aug 20 15:30:40 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 22) for client 68:96:7b:0e:46:7f / user 'user1@univ1.edu'
6 Wed Aug 20 15:29:57 2014 User Larry_Dull_231730 logged Out. Client MAC:84:a6:c8:
87:13:9c, Client IP:198.21.137.22, AP MAC:c0:7b:bc:cf:af:40, AP Name:Dot1x-AP
```

```
7 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 183) for client 48:d7:05:7d:93:a5 / user ' user2@univ2.edu '
8 Wed Aug 20 15:28:42 2014 RADIUS auth-server x.x.x.x:1812 unavailable
9 Wed Aug 20 15:28:42 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 154) for client 40:0e:85:76:00:68 / user ' user1@univ1.edu '
10 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 available
11 Wed Aug 20 15:28:41 2014 RADIUS auth-server x.x.x.x:1812 unavailable
12 Wed Aug 20 15:28:41 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 99) for client 50:2e:5c:ea:e4:ba / user ' user3@univ3.edu '
13 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
14 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
15 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 failed to respond to request
(ID 30) for client b4:18:d1:60:6b:51 / user ' user1@univ1.edu '
16 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 available
17 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 activated on WLAN 6
18 Wed Aug 20 15:28:38 2014 RADIUS server x.x.x.x:1812 deactivated on WLAN 6
19 Wed Aug 20 15:28:38 2014 RADIUS auth-server x.x.x.x:1812 unavailable
```

Optimierung von Best Practices

WLC-seitiges Tuning

- Extensible Authentication Protocol (EAP) - Der Ausschluss des 802.1X-Clients funktioniert.

  Globale Aktivierung des Client-Ausschlusses für 802.1X
  Legen Sie für die 802.1X Wireless LANs (WLANs) den Client-Ausschluss auf mindestens 120 Sekunden fest.
  Legen Sie die EAP-Timer wie im Artikel 802.1X Client Exclusion auf einem AireOS WLC beschrieben fest.

- Legen Sie für die RADIUS-Neuübertragung Zeitüberschreitungen auf mindestens fünf Sekunden fest.

- Legen Sie ein Sitzungs-Timeout auf mindestens acht Stunden fest.

- Deaktivieren Sie Aggressive Failover, wodurch eine einzelne fehlerhafte Komponente nicht dazu führt, dass der WLC zwischen den RADIUS-Servern ausfällt.

- Konfigurieren Sie schnelles sicheres Roaming für Ihre Clients.

  Stellen Sie sicher, dass Microsoft Windows EAP-Clients Wi-Fi Protected Access 2 (WPA2)/Advanced Encryption Standard (AES) verwenden, damit sie Opportunistic Key Caching (OKC) verwenden können.

  Wenn Sie Apple iOS-Clients in ein eigenes WLAN separieren können, können Sie 802.11r in diesem WLAN aktivieren.

  Aktivieren Sie Cisco Centralized Key Management (CCKM) für alle WLANs, die 792x-

Telefone unterstützen (aktivieren Sie **jedoch** CCKM **nicht** auf einem Service Set Identifier (SSID), der Microsoft Windows- oder Android-Clients unterstützt, da diese in der Regel problematische CCKM-Implementierungen haben).

Aktivieren Sie Sticky Key Caching (SKC) für jedes EAP-WLAN, das Macintosh Operating System (MAC OS) X- und/oder Android-Clients unterstützt.

Weitere Informationen finden Sie unter 802.11 WLAN Roaming und Fast-Secure Roaming auf CUWN.

Hinweis: Überwachen Sie die Auslastung des WLC Pairwise Master Key (PMK)-Cache zu Spitzenzeiten mit dem Befehl **show pmk-cache all**. Wenn Sie Ihre maximale Größe für den PMK-Cache erreichen oder sich dieser nähern, müssen Sie wahrscheinlich die SKC deaktivieren.
Wenn Sie ISE mit Profilerstellung verwenden, verwenden Sie die WLC-seitige DHCP/HTTP-Profilerstellung. Dadurch werden die Profilierungsdaten in ein RADIUS-Accounting-Paket mit einfachem Lastausgleich eingebunden, wodurch sichergestellt wird, dass alle Daten für den Endpunkt dasselbe Public Services Network (PSN) erreichen.

Stellen Sie sicher, dass die Zwischenabrechnung deaktiviert ist, es sei denn, Sie benötigen sie für byte-basierte Abrechnungsdienste. Andernfalls erhöht die Zwischenabrechnung nur die Last ohne zusätzlichen Vorteil.

Führen Sie den besten WLC-Code aus.

RADIUS Server-seitiges Tuning Reduzieren Sie die Protokollierungsrate. Die meisten RADIUS-Server sind konfigurierbar, welche Protokollierung sie speichern. Wenn der ACS oder die ISE verwendet wird, kann ein Administrator auswählen, welche Kategorien in der Überwachungsdatenbank protokolliert werden. Ein Beispiel könnte sein, wenn Abrechnungsdaten vom RADIUS-Server gesendet und mit einer anderen Anwendung wie SYSLOG angezeigt werden. Schreiben Sie die Daten dann nicht lokal in die Datenbank. Stellen Sie bei der ISE sicher, dass die Protokollunterdrückung jederzeit aktiviert bleibt. Wenn sie zur Fehlerbehebung deaktiviert werden muss, gehen Sie zu **Administration > System > Logging > Collection Filters** und verwenden Sie die Option Bypass Suppression (Unterdrückung umgehen), um die Unterdrückung auf einem einzelnen Endpunkt oder Benutzer zu deaktivieren. In ISE Version 1.3 und höher kann ein Endpunkt mit der rechten Maustaste in das Live-Authentifizierungsprotokoll geklickt werden, um auch die Unterdrückung zu deaktivieren.

Stellen Sie sicher, dass die Latenz der Backend-Authentifizierung gering ist (AD, Lightweight Directory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Wenn Sie den ACS oder

die ISE verwenden, können die Berichte zur Authentifizierungszusammenfassung ausgeführt werden, um die Latenz pro Server auf Durchschnittl- und Spitzenlatenz zu überwachen. Je länger die Verarbeitung einer Anfrage dauert, desto niedriger ist die Authentifizierungsrate, die der ACS oder die ISE verarbeiten kann. 95 % der Zeit ist eine hohe Latenz auf eine langsame Antwort aus einer Backend-Datenbank zurückzuführen.

Deaktivieren Sie PEAP-Kennwortwiederholungen (Protected Extensible Authentication Protocol). Die meisten Geräte unterstützen keine Kennwortneuversuche im PEAP-Tunnel, sodass ein erneuter Versuch vom EAP-Server dazu führt, dass das Gerät nicht mehr reagiert und mit einer neuen EAP-Sitzung neu startet. Dies führt zu EAP-Timeouts anstelle von Ablehnungen, d. h., die Client-Ausschlüsse werden nicht getroffen.

Deaktivieren nicht verwendeter EAP-Protokolle Dies ist nicht wichtig, erhöht jedoch die Effizienz des EAP-Austauschs und stellt sicher, dass ein Client keine schwache oder unbeabsichtigte EAP-Methode verwenden kann.

Aktivieren Sie PEAP Session Resume und Fast Reconnect.

Senden Sie keine MAC-Authentifizierungen an das AD, wenn dies nicht erforderlich ist. Dies ist eine häufig vorkommende Fehlkonfiguration, die die Last der Domänen-Controller erhöht, für die die ISE sich authentifiziert. Diese führen häufig zu negativen Suchergebnissen, die zeitaufwendig sind und die durchschnittliche Latenz erhöhen.

Verwenden Sie ggf. den Gerätesensor (ISE-spezifisch).