Impedire il crollo di una rete RADIUS wireless su larga scala

Sommario

Introduzione

In questo documento viene fornita una breve panoramica delle linee guida di configurazione di base per installazioni wireless su larga scala, ad esempio AireOS Wireless LAN Controller (WLC) con RADIUS con Cisco Identity Services Engine (ISE) o Cisco Secure Access Control Server (ACS). Questo documento fa riferimento ad altri documenti con maggiori dettagli tecnici.

Sintomi osservati

In genere, negli ambienti universitari si verifica questo stato di fusione del sistema di autenticazione, autorizzazione e accounting (AAA). Questa sezione descrive i sintomi/log usuali osservati in questo ambiente.

1. Monitoraggio delle prestazioni RADIUS

Nel client Dotx si verifica un ritardo notevole con numerosi tentativi di autenticazione.

Utilizzare il comando **show radius auth statistics** (GUI: **Monitoraggio > Statistiche > Server RADIUS**) per individuare eventuali problemi. Cercare in modo specifico un numero elevato di tentativi, rifiuti e timeout. Di seguito è riportato un esempio:

```
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
```

Cerca:

- Tentativo alto: Rapporto prima richiesta (non deve essere superiore al 10%)
- Rifiuto massimo: Accetta rapporto
- Timeout elevato: Rapporto prima richiesta (non deve essere superiore al 5%)

In caso di problemi, verificare:

- Client non configurati correttamente
- Problemi di raggiungibilità della rete tra il WLC e il server RADIUS
- Problemi tra il server RADIUS e il database back-end, se in uso, ad esempio con Active Directory (AD)

2. Il WLC vede la coda RADIUS piena sui Msglogs

Il WLC riceve questo messaggio relativo alla coda RADIUS:

```
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. Debug del server AAA

Durante il debug del server AAA viene visualizzato questo messaggio:

```
*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
```

Il debug di AAA restituisce il **timeout di** errore AAA **(-5)** per i dispositivi mobili. Il server AAA non è raggiungibile ed è seguito dalla disautorizzazione del client.

4. Il server RADIUS è occupato e non risponde

Di seguito è riportato il log dell'ora del sistema:

```
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
```

Ottimizzazione delle procedure ottimali

Tuning lato WLC

- Extensible Authentication Protocol (EAP) - Consente di attivare l'esclusione dei client 802.1X.

  Abilitare l'esclusione dei client a livello globale per 802.1X.
  Impostare l'esclusione dei client sulle LAN wireless (WLAN) 802.1X su almeno 120 secondi.
  Impostare i timer EAP come descritto nell'articolo 802.1X Client Exclusion on an AireOS WLC.

- Impostare i timeout di ritrasmissione RADIUS su almeno cinque secondi.

- Impostare Session-Timeout su almeno otto ore.

- Disabilitare il failover aggressivo, che non consente a un singolo supplicant che si comporta in modo errato di causare il malfunzionamento del WLC tra i server RADIUS.

- Configurare Fast Secure Roaming per i client.

  Verificare che i client Microsoft Windows EAP utilizzino Wi-Fi Protected Access 2 (WPA2)/Advanced Encryption Standard (AES) in modo da poter utilizzare Opportunistic Key Caching (OKC).

  Se è possibile segregare i client iOS Apple alla propria WLAN, è possibile abilitare 802.11r su tale WLAN.

  Abilitare la gestione centralizzata delle chiavi (CCKM) Cisco per qualsiasi rete WLAN che supporti telefoni 792x, ma **non** abilitare la funzionalità CCKM su alcun SSID (Service Set Identifier) che supporti client Microsoft Windows o Android, in quanto tendono ad avere implementazioni CCKM problematiche.

Abilitare la memorizzazione nella cache di tasti permanenti (SKC) per qualsiasi WLAN EAP che supporta i client Macintosh Operating System (MAC OS) X e/o Android.

per ulteriori informazioni, fare riferimento a 802.11 WLAN Roaming e Fast-Secure Roaming on CUWN.

Nota: Monitorare l'utilizzo della cache PMK (Pairwise Master Key) WLC negli orari di picco con il comando **show pmk-cache all**. Se si raggiungono o si avvicinano le dimensioni massime della cache PMK, è probabile che sia necessario disattivare la funzionalità SKC.
Se si usa ISE con la profilatura, usare la profilatura DHCP/HTTP sul lato WLC. In questo modo i dati di profilatura vengono raccolti in un pacchetto di accounting RADIUS con bilanciamento del carico semplice, che assicura che tutti i dati per l'endpoint raggiungano lo stesso PSN (Public Services Network).

Assicurarsi che la contabilità provvisoria sia disattivata a meno che non sia necessaria per i servizi di fatturazione basati su byte. In caso contrario, la contabilità provvisoria aggiunge solo il carico senza ulteriori vantaggi.

Esegui il codice WLC migliore.

Ottimizzazione RADIUS lato server Ridurre la velocità di registrazione. La maggior parte dei server RADIUS è configurabile per la registrazione da archiviare. Se si utilizza l'ACS o l'ISE, l'amministratore può scegliere le categorie da registrare nel database di monitoraggio. È possibile, ad esempio, che i dati di accounting vengano inviati dal server RADIUS e visualizzati con un'altra applicazione, ad esempio SYSLOG, e quindi non vengano scritti nel database localmente. Sul sito ISE, verificare che la funzione di soppressione del log sia sempre abilitata. Se è necessario disabilitarlo per la risoluzione dei problemi, selezionare **Amministrazione > Sistema > Registrazione > Filtri di raccolta** e utilizzare l'opzione Ignora eliminazione per disabilitare l'eliminazione su un singolo endpoint o utente. In ISE versione 1.3 e successive, è possibile fare clic con il pulsante destro del mouse su un endpoint nel log di autenticazione live per disabilitare anche la soppressione.

Accertarsi che la latenza di autenticazione back-end sia bassa (AD, Lightweight Directory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Se si utilizza l'ACS o l'ISE, è possibile eseguire i report di riepilogo dell'autenticazione per monitorare la latenza per server per la latenza media e di picco. Più tempo richiede l'elaborazione di una richiesta, minore è la velocità di autenticazione che ACS o ISE possono elaborare. Il 95% delle volte, una latenza elevata è dovuta a una risposta lenta da un database back-end.

Disabilitare i nuovi tentativi per la password PEAP (Protected Extensible Authentication

Protocol). Poiché la maggior parte dei dispositivi non supporta i tentativi di password all'interno del tunnel PEAP, un nuovo tentativo dal server EAP provoca l'arresto del dispositivo e il riavvio con una nuova sessione EAP. Ciò causa timeout EAP anziché rifiuti, il che significa che le esclusioni dei client non verranno trovate.

Disabilitare i protocolli EAP inutilizzati. Questo non è fondamentale, ma aggiunge una certa efficienza allo scambio EAP e garantisce che un client non possa utilizzare un metodo EAP debole o non voluto.

Abilitare la ripresa della sessione PEAP e la riconnessione rapida.

Non inviare autenticazioni MAC ad Active Directory se non necessario. Questa è una configurazione errata comune che aumenta il carico sui controller di dominio su cui ISE esegue l'autenticazione. Ciò spesso comporta ricerche negative che richiedono molto tempo e aumentano la latenza media.

Usare il sensore dispositivo, dove applicabile (specifico per ISE).