Evite los fallos de fusión de red RADIUS inalámbrica a gran escala

Contenido

Introducción

Este documento proporciona una breve descripción general de las pautas de configuración básicas para implementaciones inalámbricas a gran escala, como AireOS Wireless LAN Controller (WLC) con RADIUS con Cisco Identity Services Engine (ISE) o Cisco Secure Access Control Server (ACS). Este documento hace referencia a otros documentos con mayor detalle técnico.

Síntomas observados

Normalmente, los entornos universitarios encuentran este estado de fusión de autenticación, autorización y contabilidad (AAA). Esta sección describe los síntomas/registros habituales observados en este entorno.

1. Supervisión del rendimiento RADIUS

El cliente Dotx experimenta un gran retraso con muchos reintentos de autenticación.

Utilice el comando **show radius auth statistics** (GUI: **Supervisar > Estadísticas > Servidores RADIUS**) para buscar problemas. Busque específicamente un gran número de intentos, rechazos y tiempos de espera. Aquí tiene un ejemplo:

```
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
```

Busque:

- Reintento alto: Relación de la primera solicitud (no debe ser superior al 10%)
- Rechazo alto: Ratio de aceptación
- Tiempo de espera alto: Relación de la primera solicitud (no debe ser superior al 5%)

Si hay problemas, compruebe:

- Clientes mal configurados
- Problemas de alcance de la red entre el WLC y el servidor RADIUS
- Problemas entre el servidor RADIUS y la base de datos backend, si se está utilizando, como con Active Directory (AD)

2. El WLC ve la cola RADIUS llena en los Msglogs

El WLC recibe este mensaje acerca de la cola 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 AAA

Un debug de AAA muestra este mensaje:

```
*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
```

Una depuración de AAA devuelve el **tiempo de espera de** error AAA **(-5)** para los dispositivos móviles. El servidor AAA es inalcanzable y es seguido por la desautorización del cliente.

4. El servidor RADIUS está demasiado ocupado y no responde

Esta es la trampa de hora del sistema de registro:

```
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
```

Ajuste de las prácticas recomendadas

Ajuste del Lado WLC

- Protocolo de autenticación extensible (EAP): permite que funcione la exclusión de clientes 802.1X.

  Habilitar la exclusión de clientes globalmente para 802.1X.
  Establezca la exclusión del cliente en las LAN inalámbricas (WLAN) 802.1X en al menos 120 segundos.
  Configure los temporizadores EAP como se describe en la Exclusión de Cliente 802.1X en un artículo AireOS WLC.

- Establezca los tiempos de espera de retransmisión RADIUS en al menos cinco segundos.

- Establezca Session-Timeout en al menos ocho horas.

- Inhabilite la conmutación por fallas agresiva, que no permite que un solo suplicante de mal comportamiento haga que el WLC falle entre los servidores RADIUS.

- Configure Fast Secure Roaming para sus clientes.

  Asegúrese de que los clientes EAP de Microsoft Windows utilizan Wi-Fi Protected Access 2 (WPA2)/Advanced Encryption Standard (AES) para poder utilizar el almacenamiento en caché de claves oportunistas (OKC).

  Si puede separar los clientes Apple iOS de su propia WLAN, puede activar 802.11r en esa WLAN.

  Habilite Cisco Centralized Key Management (CCKM) para cualquier WLAN que admita

teléfonos 792x (pero **no** habilite CCKM en ningún identificador de conjunto de servicios (SSID) que admita clientes de Microsoft Windows o Android, porque suelen tener implementaciones CCKM problemáticas).

Habilite el almacenamiento en caché de claves pegajosas (SKC) para cualquier WLAN EAP que admita el sistema operativo Macintosh (MAC OS) X y/o clientes Android.

Refiérase a Roaming WLAN 802.11 y Roaming Fast-Secure en CUWN para obtener más información.

Nota: Controle el uso de la memoria caché de la clave maestra de par (PMK) del WLC en las horas punta con el comando **show pmk-cache all**. Si alcanza su tamaño máximo de caché PMK o se acerca a él, probablemente tendrá que desactivar SKC.
Si utiliza ISE con la generación de perfiles, utilice el perfil DHCP/HTTP del lado del WLC. Esto ajusta los datos de perfiles en un paquete de contabilidad RADIUS que se equilibra fácilmente con la carga, lo que garantiza que todos los datos del terminal alcancen la misma red de servicios públicos (PSN).

Asegúrese de que la contabilidad provisional está desactivada a menos que la necesite para los servicios de facturación basados en bytes. De lo contrario, la contabilidad provisional sólo agrega carga sin beneficio adicional.

Ejecute el mejor código WLC.

Ajuste del lado del servidor RADIUS Reduzca la velocidad de registro. La mayoría de los servidores RADIUS son configurables sobre el registro que almacenarán. Si se utiliza el ACS o el ISE, un administrador puede elegir qué categorías se registran en la base de datos de supervisión. Un ejemplo podría ser si los datos de contabilización se envían fuera del servidor RADIUS y se visualizan con otra aplicación como SYSLOG, no escriba los datos en la base de datos localmente. En ISE, asegúrese de que la supresión de registros permanezca habilitada en todo momento. Si se debe inhabilitar para solucionar problemas, vaya a **Administration > System > Logging > Collection Filters** y utilice la opción Bypass Suppression para inhabilitar la supresión en un terminal o usuario individual. En ISE versión 1.3 y posteriores, se puede hacer clic con el botón derecho en un terminal en el registro de autenticación en vivo para inhabilitar la supresión también.

Asegúrese de que la latencia de autenticación del motor es baja (AD, protocolo ligero de acceso a directorios (LDAP), Rivest, Shamir, Adleman (RSA)). Si utiliza el ACS o el ISE, los informes de resumen de autenticación se pueden ejecutar para monitorear la latencia por servidor tanto para la latencia media como para la máxima. Cuanto más tarde en procesarse una solicitud, menor será la velocidad de autenticación que puede procesar el ACS o el ISE.

El 95% del tiempo, la latencia alta se debe a una respuesta lenta de una base de datos backend.

Desactive los reintentos de contraseña del protocolo de autenticación extensible protegido (PEAP). La mayoría de los dispositivos no admiten reintentos de contraseñas dentro del túnel PEAP, por lo que un reintento del servidor EAP hace que el dispositivo deje de responder y reinicie con una nueva sesión EAP. Esto provoca tiempos de espera de EAP en lugar de rechazos, lo que significa que no se alcanzarán las exclusiones del cliente.

Desactive Protocolos EAP no utilizados. Esto no es crítico, pero añade cierta eficiencia al intercambio EAP y asegura que un cliente no pueda utilizar un método EAP débil o no intencionado.

Habilite la reanudación de la sesión PEAP y la conexión rápida.

No envíe las autenticaciones MAC al AD si no es necesario. Se trata de un error de configuración común que aumenta la carga en los controladores de dominio con los que se autentica ISE. A menudo, esto lleva a búsquedas negativas que llevan mucho tiempo y aumentan la latencia media.

Utilice el sensor de dispositivos cuando corresponda (específico de ISE).