Prevenga los plumones en grande del derretimiento de la red de la Tecnología inalámbrica RADIUS

Contenido

Introducción

Este documento proporciona una breve descripción de las guías de consulta de la configuración básica para las implementaciones inalámbricas en grande tales como el regulador del Wireless LAN de AireOS (WLC) con el RADIUS con el Cisco Identity Services Engine (ISE) o el Cisco Secure Access Control Server (ACS). Este documento se refiere a otros documentos con el mayor detalle técnicos.

Síntomas observados

Los entornos de la universidad encuentran típicamente este estado de la fusión del Authentication, Authorization, and Accounting (AAA). Esta sección describe los síntomas frecuentes/los registros atestiguados en este entorno.

1. Funcionamiento del monitor RADIUS

El cliente de Dotx experimenta un retardo grande con muchas recomprobaciones para autenticar.

Utilice las **estadísticas del auth del** comando show radius (GUI: **Monitor > estadísticas > servidores de RADIUS**) para buscar los problemas. Busque específicamente un gran número de Retries, de rechazos, y de descansos. 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:

- Alta recomprobación: Primera relación de transformación de la petición (deben ser no más el que 10%)
- Alto rechazo: Valide la relación de transformación
- Alto descanso: Primera relación de transformación de la petición (deben ser no más el que 5%)

Si hay problemas, marque para:

- Clientes mal configurado
- Problemas del alcance de la red entre el WLC y el servidor de RADIUS
- Problemas entre el servidor de RADIUS y la base de datos backend, si es funcionando, por ejemplo con el Active Directory (AD)

2. El WLC ve la cola RADIUS por completo en el Msglogs

El WLC recibe este mensaje sobre 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 del 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
```

Un debug del AAA vuelve el **descanso del** error AAA **(-5)** para los dispositivos móviles. El servidor de AAA es inalcanzable y es seguido por la desautorización del cliente.

4. El servidor de RADIUS está demasiado ocupado y no responde

Aquí está el desvío del Tiempo del sistema del 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
```

El ajustar de la mejor práctica

El ajustar del WLC-lado

- Protocolo de Autenticación Extensible (EAP) - Haga el trabajo de la exclusión del cliente del 802.1x.

  Habilite la exclusión del cliente global para el 802.1x.
  Fije la exclusión del cliente en la Tecnología inalámbrica LAN (WLAN) del 802.1x por lo menos a 120 segundos.
  Fije los temporizadores EAP según lo descrito en la exclusión del cliente del 802.1x en un artículo del WLC de AireOS.

- Fije los descansos de la retransmisión RADIUS por lo menos a cinco segundos.

- Fije el Sesión-descanso por lo menos a ocho horas.

- Inhabilite la Conmutación por falla agresiva, que no permite que un solo supplicant que se comporta mal haga el WLC fallar entre los servidores de RADIUS.

- Configure rápidamente la itinerancia segura para sus clientes.

  Aseegurese que acceso protegido Wi-Fi 2 del uso de los clientes EAP de Microsoft Windows (la norma de encripción WPA2)/Advanced (AES) pueden utilizar tan el almacenamiento en memoria inmediata oportunista de la clave (OKC).

  Si usted puede segregar a los clientes IOS de Apple a su propia red inalámbrica (WLAN),

después usted puede habilitar 802.11r en esa red inalámbrica (WLAN).

Habilite la administración de claves centralizada Cisco (CCKM) para cualquier red inalámbrica (WLAN) que soporte los teléfonos 792x (pero no habilite el CCKM en ningún Service Set Identifier (SSID) que apoya a los clientes de Microsoft Windows o de Android, porque tienden a tener implementaciones problemáticas del CCKM).

Habilite la clave Sticky que oculta (SKC) para cualquier red inalámbrica (WLAN) EAP que soporte el sistema operativo de Macintosh (MAC OS) los clientes X y/o de Android.

Refiera a la red inalámbrica (WLAN) del 802.11 que vaga por y que vaga por Rápido-segura en CUWN para más información.

Note: Monitoree su uso del caché de la clave principal del WLC en parejas (PMK) en los horarios pico con el **comando all del PMK-caché de la demostración**. Si usted alcanza su tamaño máximo del PMK-caché, o consigue cerca de él, después usted tendrá que probablemente inhabilitar SKC.
Si usted utiliza el ISE con el perfilado, después utilice el perfilado del WLC-lado DHCP/HTTP. Esto envuelve los datos de perfilado en un paquete de las estadísticas RADIUS que sea fácilmente la carga balanceada, que se asegura de que todos los datos para el punto final alcancen la misma red de servicios públicos (PSN).

Aseegurese que las estadísticas interinas están apagadas a menos que usted las necesite para los servicios basados en byte de la factura. Si no el considerar interino agrega solamente la carga sin el beneficio adicional.

Funcione con el mejor código del WLC.

El ajustar del lado del servidor RADIUS Reduzca la tarifa del registro. La mayoría de los servidores de RADIUS son configurables sobre qué registro salvarán. Si se utiliza el ACS o el ISE, un administrador puede elegir qué categorías se registran a la base de datos de la supervisión. Un ejemplo pudo ser si los datos de contabilidad se envían del servidor de RADIUS y se ven con otra aplicación tal como SYSLOG, después no escribe los datos a la base de datos localmente. En el ISE, asegúrese de que la supresión del registro siga habilitada siempre. Si debe ser inhabilitada para los propósitos de Troubleshooting, después ir a la **administración > al sistema > al registro > a la colección filtra** y utiliza la opción de la supresión de puente para inhabilitar la supresión en un punto final o un usuario individual. En la versión 1.3 y posterior ISE, un punto final se puede hacer clic con el botón derecho del ratón en la orden viva de la conexión con el sistema de autenticación para inhabilitar la supresión también.

Asegúrese que el tiempo de espera backend de la autenticación sea bajo (AD, Lightweight Directory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Si usted utiliza el ACS o el ISE, los informes del resumen de la autenticación se pueden funcionar con para monitorear el tiempo de espera sobre una base del por-servidor para la media y el tiempo de espera del pico. Cuanto dura una petición de ser procesado, más baja es la tarifa de la autenticación el ACS o el ISE puede procesar. el 95% del tiempo, Latencia alta es debido a una respuesta lenta de una base de datos backend.

Retries protegido neutralización de la contraseña del protocolo extensible authentication (PEAP). La mayoría de los dispositivos no soportan las recomprobaciones de la contraseña dentro del túnel PEAP, así que una recomprobación del servidor EAP hace el dispositivo parar el responder y recomenzar con una nueva sesión EAP. Esto causa los descansos EAP en vez de los rechazos, así que significa que las exclusiones del cliente no serán golpeadas.

Protocolos inusitados de la neutralización EAP. Esto no es crítico sino agrega una cierta eficacia al intercambio EAP y se asegura de que un cliente no puede utilizar un método EAP débil o involuntario.

El curriculum vitae de la sesión del permiso PEAP y rápidamente vuelve a conectar.

No envíe las autenticaciones de MAC al AD si no necesario. Ésta es las configuraciones erróneas más comunes que aumentan la carga en los controladores de dominio contra los cuales el ISE autentica. Éstos llevan a las búsquedas negativas que son largas y aumentan a menudo latencia promedio.

Utilice el sensor del dispositivo en caso pertinente (específico ISE).