Evite quedas de rede RADIUS sem fio em larga escala

Contents

Introduction

Este documento fornece uma breve visão geral das diretrizes básicas de configuração para implantações sem fio em larga escala, como o AireOS Wireless LAN Controller (WLC) com RADIUS com o Cisco Identity Services Engine (ISE) ou o Cisco Secure Access Control Server (ACS). Este documento faz referência a outros documentos com maior detalhe técnico.

Sintomas observados

Normalmente, os ambientes universitários encontram esse estado de fusão de Autenticação, Autorização e Contabilidade (AAA). Esta seção descreve os sintomas/registros comuns observados neste ambiente.

1. Monitore o desempenho do RADIUS

O cliente Dotx experimenta um grande atraso com muitas novas tentativas de autenticação.

Use o comando **show radius auth statistics** (GUI: **Monitor > Statistics > RADIUS Servers**) para procurar problemas. Procure especificamente um grande número de repetições, rejeitos e timeouts. Aqui está um exemplo:

```
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
```

Procure:

- Alta repetição: Taxa de primeira solicitação (não deve ser superior a 10%)
- Rejeição Alta: Taxa de aceitação
- Tempo limite máximo: Taxa de primeira solicitação (não deve ser superior a 5%)

Se houver problemas, verifique:

- Clientes configurados incorretamente
- Problemas de acessibilidade de rede entre o WLC e o servidor RADIUS
- Problemas entre o servidor RADIUS e o banco de dados de back-end, se estiver em uso, como com o Ative Diretory (AD)

2. A WLC vê a fila RADIUS cheia nos Msglogs

A WLC recebe esta mensagem sobre a fila 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. Depurar AAA

Uma depuração de AAA mostra esta mensagem:

```
*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
```

Uma depuração de AAA retorna o AAA Error **Timeout (-5)** para dispositivos móveis. O servidor AAA está inacessível e é seguido por desautorização do cliente.

4. O servidor RADIUS está muito ocupado e não responde

Aqui está o Intervalo de tempo do sistema de log:

```
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 melhores práticas

Ajuste do lado da WLC

- Extensible Authentication Protocol (EAP) - Faça com que a exclusão do cliente 802.1X funcione.

  Ative a exclusão do cliente globalmente para 802.1X.
  Defina a exclusão do cliente nas LANs sem fio (WLANs) 802.1X como pelo menos 120 segundos.
  Defina os temporizadores EAP conforme descrito no artigo 802.1X Client Exclusion on an AireOS WLC.

- Defina os tempos limite de retransmissão RADIUS para pelo menos cinco segundos.

- Defina Session-Timeout como pelo menos oito horas.

- Desative o Failover Agressivo, que não permite que um único suplicante com mau comportamento faça com que a WLC falhe entre os servidores RADIUS.

- Configure o Fast Secure Roaming para seus clientes.

  Certifique-se de que os clientes EAP do Microsoft Windows usam o WPA2 (Wi-Fi Protected Access 2)/AES (Advanced Encryption Standard) para que possam usar o OKC (Opportunistic Key Caching).

  Se você puder segregar os clientes iOS da Apple em sua própria WLAN, você poderá habilitar o 802.11r nessa WLAN.

  Ative o Cisco Centralized Key Management (CCKM) para qualquer WLAN que suporte

telefones 792x (mas **não** habilite o CCKM em qualquer Service Set Identifier (SSID) que suporte clientes Microsoft Windows ou Android, pois eles tendem a ter implementações CCKM problemáticas).

Habilite a SKC (Sticky Key Caching) para qualquer WLAN EAP que suporte os clientes Macintosh Operating System (MAC OS) X e/ou Android.

Consulte Roaming de WLAN 802.11 e Roaming rápido e seguro no CUWN para obter mais informações.

Observação: monitore o uso do cache PMK (Pairwise Master Key) da WLC nos horários de pico com o comando **show pmk-cache all**. Se você atingir o tamanho máximo do cache PMK ou se aproximar dele, provavelmente terá que desabilitar o SKC.
Se você usar o ISE com criação de perfil, use o perfil DHCP/HTTP do lado da WLC. Isso envolve os dados de perfil em um pacote de contabilidade RADIUS que é facilmente balanceado de carga, o que garante que todos os dados do endpoint atinjam a mesma Rede de Serviços Públicos (PSN).

Certifique-se de que a contabilidade temporária esteja desativada, a menos que você precise dela para serviços de cobrança baseados em bytes. Caso contrário, a contabilidade intermediária só adiciona carga sem nenhum benefício adicional.

Execute o melhor código de WLC.

RADIUS Server-Side Tuning Reduza a taxa de registro. A maioria dos servidores RADIUS é configurável sobre qual registro eles armazenarão. Se o ACS ou o ISE for usado, um administrador pode escolher quais categorias estão registradas no banco de dados de monitoramento. Um exemplo pode ser se os dados de contabilização forem enviados do servidor RADIUS e exibidos com outro aplicativo como SYSLOG, então não grave os dados no banco de dados localmente. No ISE, certifique-se de que a supressão de log permaneça ativada o tempo todo. Se tiver de ser desativado para fins de resolução de problemas, vá para **Administração > Sistema > Registro > Filtros de Coleta** e utilize a opção Ignorar Supressão para desativar a supressão num ponto final ou utilizador individual. No ISE versão 1.3 e posterior, um endpoint pode ser clicado com o botão direito do mouse no registro de autenticação ao vivo para desabilitar a supressão também.

Verifique se a latência da autenticação de backend é baixa (AD, Lightweight Diretory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Se você usar o ACS ou o ISE, os relatórios de resumo de autenticação podem ser executados para monitorar a latência por servidor para latência média e máxima. Quanto mais tempo uma solicitação for processada, menor será a taxa de autenticação processada pelo ACS ou pelo ISE. 95% do tempo, alta

latência é devido a uma resposta lenta de um banco de dados back-end.

Desative as Tentativas de Senha do PEAP (Protected Extensible Authentication Protocol). A maioria dos dispositivos não suporta novas tentativas de senha dentro do túnel PEAP, portanto, uma nova tentativa do servidor EAP faz com que o dispositivo pare de responder e reinicie com uma nova sessão EAP. Isso causa tempos limite de EAP em vez de rejeitos, o que significa que as exclusões do cliente não serão atingidas.

Desative os protocolos EAP não utilizados. Isso não é crítico, mas adiciona alguma eficiência ao intercâmbio EAP e garante que um cliente não possa usar um método EAP fraco ou não intencional.

Habilite Retomar sessão PEAP e Reconectar rapidamente.

Não envie Autenticações MAC para o AD se não for necessário. Essa é uma configuração incorreta comum que aumenta a carga nos controladores de domínio com os quais o ISE se autentica. Geralmente, isso leva a pesquisas negativas que são demoradas e aumentam a latência média.

Use o sensor de dispositivo quando aplicável (específico do ISE).