Impeça penas wireless em grande escala do derretimento da rede do RAIO

Índice

Introdução

Este documento fornece uma breve visão geral de diretrizes da configuração básica para disposições wireless em grande escala tais como o controlador do Wireless LAN de AireOS (WLC) com o RAIO o Cisco Identity Services Engine (ISE) ou o Serviço de controle de acesso Cisco Secure (ACS). Este documento provê outros documentos com maior detalhe técnico.

Sintomas observados

Tipicamente os ambientes da universidade encontram este estado da fusão do Authentication, Authorization, and Accounting (AAA). Esta seção descreve os sintomas comuns/logs testemunhados neste ambiente.

1. Monitore o desempenho do RAIO

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

Use as **estatísticas do AUTH do** comando show radius (GUI: **Monitor > estatísticas > servidores Radius**) a fim procurar problemas. Procure especificamente um grande número Retries, rejeições, e intervalos. 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:

- Nova tentativa alta: Primeira relação do pedido (deve ser não mais de 10%)
- Rejeição alta: Aceite a relação
- Intervalo alto: Primeira relação do pedido (deve ser não mais de 5%)

Se há uns problemas, verifique:

- Clientes desconfigurados
- Problemas da alcançabilidade de rede entre o WLC e o servidor Radius
- Problemas entre o servidor Radius e o base de dados backend, se no uso, como com o diretório ativo (AD)

2. O WLC vê a fila do RAIO completamente no Msglogs

O WLC recebe esta mensagem sobre a fila do RAIO:

```
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. Debugar o AAA

Debugar do 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
```

Debugar do AAA retorna o **intervalo do** erro AAA **(-5)** para dispositivos móveis. O servidor AAA é inacessível e é seguido pelo deauthorization do cliente.

4. O servidor Radius é demasiado ocupado e não responde

Está aqui a armadilha do tempo de sistema do 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
```

Ajustamento do melhor prática

Ajustamento do WLC-lado

- Extensible Authentication Protocol (EAP) - Faça o trabalho da exclusão do cliente do 802.1X.

  Permita a exclusão do cliente globalmente para o 802.1X.
  Ajuste a exclusão do cliente no Sem fio LAN do 802.1X (WLAN) pelo menos a 120 segundos.
  Ajuste temporizadores EAP como descrito na exclusão do cliente do 802.1X em um artigo de AireOS WLC.

- Ajuste intervalos da retransmissão do RAIO pelo menos a cinco segundos.

- Ajuste o Sessão-intervalo pelo menos a oito horas.

- Desabilite o Failover agressivo, que não permite um único suplicante se portando mal faça com que o WLC falhe entre os servidores Radius.

- Configurar rapidamente vaguear seguro para seus clientes.

  Certifique-se de que acesso protegido por wi-fi 2 do uso dos clientes EAP de Microsoft Windows (o padrão de codificação WPA2)/Advanced (AES) assim podem usar pôr em esconderijo oportunista da chave (OKC).

  Se você pode segregar clientes iOS de Apple a seu próprio WLAN, a seguir você pode permitir 802.11r nesse WLAN.

  Permita o gerenciamento chave centralizado Cisco (CCKM) para todo o WLAN que apoiar os telefones 792x (mas não permita o CCKM em nenhum Service Set Identifier (SSID) que apoia clientes de Microsoft Windows ou de Android, porque tendem a ter aplicações problemáticas

CCKM).

Permita a chave pegajosa que põe em esconderijo (SKC) para todo o EAP WLAN que apoiar o sistema operacional de Macintosh (MAC OS) clientes X e/ou de Android.

Refira o 802.11 WLAN que vagueia e que vagueia Rápido-seguro em CUWN para mais informação.

Note: Monitore seu uso do esconderijo do chave mestre WLC por pares (PMK) no tempo de pico com o **comando all do PMK-esconderijo da mostra**. Se você alcança seu tamanho máximo do PMK-esconderijo, ou se aproxima ele, a seguir você terá que provavelmente desabilitar SKC.
Se você usa o ISE com perfilamento, a seguir use o perfilamento do WLC-lado DHCP/HTTP. Isto envolve os dados de perfilamento em um pacote da contabilidade do RAIO que seja facilmente a função de balanceamento de carga, que se assegura de que todos os dados para o valor-limite alcancem a mesma rede de serviços públicos (PSN).

Certifique-se de que a contabilidade provisória está a menos que você a precisar para serviços de fatura byte-baseados. Se não explicar provisório adiciona somente a carga sem o benefício adicional.

Execute o melhor código WLC.

Ajustamento do lado de servidor do RAIO Reduza a taxa de registro. A maioria de servidores Radius são configuráveis sobre o que que registra armazenarão. Se o ACS ou o ISE são usados, um administrador pode escolher que categorias são registradas ao base de dados da monitoração. Um exemplo pôde ser se os dados de contabilidade são enviados fora do servidor Radius e vistos com um outro aplicativo tal como o SYSLOG, a seguir não redige os dados ao base de dados localmente. No ISE, assegure-se de que as sobras da supressão do log permitidas em todas as vezes. Se deve ser desabilitada para propósitos de Troubleshooting, a seguir para ir à **administração > ao sistema > registrando > a coleção filtra** e usa a opção da supressão do desvio a fim desabilitar a supressão em um valor-limite ou em um usuário individual. Na versão 1.3 e mais recente ISE, um valor-limite pode ser clicado com o botão direito na ordem viva da autentificação de login para desabilitar também a supressão.

Assegure-se de que a latência backend da autenticação esteja baixa (AD, Lightweight Directory Access Protocol (LDAP), Rivest, Shamir, Adleman (RSA)). Se você usa o ACS ou o ISE, os relatórios sumário da autenticação podem ser executados a fim monitorar a latência em uma base do por-server para a média e a latência do pico. Mais por muito tempo toma um pedido ser processado, mais baixa a taxa da autenticação o ACS ou o ISE pode processar. 95% do tempo, alta latência é devido a uma resposta lenta de um base de dados backend.

O desabilitação protegeu o Retries da senha do protocolo extensible authentication (PEAP). A maioria de dispositivos não apoiam novas tentativas da senha dentro do túnel PEAP, assim que uma nova tentativa do server EAP faz com que o dispositivo pare de responder e reinicie com uma sessão nova EAP. Isto causa intervalos EAP em vez das rejeições, assim que significa que as exclusões do cliente não estarão batidas.

Protocolos não utilizados do desabilitação EAP. Isto não é crítico mas adiciona alguma eficiência à troca EAP e assegura-se de que um cliente não possa usar um método de EAP fraco ou sem intenção.

Permita o resumo da sessão PEAP e reconecte-o rapidamente.

Não envie autenticações de MAC ao AD se não necessário. Esta é uma falta de configuração comum que aumente a carga nos controladores de domínio que o ISE autentica contra. Estes frequentemente conduzem às buscas negativas que são demoradas e aumentam a latência média.

Use o sensor do dispositivo onde aplicável (específico ISE).