Use o script EEM para solucionar problemas de falhas intermitentes do servidor RADIUS

Contents

Introduction

Este documento descreve como solucionar problemas de um servidor RADIUS marcado como com falha no ASA e como isso pode causar interrupções para a infraestrutura do cliente.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Reconhecimento básico ou script EEM no Cisco ASA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problema

Os servidores RADIUS são marcados como falha/inoperante no Cisco ASA. O problema é intermitente, mas causa interrupções na infraestrutura do cliente. O TAC deve diferenciar se esse é um problema do ASA, do caminho de dados ou do servidor Radius. Se uma captura é feita no momento da falha, ele descarta o Cisco ASA ao discernir se o ASA envia os pacotes para o servidor RADIUS e se eles são recebidos em troca.

Topologia

Para este exemplo, esta é a topologia que é usada:

Para corrigir esse problema, siga estas próximas etapas.

Etapa 1: Configurar a captura de pacotes e as listas de acesso aplicáveis para capturar pacotes entre servidores

A primeira etapa é configurar a Captura de pacotes e as listas de acesso aplicáveis para capturar pacotes entre os servidores ASA e RADIUS.

Se precisar de ajuda com a Captura de pacotes, consulte o Gerador e analisador de configuração de captura de pacotes.

access-list licença estendida TAC ip host 10.20.20.180 host 10.10.10.150

access-list licença estendida TAC ip host 10.10.10.150 host 10.20.20.180

access-list licença estendida TAC ip host 10.20.20.180 host 10.10.20.150

access-list licença estendida TAC ip host 10.10.20.150host 10.20.20.180

capturar buffer TAC de lista de acesso de dados brutos do tipo RADIUS 30000000 interface dentro de buffer circular

> **Observação**: você precisa verificar o tamanho do buffer para garantir que ele não sobrecarregue e faça os dados. Um tamanho de buffer de 1000000 é suficiente. Observe

que nosso buffer de exemplo é 3000000.

Etapa 2: Configurar o script EEM

Em seguida, configure o script EEM.

Este exemplo usa o ID de Syslog de 113022 e você pode acionar o EEM em muitas outras mensagens de Syslog:

Os tipos de mensagem para o ASA são encontrados em Cisco Secure Firewall ASA Series Syslog Messages.

O disparador nesse cenário é:

Error Message %ASA-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED

O ASA tentou uma solicitação de autenticação, autorização ou contabilização para o servidor AAA e não recebeu uma resposta dentro da janela de tempo limite configurada. Em seguida, o servidor AAA é marcado como com falha e removido do serviço.

applet do gerenciador de eventos ISE_Radius_Check

event syslog id **113022**

ação 0 comando cli "show clock"

ação 1 comando cli "show aaa-server ISE"

ação 2 comando cli "aaa-server ISE ative host 10.10.10.150"

ação 3 comando cli "aaa-server ISE ative host 10.10.20.150"

ação 4 comando cli "show aaa-server ISE"

ação 5 comando cli "show capture radius decode dump"

arquivo de saída append disk0:/ISE_Recover_With_Cap.txt

Explicação do script EEM

applet do gerenciador de eventos ISE_Radius_Check. —*Você nomeia seu script eem.*

evento syslog id **113022** —Seu acionador: (consulte a explicação anterior)

action 0 cli command "show clock" — *práticas recomendadas para capturar carimbos de data/hora precisos enquanto soluciona problemas, a fim de comparar com outros registros que o cliente pode ter.*

action 1 cli command "show aaa-server ISE" — *Mostra o status do nosso grupo de servidores aaa. Nesse caso, esse grupo é chamado de ISE.*

ação 2 comando cli "aaa-server ISE ative host 10.10.10.150" — *Este comando é para "ativar*

novamente" o aaa-server com aquele IP. Isso permite que você continue tentando pacotes radius para determinar erros de caminho de dados.

ação 3 comando cli "aaa-server ISE ative host 10.10.20.150" —*Consulte a explicação do comando anterior.*

ação 4 comando cli "show aaa-server ISE". --*Este comando verifica se os servidores voltaram a funcionar.*

action 5 cli command "show capture radius decode dump" — *agora você decodifica/despeja sua captura de pacotes.*

arquivo de saída append disk0:/ISE_Recover_With_Cap.txt — *essa captura agora é salva em um arquivo de texto no ASA e novos resultados são anexados ao final.*

Passos finais

Finalmente, você pode carregar essas informações em um caso do Cisco TAC ou usar as informações para analisar os pacotes mais recentes no fluxo e descobrir por que os servidores RADIUS são marcados como com falha.

O arquivo de texto pode ser decodificado e transformado em um pcap no Packet Capture Config Generator and Analyzer mencionado anteriormente.

Exemplo do mundo real

No próximo exemplo, a captura do tráfego RADIUS é filtrada. Você verá que o ASA é o dispositivo que termina em .180 e o servidor RADIUS termina em .21

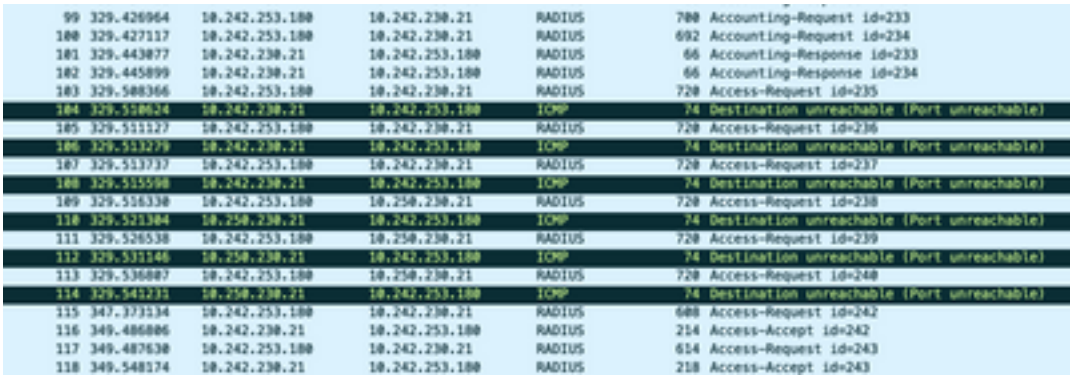
Neste exemplo, *ambos os* servidores RADIUS retornam uma "porta inalcançável", 3 vezes seguidas para cada um. Isso aciona o ASA para marcar *ambos os* servidores RADIUS como inativos dentro de milissegundos um do outro.

O resultado

Cada endereço .21 neste exemplo era um endereço VIP F5. Isso significa que, por trás dos VIPS, havia clusters de nós do Cisco ISE na persona da PSN.

O F5 retornou "porta inalcançável" devido a um defeito F5.

Neste exemplo, a equipe do Cisco TAC provou com sucesso que o ASA funcionou como esperado. Ou seja, ele enviou pacotes radius e recebeu 3 portas que antes não estavam acessíveis e afetou o servidor Radius marcado como failed:



99	329.426964	10.242.253.180	10.242.230.21	RADIUS	700	Accounting-Request id=233
100	329.427117	10.242.253.180	10.242.230.21	RADIUS	692	Accounting-Request id=234
101	329.443877	10.242.230.21	10.242.253.180	RADIUS	66	Accounting-Response id=233
102	329.445899	10.242.230.21	10.242.253.180	RADIUS	66	Accounting-Response id=234
103	329.508366	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=235
104	329.510624	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
105	329.511127	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=236
106	329.513279	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
107	329.513737	10.242.253.180	10.242.230.21	RADIUS	720	Access-Request id=237
108	329.515598	10.242.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
109	329.516330	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=238
110	329.521384	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
111	329.526538	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=239
112	329.531146	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
113	329.536807	10.242.253.180	10.250.230.21	RADIUS	720	Access-Request id=240
114	329.541231	10.250.230.21	10.242.253.180	ICMP	74	Destination unreachable (Port unreachable)
115	347.373134	10.242.253.180	10.242.230.21	RADIUS	608	Access-Request id=242
116	349.486086	10.242.230.21	10.242.253.180	RADIUS	214	Access-Accept id=242
117	349.487630	10.242.253.180	10.242.230.21	RADIUS	614	Access-Request id=243
118	349.548174	10.242.230.21	10.242.253.180	RADIUS	218	Access-Accept id=243

Informações Relacionadas

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.