Utilice la secuencia de comandos EEM para solucionar fallos intermitentes del servidor RADIUS

Contenido

Introducción

Este documento describe cómo resolver problemas de un servidor RADIUS marcado como fallado en ASA y cómo esto puede causar interrupciones para la infraestructura del cliente.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Reconocimiento básico o scripting de EEM en Cisco ASA

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

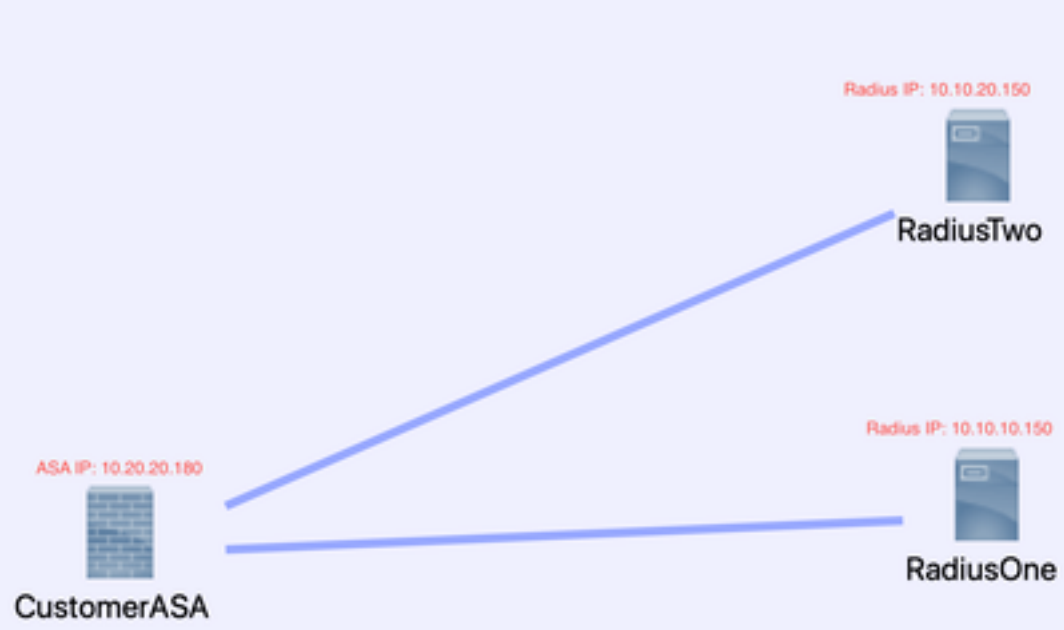
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Los servidores RADIUS están marcados como fallados/muertos en Cisco ASA. El problema es intermitente, pero provoca interrupciones en la infraestructura del cliente. El TAC debe diferenciar si se trata de un problema de ASA, un problema de ruta de datos o un problema del servidor Radius. Si se realiza una captura en el momento del fallo, se descarta el Cisco ASA a la hora de discernir si el ASA envía los paquetes al servidor RADIUS y si se reciben a cambio.

Topología

Para este ejemplo, esta es la topología que se utiliza:



Para solucionar este problema, siga estos pasos.

Paso 1: Configurar la captura de paquetes y las listas de acceso aplicables para capturar paquetes entre servidores

El primer paso es configurar la captura de paquetes y las listas de acceso aplicables para capturar paquetes entre los servidores ASA y RADIUS.

Si necesita ayuda con la captura de paquetes, consulte Generador y analizador de configuración de captura de paquetes.

access-list TAC extended permit ip host 10.20.20.180 host 10.10.10.150

access-list TAC extended permit ip host 10.10.10.150 host 10.20.20.180

access-list TAC extended permit ip host 10.20.20.180 host 10.10.20.150

access-list TAC extended permit ip host 10.10.20.150host 10.20.20.180

capture RADIUS type raw-data access-list TAC buffer 30000000 interface inside circular-buffer

Nota: Debe comprobar el tamaño del búfer para asegurarse de que no se rellena en exceso y de que no contiene los datos. Un tamaño de búfer de 1000000 es suficiente. Observe que nuestro búfer de ejemplo es 3000000.

Paso 2: Configurar script EEM

A continuación, configure el script EEM.

Este ejemplo utiliza el ID de Syslog 113022 y puede activar EEM en muchos otros mensajes de Syslog:

Los tipos de mensajes para ASA se encuentran en Mensajes de Syslog de la serie ASA de Cisco Secure Firewall.

El desencadenador en esta situación es:

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

ASA ha intentado una solicitud de autenticación, autorización o contabilización al servidor AAA y no ha recibido una respuesta dentro de la ventana de tiempo de espera configurada. El servidor AAA se marca como fallado y se elimina del servicio.

applet del administrador de eventos ISE_Radius_Check

event syslog id **113022**

action 0 cli command "show clock"

action 1 cli command "show aaa-server ISE"

action 2 cli command "aaa-server ISE active host 10.10.10.150"

action 3 cli command "aaa-server ISE active host 10.10.20.150"

action 4 cli command "show aaa-server ISE"

action 5 cli command "show capture radius decode dump"

archivo de resultados append disk0:/ISE_Recover_With_Cap.txt

Explicación de script EEM

applet del administrador de eventos ISE_Radius_Check. *: se le asigna un nombre a la secuencia de comandos eem.*

event syslog id **13022** —Su desencadenador: (ver explicación anterior)

comando de cli de acción 0 "show clock" *: prácticas recomendadas para capturar marcas de tiempo precisas mientras se solucionan problemas con el fin de comparar con otros registros que el cliente puede tener.*

action 1 cli command "show aaa-server ISE" - *Muestra el estado de nuestro grupo aaa-server. En*

este caso, ese grupo se denomina ISE.

action 2 cli command "aaa-server ISE active host 10.10.10.150" - *Este comando es para "hacer una copia de seguridad" del aaa-server con esa IP. Esto le permite continuar intentando paquetes RADIUS para determinar errores de ruta de datos.*

action 3 cli command "aaa-server ISE active host 10.10.20.150" —*Consulte la explicación del comando anterior.*

action 4 cli command "show aaa-server ISE". --*Este comando verifica si los servidores volvieron a estar activos.*

action 5 cli command "show capture radius decode dump" *: ahora decodifica/vuelca su captura de paquetes.*

archivo de salida append disk0:/ISE_Recover_With_Cap.txt*: esta captura se guarda ahora en un archivo de texto en el ASA y los nuevos resultados se agregan al final.*

Últimos pasos

Por último, puede cargar esta información en un caso del TAC de Cisco o utilizar la información para analizar los últimos paquetes en el flujo y averiguar por qué los servidores RADIUS están marcados como fallidos.

El archivo de texto se puede descodificar y convertir en un pcap en el Generador y Analizador de configuración de captura de paquetes mencionado anteriormente.

Ejemplo real

En el siguiente ejemplo, se filtra la captura para el tráfico RADIUS. Verá que el ASA es el dispositivo que termina en .180 y el servidor RADIUS termina en .21

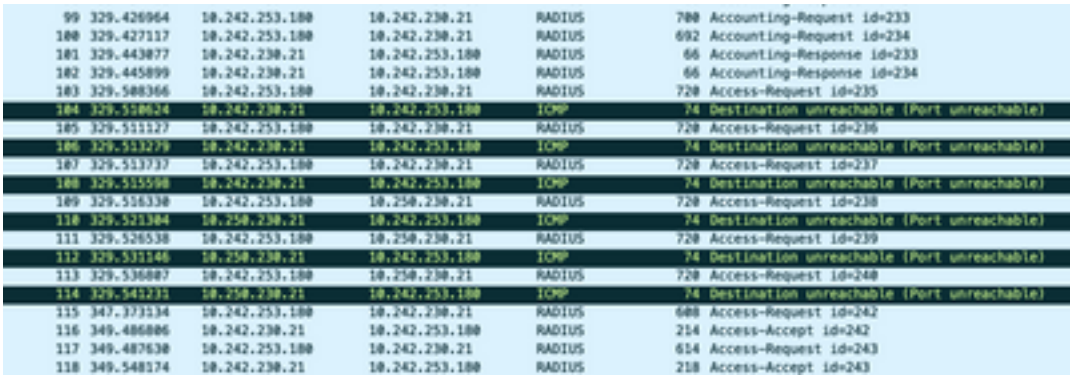
En este ejemplo, *ambos* servidores RADIUS devuelven un "puerto inalcanzable", 3 veces seguidas para cada uno. Esto hace que ASA marque *ambos* servidores RADIUS como muertos en milisegundos entre sí.

El resultado

Cada dirección .21 de este ejemplo era una dirección F5 VIP. Esto significa que detrás de los VIP había clústeres de nodos Cisco ISE en el personaje de PSN.

El F5 devolvió un "puerto inalcanzable" debido a un defecto F5.

En este ejemplo, el equipo del TAC de Cisco demostró con éxito que el ASA funcionaba como se esperaba. Es decir, envió paquetes RADIUS y recibió 3 puertos que eran inalcanzables antes, y efectuó el servidor Radius marcado como fallado:



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

Información Relacionada

- Asistencia técnica y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).