Utiliser le script EEM pour résoudre les pannes de serveur RADIUS intermittentes

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Problème
Topologie
Étape 1 : configurez la capture de paquets et les listes d'accès applicables pour capturer les paquets entre les serveurs
Étape 2 : configurez le script EEM
Explication du script EEM
Étapes finales
Exemple réel
Informations connexes

Introduction

Ce document décrit comment dépanner un serveur RADIUS marqué comme défaillant dans ASA et comment cela peut provoquer des pannes pour l'infrastructure client.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base des scripts EEM sur Cisco ASA

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Les serveurs RADIUS sont marqués comme défaillants/morts dans Cisco ASA. Le problème est intermittent, mais il entraîne des pannes pour l'infrastructure client. Le TAC doit déterminer s'il s'agit d'un problème ASA, d'un problème de chemin de données ou d'un problème de serveur Radius. Si une capture est effectuée au moment de la défaillance, elle exclut le Cisco ASA lorsqu'il détermine si le périphérique ASA envoie les paquets au serveur RADIUS et s'ils sont reçus en retour.

Topologie

Pour cet exemple, il s'agit de la topologie utilisée :

Pour résoudre ce problème, procédez comme suit.

Étape 1 : configurez la capture de paquets et les listes d'accès applicables pour capturer les paquets entre les serveurs

La première étape consiste à configurer la capture de paquets et les listes d'accès applicables pour capturer les paquets entre les serveurs ASA et RADIUS.

Si vous avez besoin d'aide avec Packet Capture, référez-vous à Packet Capture Config Generator and Analyzer.

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 circulaire-buffer

> **Remarque** : vous devez vérifier la taille de la mémoire tampon pour vous assurer qu'elle n'est pas saturée et qu'elle n'utilise pas les données. Une taille de tampon de 1000000 est

suffisante. Notez que notre exemple de tampon est 3000000.

Étape 2 : configurez le script EEM

Configurez ensuite le script EEM.

Cet exemple utilise l'ID Syslog 113022 et vous pouvez déclencher EEM sur de nombreux autres messages Syslog :

Les types de message pour ASA se trouvent dans les messages Syslog de la gamme Cisco Secure Firewall ASA.

Le déclencheur de ce scénario est :

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

Les ASA a tenté une demande d'authentification, d'autorisation ou de gestion des comptes au serveur AAA et n'a pas reçu de réponse dans le délai d'attente configuré. Le serveur AAA est alors marqué comme défaillant et supprimé du service.

applet du gestionnaire d'événements ISE_Radius_Check

event id syslog **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"

fichier de sortie append disk0:/ISE_Recover_With_Cap.txt

Explication du script EEM

applet du gestionnaire d'événements ISE_Radius_Check. *: vous nommez votre script eem.*

event syslog id **113022** —*Votre déclencheur : (voir l'explication précédente)*

action 0 cli command "show clock" - *meilleures pratiques pour capturer des horodatages précis pendant le dépannage afin de comparer avec d'autres journaux que le client peut avoir.*

action 1 cli command "show aaa-server ISE" - *Affiche l'état de votre groupe aaa-server. Dans ce cas, ce groupe est appelé ISE.*

action 2 cli command "aaa-server ISE active host 10.10.10.150" - *Cette commande permet de "ramener" le serveur aaa-server avec cette adresse IP. Cela vous permet de continuer à essayer*

les paquets radius pour déterminer les erreurs de chemin de données.

action 3 cli command "aaa-server ISE active host 10.10.20.150" —*Voir l'explication de la commande précédente.*

action 4 cli command "show aaa-server ISE". --*Cette commande vérifie si les serveurs sont de nouveau opérationnels.*

action 5 cli command "show capture radius decode dump" - *vous décodez/videz maintenant votre capture de paquets.*

output file append disk0:/ISE_Recover_With_Cap.txt *: cette capture est maintenant enregistrée dans un fichier texte sur l'ASA et les nouveaux résultats sont ajoutés à la fin.*

Étapes finales

Enfin, vous pouvez télécharger ces informations dans un dossier Cisco TAC ou les utiliser pour analyser les derniers paquets dans le flux et comprendre pourquoi les serveurs RADIUS sont marqués comme défaillants.

Le fichier texte peut être décodé et transformé en pcap au niveau du générateur et analyseur de configuration de capture de paquets mentionné précédemment.

Exemple réel

Dans l'exemple suivant, la capture du trafic RADIUS est filtrée. Vous voyez que l'ASA est le périphérique qui se termine par .180 et le serveur RADIUS par .21

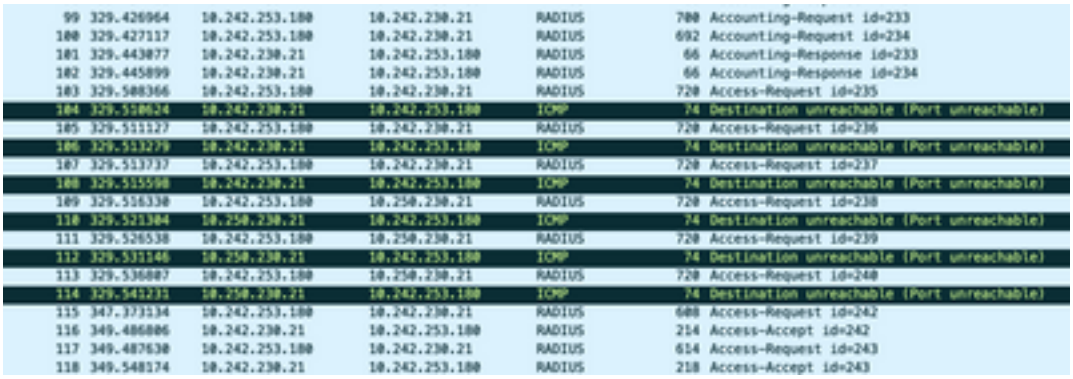
Dans cet exemple, *les deux* serveurs RADIUS renvoient un « port inaccessible », 3 fois de suite pour chacun. Cela déclenche l'ASA pour marquer *les deux* serveurs RADIUS comme étant morts dans les millisecondes de l'autre.

Le résultat

Chaque adresse .21 dans cet exemple était une adresse VIP F5. Cela signifie que derrière le VIPS se trouvaient des clusters de noeuds Cisco ISE dans le personnage PSN.

Le F5 a renvoyé « port inaccessible » en raison d'un défaut F5.

Dans cet exemple, l'équipe Cisco TAC a réussi à prouver que l'ASA fonctionnait comme prévu. Autrement dit, il a envoyé des paquets radius et a reçu 3 ports qui étaient inaccessibles avant, et a effectué le serveur Radius marqué en échec :



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

Informations connexes

- Assistance technique et téléchargements Cisco

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.