Utilizzare lo script EEM per risolvere i problemi relativi agli errori del server RADIUS intermittenti

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a un server RADIUS contrassegnato come non riuscito nell'appliance ASA e come ciò possa causare interruzioni delle attività per l'infrastruttura client.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di base degli script EEM su Cisco ASA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

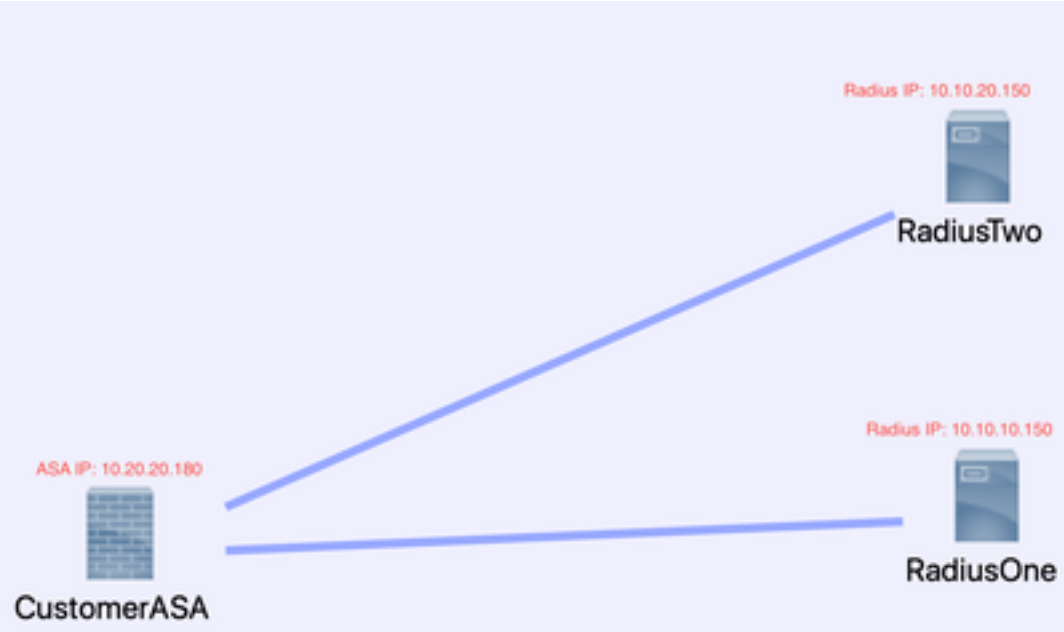
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

I server RADIUS sono contrassegnati come guasti/inattivi nell'appliance Cisco ASA. Il problema è intermittente ma causa interruzioni delle attività dell'infrastruttura client. TAC deve differenziare se si tratta di un problema di ASA, di percorso dei dati o di server Radius. Se l'acquisizione viene effettuata al momento del guasto, l'appliance Cisco ASA viene esclusa in quanto rileva se i pacchetti sono stati inviati al server RADIUS dall'appliance ASA e se sono stati ricevuti in cambio.

Topologia

Per questo esempio viene utilizzata la topologia seguente:



Per risolvere il problema, eseguire la procedura seguente.

Passaggio 1: Configurare l'acquisizione dei pacchetti e gli elenchi degli accessi applicabili per acquisire i pacchetti tra i server

Il primo passaggio consiste nella configurazione di Packet Capture e degli elenchi degli accessi applicabili per l'acquisizione dei pacchetti tra i server ASA e RADIUS.

Per assistenza sull'acquisizione dei pacchetti, consultare il Generatore e analizzatore di configurazioni di acquisizione pacchetti.

access-list TAC extended allow ip host 10.20.20.180 host 10.10.150

access-list TAC extended allow ip host 10.10.10.150 host 10.20.20.180

access-list TAC extended allow ip host 10.20.20.180 host 10.10.20.150

access-list TAC extended allow ip host 10.10.20.150host 10.20.20.180

acquisire il tipo RADIUS raw-data access-list TAC buffer 3000000 interfaccia all'interno del buffer circolare

Nota: è necessario controllare le dimensioni del buffer per assicurarsi che non sovraccarichi e che esegua i dati. È sufficiente una dimensione del buffer di 1000000. Il nostro buffer di esempio è 3000000.

Passaggio 2: Configurare lo script EEM

Configurare quindi lo script EEM.

In questo esempio viene utilizzato l'ID syslog 113022 ed è possibile attivare EEM su molti altri messaggi syslog:

I tipi di messaggi per l'ASA sono disponibili nei messaggi di syslog della serie ASA di Cisco Secure Firewall.

Il trigger in questo scenario è:

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

OSPF (Open Shortest Path First) ASA ha tentato di inviare una richiesta di autenticazione, autorizzazione o accounting al server AAA e non ha ricevuto risposta entro la finestra di timeout configurata. Il server AAA viene quindi contrassegnato come non riuscito e rimosso dal servizio.

applet di gestione eventi ISE_Radius_Check

evento syslog id **113022**

azione 0 comando cli "show clock"

azione 1 comando cli "show aaa-server ISE"

azione 2 comando cli "aaa-server ISE active host 10.10.10.150"

azione 3 comando cli "aaa-server ISE active host 10.10.20.150"

azione 4 comando cli "show aaa-server ISE"

azione 5 comando cli "show capture radius decode dump"

file di output append disco0:/ISE_Recover_With_Cap.txt

Spiegazione script EEM

applet di gestione eventi ISE_Radius_Check. - *Assegnate un nome allo script EEM.*

event syslog id **113022** - Il trigger: (vedere la spiegazione precedente)

azione 0 comando cli "show clock" *—best practice per acquisire timestamp accurati durante la risoluzione dei problemi it in modo da confrontarli con altri log che il client può avere.*

action 1 cli command "show aaa-server ISE" - *Mostra lo stato del nostro gruppo di server aaa. In questo caso, il nome del gruppo è ISE.*

azione 2 comando cli "aaa-server ISE active host 10.10.10.150" - *Questo comando ha lo scopo di "ripristinare" il server aaa con l'IP specificato. In questo modo è possibile continuare a tentare i pacchetti radius per determinare gli errori dei percorsi dei dati.*

azione 3 comando cli "aaa-server ISE active host 10.10.20.150" - *Vedere la spiegazione del comando precedente.*

azione 4 comando cli "show aaa-server ISE". --*Questo comando verifica se i server sono tornati attivi.*

azione 5 comando cli "show capture radius decode dump" - *è ora possibile decodificare/eseguire il dump dell'acquisizione del pacchetto.*

output file append disk0:/ISE_Recover_With_Cap.txt*: l'acquisizione viene salvata in un file di testo sull'appliance ASA e i nuovi risultati vengono aggiunti alla fine.*

Operazioni finali

Infine, è possibile caricare le informazioni in una richiesta Cisco TAC o utilizzarle per analizzare i pacchetti più recenti nel flusso e capire perché i server RADIUS sono contrassegnati come non riusciti.

Il file di testo può essere decodificato e trasformato in un cappuccio in corrispondenza del generatore e dell'analizzatore di configurazioni di acquisizione pacchetti precedentemente menzionati.

Esempio di mondo reale

Nell'esempio successivo, l'acquisizione del traffico RADIUS viene filtrata. L'appliance ASA termina con .180 e il server RADIUS con .21

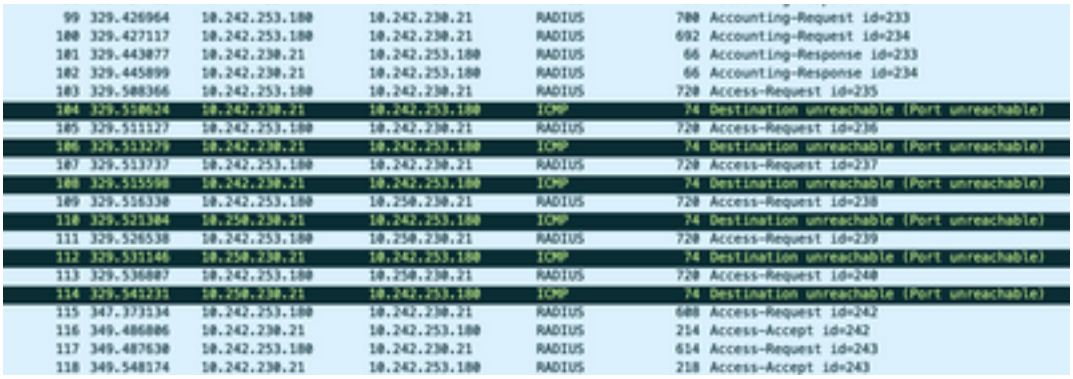
In questo esempio, *entrambi* i server RADIUS restituiscono una "porta non raggiungibile", 3 volte di seguito per ciascuno di essi. In questo modo, l'appliance ASA contrassegna *entrambi* i server RADIUS come inattivi entro millisecondi l'uno dall'altro.

Il risultato

Ogni indirizzo .21 in questo esempio era un indirizzo VIP F5. Ciò significa che dietro i VIPS c'erano dei cluster di nodi Cisco ISE nella persona del PSN.

La F5 ha restituito "port unreachable" (porta non raggiungibile) a causa di un difetto della F5.

Nell'esempio, il team Cisco TAC ha dimostrato con successo che l'ASA funzionava come previsto. In altre parole, ha inviato pacchetti radius e ricevuto 3 porte che prima non erano raggiungibili ed ha eseguito il comando Radius Server contrassegnato come 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

Informazioni correlate

- Supporto tecnico e download Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).