Guida alla risoluzione dei problemi ASA: Log mancanti nelle destinazioni Syslog

Sommario

Introduzione

Questo documento descrive come risolvere il problema della capacità dell'appliance ASA (Adaptive Security Appliance) di inviare syslog a diverse destinazioni e, più specificamente, i problemi dove vengono osservati sintomi come questi:

- Registrazione lenta in tempo reale su Adaptive Security Device Manager (ASDM).
- syslog intermittenti mancanti in una o più destinazioni syslog.

Operazioni preliminari

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni di questo documento si basano sulle appliance Cisco ASA e non sono limitate a una versione specifica del software ASA.

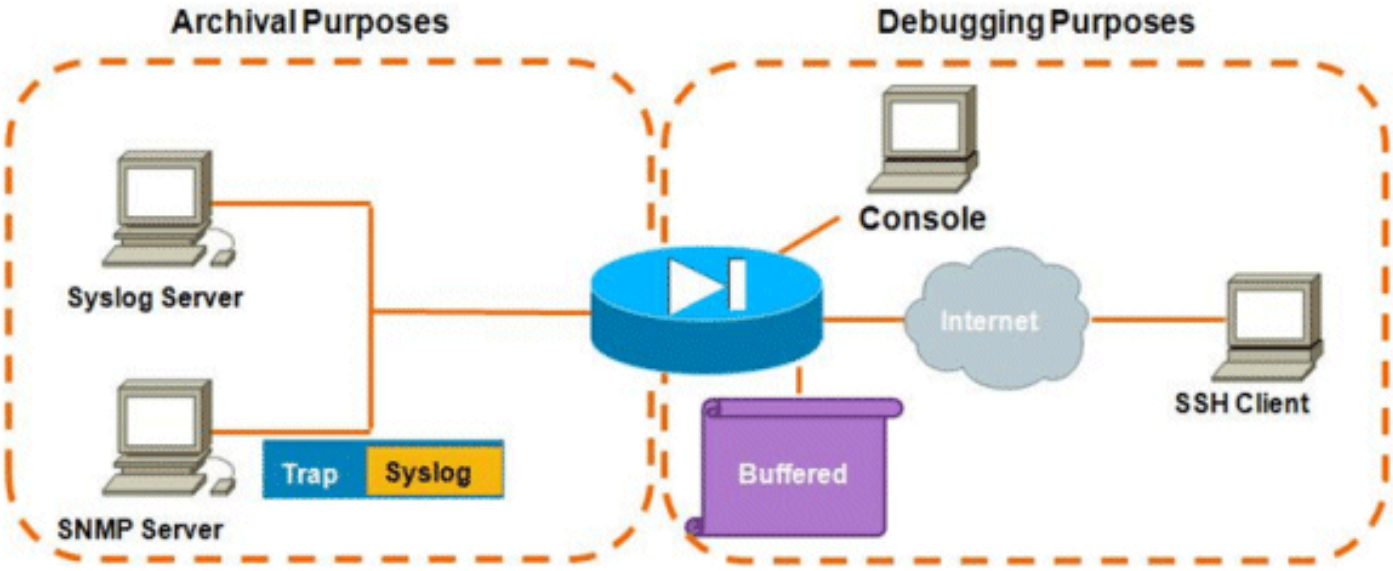
Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni

nei suggerimenti tecnici.

Informazioni sulle funzionalità

Come la maggior parte degli altri dispositivi Cisco, le appliance ASA possono inviare syslog a più destinazioni. Di seguito sono illustrate alcune delle destinazioni più utilizzate:



Il numero di destinazioni possibili è un vantaggio reale. Se scelti con attenzione, e come illustrato qui, possono essere ampiamente classificati in due categorie principali in base allo scopo che servono:

- Archiviazione
- Debug e risoluzione dei problemi in tempo reale

Nella maggior parte delle reti è sufficiente abilitare solo le destinazioni di archiviazione, a meno che non sia necessaria una o più destinazioni di debug. Allo stesso tempo, e molto spesso, i problemi derivano dall'abilitazione simultanea di più destinazioni di syslog a livelli di log elevati, ad esempio informativo (livello 6) o superiore.

Metodologia di risoluzione dei problemi

Quando si verificano problemi di perdita di informazioni di syslog in una o più destinazioni, è consigliabile verificare quanto segue:

- Esaminare la configurazione syslogging (output di **show run logging**).
- Esaminare l'output della **coda di registrazione** del **comando show**.

Analisi dei dati

Verifica della configurazione di Syslogging

Attenersi alla seguente procedura:

1. Verificare che il messaggio syslog desiderato non sia disabilitato dal comando **no logging**

message *<ID>*.

2. Dopo la conferma, controllare il numero di destinazioni syslog abilitate e il livello a cui ogni log viene inviato a ciascuna. Questo è un esempio di una tale configurazione:

```
logging enable
logging timestamp
logging standby
logging console informational
logging buffered informational
logging trap informational
logging asdm informational
logging device-id hostname
logging host inside 172.16.110.32
```

Nell'esempio, l'ASA invia i syslog a 4 destinazioni diverse a livello informativo (livello 6).

Output della coda di registrazione di visualizzazione

Con una configurazione come questa, in cui più destinazioni ricevono grandi quantità di messaggi di log, è possibile che l'ASA scarti i messaggi di syslog a causa di un overflow della coda di log. In questi casi, l'output sarà simile al seguente:

```
ciscoasa# show logging queue

   Logging Queue length limit : 512 msg(s)
   2352325 msg(s) discarded due to queue overflow
   0 msg(s) discarded due to memory allocation failure
   Current 512 msg on queue, 512 msgs most on queue
```

Per impostazione predefinita, la coda di registrazione contiene 512 messaggi.

Problemi comuni

Quando si verificano problemi in cui i messaggi syslog non vengono registrati, prendere in considerazione le seguenti opzioni:

- Disabilita la registrazione della console. L'accesso alla console **non deve** essere abilitato per il normale funzionamento. La registrazione della console deve essere utilizzata solo per la risoluzione dei problemi in tempo reale, con un livello di registrazione basso o traffico basso. Se si accede alla console con una velocità elevata, il processo di registrazione limiterà notevolmente la velocità dei messaggi. La console è in grado di registrare i messaggi solo a 9600 bps e non richiede una quantità di log prima di iniziare a eseguire il dump nella console superiore a quella che la console può inviare allo schermo. In questo caso, i registri inizieranno ad essere memorizzati nel buffer nella coda di registrazione. Una volta che la coda di registrazione si è riempita, i messaggi verranno eliminati.
- Aumentare le dimensioni della coda di log oltre il 512. La coda di log massima è 1024 su ASA-5505, 2048 su ASA-5510 e 8192 su tutte le altre piattaforme. Nota: La coda di registrazione viene utilizzata per i "burst" dei syslog. Se la velocità di trasmissione dei syslog è superiore a quella che l'ASA è in grado di trasmettere alle diverse destinazioni, il limite della coda di registrazione non sarà sufficiente.
- Disabilitare i singoli messaggi syslog non desiderati per l'archiviazione. Usare il comando no logging message *<syslog_id>* per disabilitare i singoli syslog.
- Fare attenzione a registrare i messaggi sul disco (flash) dell'appliance ASA. La scrittura sul

flash è un'operazione molto lenta. Un'eccessiva capacità di log per la memoria flash causerà l'archiviazione dei file syslog da parte dell'ASA nella memoria, che finirà per esaurire tutta la memoria (RAM) disponibile. Inoltre, la registrazione di grandi quantità di messaggi syslog nella memoria flash può causare un aumento della CPU. Si consiglia di registrare nella memoria flash solo i messaggi di livello 1 (che coprono gli eventi critici del sistema).

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems