ASA gids voor probleemoplossing: Ontbrekende loggen op Syslog-bestemming(en)

Inhoud

Inleiding
Voordat u begint
Vereisten
Gebruikte componenten
Conventies
Functieinformatie
Methode voor probleemoplossing
Gegevensanalyse
Controleer de configuratie van het systeem
Uitvoer van de blogwachtrij
Vaak voorkomende problemen
Gerelateerde informatie

Inleiding

Dit document beschrijft hoe het probleem moet worden opgelost met de mogelijkheden van de adaptieve security applicatie (ASA) om syslogs naar verschillende bestemmingen te sturen, en meer in het bijzonder kwesties waar symptomen zoals deze worden waargenomen:

- Traag real-time loggen op Adaptieve Security Devices Manager (ASDM).
- Intermitterende blogs vermist op een of meer bestemmingen.

Voordat u begint

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

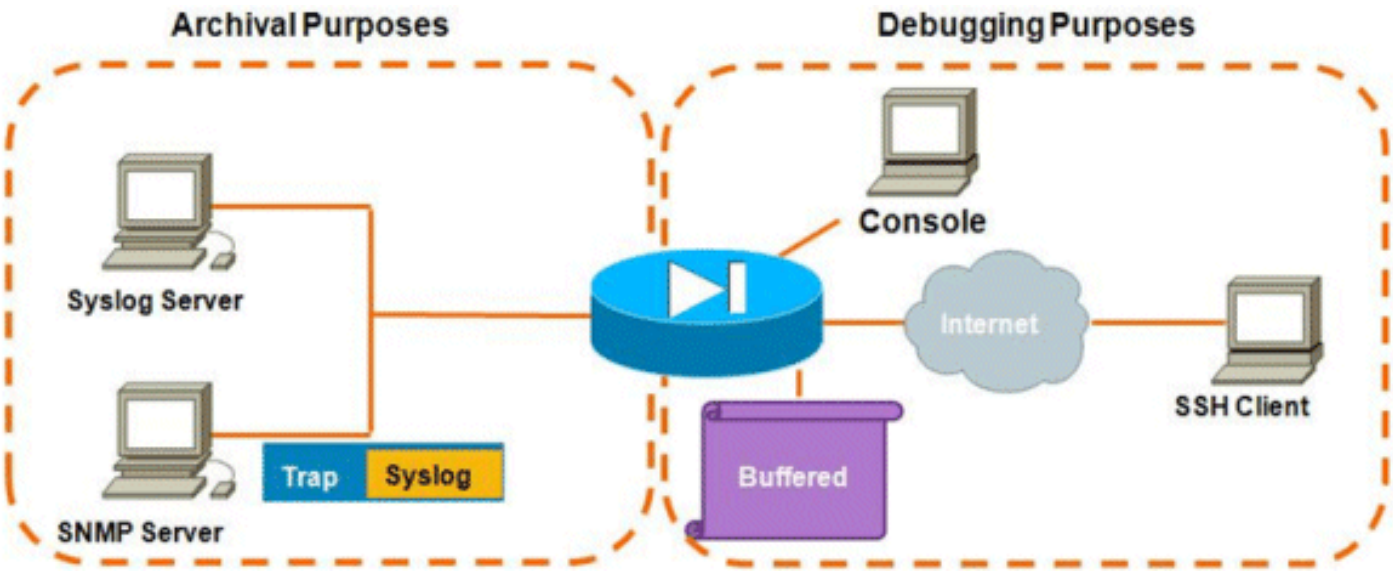
De informatie in dit document is gebaseerd op Cisco ASA en is niet beperkt tot een specifieke ASA-softwareversie.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Functieinformatie

ASA's zijn, net als de meeste andere Cisco-apparaten, in staat systemen naar meerdere syslig-bestemmingen te verzenden. Enkele van de meest gebruikte bestemmingen worden hier geïllustreerd:



Het aantal mogelijke bestemmingen is een reëel voordeel. Indien zorgvuldig gekozen, en zoals hier wordt geïllustreerd, kunnen zij globaal in twee categorieën worden ingedeeld op basis van het doel dat zij dienen:

- Archief
- Realtime foutherstel/probleemoplossing

In de meeste netwerken is het voldoende om slechts de toegelaten archiefbestemmingen te hebben tenzij één of meer van de bestemmingen die het debuggen ondergaan noodzakelijk zijn. Op hetzelfde moment, en heel vaak, komen problemen voort uit het tegelijkertijd mogelijk maken van meerdere syslogbestemmingen op hoge houtkap zoals informatie (niveau 6) of hoger.

Methode voor probleemoplossing

Wanneer een probleem zich voordoet met een verlies aan syslig-informatie op een of meer bestemmingen, kunt u twee dingen controleren:

- Bekijk de configuratie van het systeem (uitvoer van **testrun-vastlegging**).
- Kijk naar de uitvoer van de **blogwachtrij.**

Gegevensanalyse

Controleer de configuratie van het systeem

Voer de volgende stappen uit:

1. Zorg ervoor dat het zoekbericht niet wordt uitgeschakeld met de opdracht **Geen logbericht** ***<ID>***.

2. Na bevestiging, bekijk het aantal toegelaten syslogbestemmingen en het niveau waarop elk logboek naar elk wordt verzonden. Dit is een voorbeeld van zo'n configuratie:

```
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
```

In dit voorbeeld stuurt de ASA systemen naar 4 verschillende bestemmingen op informatieniveau (niveau 6).

Uitvoer van de blogwachtrij

Met een configuratie zoals het bovenstaande, waar meerdere bestemmingen grote hoeveelheden logberichten ontvangen, kunt u in een situatie belanden waar de ASA syslipberichten laat vallen door een overstroming van de houtwachtrij. In dergelijke gevallen wordt de output hier ongeveer gelijk aan weergegeven:

```
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
```

Standaard houdt de houtwachtrij 512 meldingen in.

Vaak voorkomende problemen

Denk bij het bekijken van kwesties waar de syslogberichten niet worden geregistreerd aan deze opties:

- Compenhoutkap uitschakelen. Vastleggen op de console **zou niet** voor normaal gebruik kunnen worden ingeschakeld. De loggen van de console zou slechts voor de oplossing in real-time, met of laag houtklokniveau of laag verkeer moeten worden gebruikt. Wanneer u met een hoog tempo aan de console inlogt, zal het logproces de berichten aanzienlijk beperken. De console is alleen in staat om berichten te registreren bij 9600 bps, en het neemt geen van logbestanden mee voordat het meer naar de console gaat dumpen dan de console kan uitvoeren naar het scherm. In deze situatie worden de logbestanden opgeslagen in de houtwachtrij. Zodra de houtkaprij vol is, worden de berichten munt laten vallen.
- Vergroot de grootte van de houtkapwachtrij tot boven 512. De maximale houtkap is 1024 op de ASA-5505, 2048 op de ASA-5510 en 8192 op alle andere platforms. Opmerking: De houtkaprij wordt gebruikt voor "uitbarstingen" van syslogs. Als het aanhoudende aantal syslogs sneller is dan de ASA ze naar de verschillende bestemmingen kan doorgeven, zal geen blogrijbeperkingen groot genoeg zijn.
- Schakel individuele syslogberichten uit die u niet in archivering wilt opslaan. Geef de opdracht no logging bericht *<syslog_id>* uit om individuele syslogs uit te schakelen.
- Wees voorzichtig met logberichten naar de disk (flitser) van de ASA. Schrijven naar de flitser is een zeer langzame operatie. Excessieve houtkap aan flitser zal de ASA ertoe aanzetten de

syslog bestanden in het geheugen op te buffer, uiteindelijk alle beschikbare geheugen (RAM) vernietigen. Bovendien kan het registreren van grote hoeveelheden syslogberichten aan flitser de CPU verhogen. Aanbevolen wordt alleen om niveau 1-berichten naar flitser te loggen (die kritieke systeemgebeurtenissen bestrijken).

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems