ASA 문제 해결 가이드: Syslog 대상에서 로그 누락

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance)의 기능을 통해 다양한 목적지로 syslog를 전송하는 문제를 해결하는 방법, 특히 이러한 증상이 관찰되는 문제에 대해 설명합니다.

- ASDM(Adaptive Security Device Manager)에서 느린 실시간 로깅.
- 하나 이상의 syslog 대상에서 간헐적인 syslog가 누락되었습니다.

시작하기 전에

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

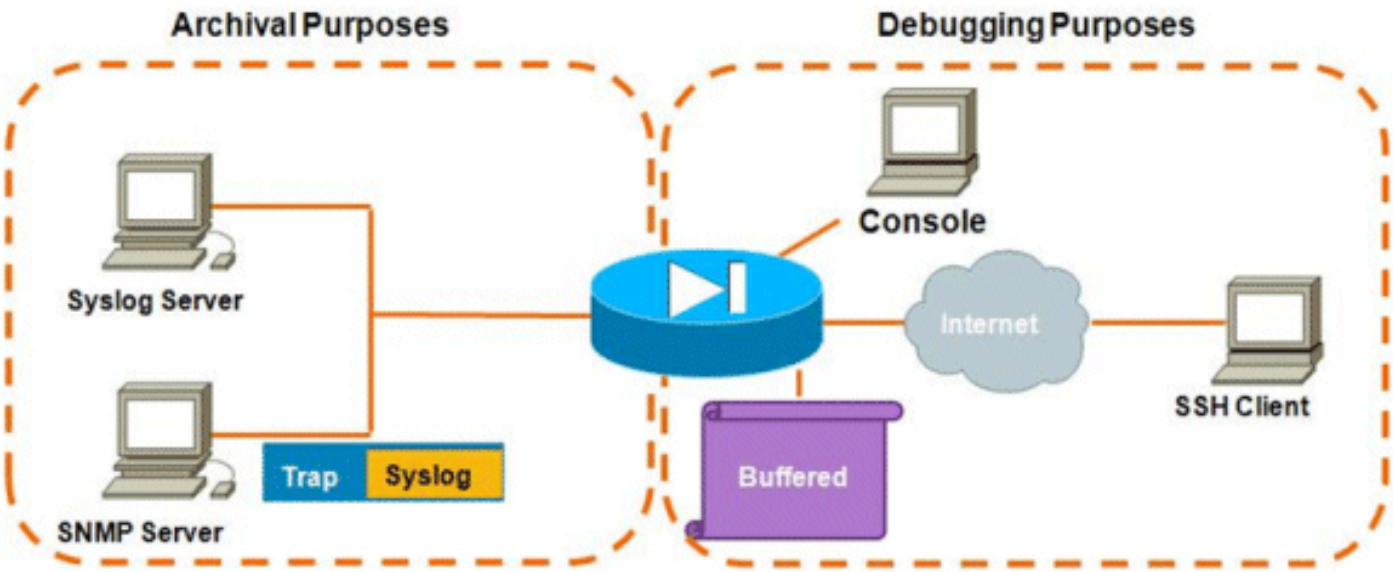
이 문서의 정보는 Cisco ASA를 기반으로 하며 특정 ASA 소프트웨어 버전에 국한되지 않습니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

기능 정보

대부분의 다른 Cisco 디바이스처럼 ASA는 여러 syslog 대상으로 syslog를 전송할 수 있습니다. 다음은 자주 사용되는 목적지 중 일부에 대한 설명입니다.



가능한 대상의 수가 실질적인 이점입니다. 주의깊게 선택되고 여기에 설명된 대로, 이러한 범주는 제공 목적에 따라 크게 두 가지 주요 범주로 분류될 수 있습니다.

- 보관
- 실시간 디버깅/문제 해결

대부분의 네트워크에서는 하나 이상의 디버깅 대상이 필요하지 않으면 아카이브 대상만 활성화할 수 있습니다. 정보(수준 6) 이상 등의 높은 로깅 레벨에서 동시에 여러 syslog 대상을 활성화하여 발생하는 문제가 동시에 자주 발생합니다.

문제 해결 방법론

하나 이상의 대상에서 syslog 정보가 손실되는 문제가 발생할 때마다 다음 두 가지를 확인해야 합니다.

- syslogging 컨피그레이션을 검토합니다(**show run logging 출력**).
- **show logging queue**의 출력을 **확인합니다.**

데이터 분석

Syslog 구성 검토

다음 단계를 완료하십시오.

1. 찾고 있는 syslog 메시지가 no logging **message *<ID>* 명령**으로 비활성화되지 않았는지 **확인합니다.**
2. 확인되면 활성화된 syslog 대상 수 및 각 로그가 각 로그로 전송되는 레벨을 확인합니다. 다음은 이러한 구성의 예입니다.

```
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
```

이 예에서 ASA는 정보 레벨(레벨 6)에서 4개의 서로 다른 목적지로 syslog를 전송합니다.

show logging queue 출력

여러 대상이 많은 로그 메시지를 수신하는 위와 같은 컨피그레이션을 사용하면 ASA가 로깅 대기열의 오버플로로 인해 syslog 메시지를 삭제하는 상황을 실행할 수 있습니다. 이러한 경우 다음과 유사한 출력이 표시됩니다.

```
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
```

기본적으로 로깅 대기열에는 512개의 메시지가 저장됩니다.

일반적인 문제

syslog 메시지가 기록되지 않는 문제로 실행할 경우 다음 옵션을 고려하십시오.

- 콘솔 로깅을 비활성화합니다. 콘솔 로그인은 정상 작업**에** 대해 활성화해서는 **안 됩니다**. 콘솔 로깅은 로깅 수준이 낮거나 트래픽이 낮은 실시간 문제 해결에만 사용해야 합니다. 콘솔에 높은 속도로 로그인하면 로깅 프로세스가 메시지를 크게 제한합니다. 콘솔은 9600bps의 메시지만 로깅할 수 있으며 콘솔이 화면에 출력할 수 있는 것보다 콘솔에 더 많은 메시지를 덤프하기 시작하기 전에 로그가 오래 걸리지 않습니다. 이 경우 로그는 로깅 대기열에서 버퍼링되기 시작합니다. 로깅 대기열이 가득 차면 메시지가 tail-dropp됩니다.
- 로깅 대기열의 크기를 512 이상으로 늘립니다. 최대 로깅 대기열은 ASA-5505의 경우 1024, ASA-5510의 경우 2048, 다른 모든 플랫폼의 경우 8192입니다. 참고: 로깅 대기열은 syslog의 "버스트"에 사용됩니다. 지속적인 syslog 속도가 ASA에서 여러 대상으로 전송할 수 있는 속도보다 빠른 경우 로깅 큐 제한은 충분히 커지지 않습니다.
- 아카이빙에 관심이 없는 개별 syslog 메시지를 비활성화합니다. 개별 syslog를 비활성화하려면 no logging **message** ***<syslog_id>*** **명령**을 실행합니다.
- ASA의 디스크(플래시)에 메시지를 기록하지 않도록 주의하십시오. 플래시에 쓰는 것은 매우 느린 작업입니다. 플래시에 대한 과도한 로깅은 ASA가 syslog 파일을 메모리에 버퍼링하여 사용 가능한 모든 메모리(RAM)를 구축합니다. 또한 플래시에 대량의 syslog 메시지를 로깅하면 CPU가 증가할 수 있습니다. Level 1 메시지만 플래시에 로깅하는 것이 좋습니다(중요한 시스템 이벤트를 다룹니다).

관련 정보

- 기술 지원 및 문서 – Cisco Systems