Network Services Orchestrator 5.X 로그에 대한 Syslog 구성

목차

소개

이 문서에서는 NSO(Network Services Orchestrator) 5.x용 syslog 서버를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

구성 요구 사항

설치가 완료되면 다음 파일이 필요합니다.

- 구성 파일: /etc/rsyslog.conf .

- 특정 컨피그레이션 파일로 정의된 디렉토리 **/etc/rsyslog.d/.**

이 컨피그레이션에서는 여러 Linux 배포판에서 기본적으로 제공되는 rsyslog 서비스를 사용합니다. 서버에서 사용할 수 없는 경우 다음과 같이 다운로드합니다(RHEL/CentOS).

```
yum install rsyslog
```

NSO 5.1에서는 ncs.conf 오래된 파일로 만들었습니다.

참고: Cisco 보안 요구 사항을 준수하기 위해 UDP를 통한 syslog 지원이 제거되었습니다. 기본값 syslog 기능을 제공합니다 libc syslog(3) 을(를) 계속 사용할 수 있습니다.

NSO 로그를 원격 서버로 리디렉션하려면 NSO Syslog Relay Readme 파일을 참조하고 syslog 데몬 릴레이 컨피그레이션을 사용합니다.

설정

컨피그레이션에는 두 세트의 컨피그레이션 파일이 필요합니다. 하나는 NSO가 실행되는 서버, 이 경우 발신자, 다른 하나는 모든 로그를 저장하는 수신자(원격 서버)에 있습니다.

1단계: ncs.conf 파일에 다음 섹션이 있습니다.

```
<logs>
<syslog-config>
<facility>daemon</facility>
</syslog-config>
...
</logs>
```

2단계: /etc/rsyslog.conf 다음과 같이 표시됩니다.

- 아래 #### RULES ####; 섹션 추가:

```
*.* @remote_ip
```

예를 들면 다음과 같습니다.

```
*.* @10.127.200.61
```

이 행은 rsyslog 서비스로 지정된 IP의 'all' 데몬 로그를 원격 호스트로 리디렉션하도록 지시합니다.

3단계: /etc/rsyslog.d/ 다음 예제와 같은 경로.

- 새 파일은 Firepower Threat Defense에syslog daemon 네트워크를 통해 원격 서버로 전송할 파일에 대한 세부 정보.

예를 들면 다음과 같습니다.

```
$ModLoad imfile
$InputFileName /var/log/ncs/devel.log
$InputFileTag devel:
$InputFileStateFile stat-devel
$InputFileSeverity info
$InputFileFacility local6
$InputRunFileMonitor
...
```

- 모든 파일이 정의되고 세부 정보가 포함되면 프로토콜을 통해 파일이 전송되는 위치를 지정할 수 있습니다.

```
# Send over UDP
local6.* @remote_ip:port
```

예를 들면 다음과 같습니다.

```
local6.* @10.127.200.61:514
```

4단계: rsyslog 서비스:

```
service rsyslog restart
```

참고: 2~4단계는 발신자, 즉 NSO 서비스가 가동 중인 서버에서 실행해야 합니다.

5단계: 의 요구 사항에 따라 UDP/TCP 섹션의 코멘트를 제거하십시오. /etc/rsyslog.conf 파일:

<#root>

```
$ModLoad imudp
$UDPServerRun 514
```

참고: 514는 이 전송에 사용되는 포트입니다.

6단계: 수정 /etc/rsyslog.conf 파일을 클릭합니다. 아래에 행을 추가합니다. ###MODULES### 섹션:

```
$template FileTemplate,"/var/log/ncs-server/%programname%.log"
if $programname startswith 'devel' then -?FileTemplate
if $programname startswith 'audit' then -?FileTemplate
if $programname startswith 'ncs' then -?FileTemplate
if $programname startswith 'ncs-java-vm' then -?FileTemplate
if $programname startswith 'ncserr' then -?FileTemplate
```

참고: 디렉터리에 ncs-server라는 이름을 사용할 수 있습니다.

이 단계에서는 지정된 위치에 NSO에 특별히 로그를 저장하도록 규칙을 정의합니다.

7단계: rsyslog 서비스:

```
service rsyslog restart
```

참고: 5~7단계는 로그를 저장할 수신기인 원격 서버에서 실행해야 합니다.

추가 구성

syslog 데몬 릴레이 기능은 다음 단계를 통해 설정해야 합니다. 그러나 프로덕션 환경에서는 방화벽 서비스 및 SELinux가 일반적으로 활성화되어 있습니다. 활성화된 경우 로그는 원격으로 저장되지 않습니다. 이로 인해 문제가 발생하지 않도록 하려면 두 서버에서 다음 컨피그레이션을 추가해야 합니다.

- semanage port -a -t syslogd_port_t -p udp 514
- firewall-cmd --add-port=514/udp --permanent
- firewall-cmd --reload

확인

단계를 올바르게 수행한 경우 syslog 서버가 원격으로 설정되어 있습니다. 이를 확인하려면 다음을 수

행합니다.

원격 서버에서 다음을 수행합니다.

```
nc -l -u -p 514
```

보낸 사람:

```
logger "Message from client"
```

원격 서버가 다음 메시지를 받았어야 합니다.

```
May 11 22:12:10 nso-recreate root: Message from client
```

문제 해결

릴레이가 성공하지 못한 경우 컨피그레이션 파일을 다시 확인해야 합니다.

또한 NSO 및 rsyslog:

1. systemctl status ncs.service
   Expected output: [root@nso-recreate ncs]# systemctl status ncs.service ● ncs.service - LSB: NCS Loaded: loaded (/etc/rc.d/init.d/ncs; bad; vendor preset: disabled) Active: active (runnin) since Tue 2022-05-10 21:55:59 EDT; 24h ago ... No other lines in red in the status output.

2. service rsyslog status
   Expected output: [root@nso-recreate ncs]# service rsyslog status Redirectin to /bin/systemctl status rsyslog.service ● rsyslog.service - System Loggin Service Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled) Active: active (runnin) since Wed 2022-05-11 01:12:08 EDT; 21h ago ... No other lines in red in the status output.

방화벽 규칙 또는 SELinux 컨피그레이션을 확인할 수 있습니다. 원격 대상으로의 로그 전송을 차단할 수 있습니다.

1. systemctl status firewalld.service
2. sestatus

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.