Syslog voor Network Services Orchestrator-logbestanden 5.x configureren

Inhoud

Inleiding

Dit document beschrijft hoe u syslog-servers voor Network Services Orchestrator (NSO) 5.x. moet configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Configuratievereisten

Nadat de installatie is voltooid, zijn deze bestanden nodig:

- Het configuratiebestand is /etc/rsyslog.conf .
- Map gedefinieerd met specifieke configuratiebestanden is **/etc/rsyslog.d/**.

Voor deze configuratie, gebruik de rsyslog service die standaard beschikbaar is in verschillende Linux distributies. Als het niet beschikbaar is op de server, download het als volgt (RHEL/CentOS):

```
yum install rsyslog
```

Met NSO 5.1, de syslog-server elementen die deel uitmaakten van de ncs.conf dossier dat achterhaald was.

> **Opmerking:** Ondersteuning voor de syslog via UDP is verwijderd om te voldoen aan Cisco-beveiligingsvereisten. De standaardinstelling syslog functionaliteit via de libc syslog(3) is nog steeds beschikbaar.

Raadpleeg het leesmij-bestand van NSO Syslog Relay om NSO-logbestanden door te sturen naar een externe server en gebruik de configuratie van syslog daemon Relay.

Configuratie

Er zijn twee sets configuratiebestanden nodig voor de configuratie. De ene is op de server waar NSO wordt uitgevoerd, de afzender in dit geval, en de andere op de ontvanger (remote-server) die alle logbestanden opslaat.

Stap 1: Controleer of de ncs.conf bestand bevat deze sectie:

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

Stap 2: Configureer de /etc/rsyslog.conf als volgt:

- Onder #### RULES ####; deel toevoegen:

```
*.* @remote_ip
```

Voorbeeld:

```
*.* @10.127.200.61
```

Deze lijn geeft de rsyslog-service de opdracht om 'alle' daemon-logbestanden ook te sturen naar de externe host op de opgegeven IP.

Stap 3: Voeg een nieuw bestand toe in de /etc/rsyslog.d/ pad zoals in het volgende voorbeeld.

- Het nieuwe bestand is een configuratiebestand dat de rsyslog daemon details over welke bestanden worden verzonden over het netwerk naar de externe server.

Voorbeeld:

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

- Zodra alle bestanden zijn gedefinieerd en details bevatten, kunt u specificeren waar de bestanden worden verzonden via het protocol:

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

Voorbeeld:

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

Stap 4: Start het wasprogramma rsyslog service:

```
service rsyslog restart
```

> Opmerking: De stappen 2 tot 4 moeten worden uitgevoerd op de afzender, dat wil zeggen de server waarop de NSO-service is ingeschakeld.

Stap 5: Uncomment de sectie voor UDP/TCP gebaseerd op uw vereiste in /etc/rsyslog.conf bestand:

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

> Opmerking: 514 is de haven die voor deze overdracht wordt gebruikt.

Stap 6: Wijzig de /etc/rsyslog.conf bestand. Voeg de regels toe onder ###MODULES### Afdeling:

```
$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
```

> Opmerking: U kunt de naam ncs-server gebruiken voor uw map.

In deze stap worden de regels gedefinieerd om de logbestanden specifiek op te slaan naar NSO in aangewezen locatie.

Stap 7: Start het wasprogramma rsyslog service:

```
service rsyslog restart
```

Opmerking: Stap 5 tot en met 7 moet worden uitgevoerd op de ontvanger, de afstandsserver, waar de logbestanden moeten worden opgeslagen.

Aanvullende configuraties

De syslog daemon relay functionaliteit moet met deze stappen worden ingesteld. In een productieomgeving zijn de Firewallservice en SELinux meestal ingeschakeld. Als zij worden toegelaten, worden de logboeken niet opgeslagen ver. Om er zeker van te zijn dat dit geen problemen veroorzaakt, moet u deze configuraties op beide servers toevoegen:

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

Verificatie

Als de stappen correct zijn gevolgd, kan de syslog -server op afstand is ingesteld. U verifieert dit als volgt:

Op de afstandsserver:

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

Van de afzender:

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

De externe server moet dit bericht ontvangen hebben:

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

Problemen oplossen

In situaties waar het relay niet succesvol is, moet u de configuratiebestanden opnieuw controleren.

Het is ook nuttig de status van de nationale veiligheidsinstantie te bevestigen en 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.

U kunt controleren op firewallregels of SELinux-configuraties. Deze kunnen de logoverdracht naar de verre bestemming blokkeren.

1. systemctl status firewalld.service
2. sestatus

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.