Configurazione di Syslog per i registri di Network Services Orchestrator 5.X

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

- [Requisiti di configurazione](#)

[Configurazione](#)

[Configurazioni aggiuntive](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare i server syslog per Network Services Orchestrator (NSO) 5.x.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Requisiti di configurazione

Al termine dell'installazione, sono necessari i seguenti file:

- Il file di configurazione /etc/rsyslog.conf .
- La directory definita con i file di configurazione specifici è **/etc/rsyslog.d/**.

Per questa configurazione, utilizzare il servizio rsyslog, disponibile per impostazione predefinita in diverse distribuzioni Linux. Se non è disponibile sul server, scaricarlo come segue (RHEL/CentOS):

```
yum install rsyslog
```

Con NSO 5.1, gli elementi syslog-server che facevano parte ncs.conf file reso obsoleto.

Nota: il supporto per il syslog tramite UDP è stato rimosso per conformità ai requisiti di sicurezza di Cisco. Il valore predefinito syslog tramite libc syslog(3) è ancora disponibile.

Per reindirizzare i registri NSO su un server remoto, fare riferimento al file Readme di Syslog Relay NSO e utilizzare la configurazione del relay del daemon syslog.

Configurazione

Per la configurazione sono necessari due set di file di configurazione. Una si trova sul server in cui viene eseguito NSO, in questo caso il mittente e l'altra si trova sul ricevitore (server remoto) che memorizza tutti i registri.

Passaggio 1: verificare che il ncs.conf Il file contiene la seguente sezione:

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

Passaggio 2: configurare /etc/rsyslog.conf come segue:

- Inferiore #### RULES ####; sezione aggiungi:

```
*.* @remote_ip
```

Ad esempio:

```
*.* @10.127.200.61
```

Questa riga indica al servizio rsyslog di reindirizzare anche i log del daemon 'all' sull'host remoto all'indirizzo IP specificato.

Passaggio 3: Aggiungere un nuovo file nella /etc/rsyslog.d/ come illustrato nell'esempio seguente.

- Il nuovo file è un file di configurazione da comunicare alsyslog daemon dettagli sui file da inviare in rete al server remoto.

Ad esempio:

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

- Dopo aver definito tutti i file e averne fornito i dettagli, è possibile specificare dove inviare i file tramite il protocollo:

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

Ad esempio:

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

Passaggio 4: riavviare rsyslog servizio:

```
service rsyslog restart
```

Nota: i passaggi da 2 a 4 devono essere eseguiti sul mittente, ovvero sul server in cui è attivo il servizio NSO.

Passaggio 5: rimuovere il commento dalla sezione per UDP/TCP in base ai requisiti indicati nel /etc/rsyslog.conf file:

<#root>

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

Nota: la porta utilizzata per questo trasferimento è la 514.

Passaggio 6: Modificare la /etc/rsyslog.conf file. Aggiungere le righe in ###MODULES### sezione:

```
$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
```

Nota: è possibile utilizzare il nome ncs-server per la directory.

In questo passaggio vengono definite le regole per archiviare i registri in modo specifico nell'NSO nel percorso designato.

Passaggio 7: Riavviare rsyslog servizio:

```
service rsyslog restart
```

Nota: i punti da 5 a 7 devono essere eseguiti sul ricevitore, il server remoto, in cui si desidera archiviare i log.

Configurazioni aggiuntive

La funzionalità di inoltro del daemon syslog deve essere configurata eseguendo i seguenti passaggi. Tuttavia, in un ambiente di produzione il servizio Firewall e SELinux sono generalmente

attivati. Se attivati, i registri non vengono archiviati in remoto. Per evitare problemi, aggiungere le seguenti configurazioni su entrambi i server:

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

Verifica

Se i passaggi sono stati seguiti correttamente, il syslog il server è configurato in modalità remota. Per verificarlo:

Sul server remoto:

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

Dal mittente:

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

Il server remoto deve aver ricevuto questo messaggio:

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

Risoluzione dei problemi

Se l'inoltro non ha esito positivo, controllare nuovamente i file di configurazione.

È inoltre utile confermare lo stato di NSO e 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.

È possibile controllare le regole firewall o le configurazioni SELinux. che possono bloccare il trasferimento del log alla destinazione remota.

1. systemctl status firewalld.service
2. sestatus

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).