Configuration de Syslog pour les journaux Network Services Orchestrator 5.X

Table des matières

Introduction

Ce document décrit comment configurer les serveurs syslog pour Network Services Orchestrator (NSO) 5.x.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Configuration requise

Une fois l'installation terminée, les fichiers suivants sont nécessaires :

- Le fichier de configuration est `/etc/rsyslog.conf` .

- Le répertoire défini avec des fichiers de configuration spécifiques est **/etc/rsyslog.d/**.

Pour cette configuration, utilisez le service rsyslog qui est disponible par défaut dans plusieurs distributions Linux. S'il n'est pas disponible sur le serveur, téléchargez-le comme suit (RHEL/CentOS) :

```
yum install rsyslog
```

Avec NSO 5.1, les éléments syslog-server qui faisaient partie de la ncs.conf qui a été rendu obsolète.

Remarque : la prise en charge du syslog via UDP a été supprimée afin de respecter les exigences de sécurité de Cisco. La valeur par défaut syslog fonctionnalité via le libc syslog(3) est toujours disponible.

Afin de rediriger les journaux NSO vers un serveur distant, référez-vous au fichier NSO Syslog Relay Readme et utilisez la configuration du relais de démon Syslog.

Configuration

Deux jeux de fichiers de configuration sont nécessaires pour la configuration. L'un se trouve sur le serveur où NSO est exécuté, l'expéditeur dans ce cas, et l'autre est sur le récepteur (serveur distant) qui stocke tous les journaux.

Étape 1 : vérifiez que le ncs.conf a cette section :

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

Étape 2 : configurez le /etc/rsyslog.conf comme suit :

- Sous #### RULES ####; ajout de section :

```
*.* @remote_ip
```

Exemple :

```
*.* @10.127.200.61
```

Cette ligne indique au service rsyslog de rediriger également « tous » les journaux de démon vers l'hôte distant à l'adresse IP spécifiée.

Étape 3 : ajoutez un nouveau fichier dans le /etc/rsyslog.d/ comme indiqué dans l'exemple suivant.

- Le nouveau fichier est un fichier de configuration qui indique à l'syslog daemon des détails sur les fichiers à envoyer sur le réseau au serveur distant.

Exemple :

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

- Une fois que tous les fichiers sont définis et contiennent des détails, vous pouvez spécifier où les fichiers sont envoyés via le protocole :

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

Exemple :

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

Étape 4 : Redémarrez le rsyslog service :

```
service rsyslog restart
```

Remarque : les étapes 2 à 4 doivent être exécutées sur l'expéditeur, c'est-à-dire sur le serveur sur lequel le service NSO est activé.

Étape 5 : supprimez les commentaires de la section relative au protocole UDP/TCP en fonction de vos besoins dans la /etc/rsyslog.conf fichier:

<#root>

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

Remarque : 514 est le port utilisé pour ce transfert.

Étape 6 : Modifiez le /etc/rsyslog.conf fichier. Ajoutez les lignes sous ###MODULES### section :

```
$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
```

Remarque : vous pouvez utiliser le nom ncs-server pour votre répertoire.

Dans cette étape, les règles sont définies pour stocker les journaux spécifiquement à NSO dans un emplacement désigné.

Étape 7 : Redémarrez le rsyslog service :

```
service rsyslog restart
```

Remarque : les étapes 5 à 7 doivent être exécutées sur le récepteur, le serveur distant, où les journaux sont destinés à être stockés.

Configurations supplémentaires

La fonctionnalité de relais de démon Syslog doit être configurée en procédant comme suit. Cependant, dans un environnement de production, le service de pare-feu et SELinux sont

généralement activés. S'ils sont activés, les journaux ne sont pas stockés à distance. Pour vous assurer que cela ne pose aucun problème, vous devez ajouter ces configurations sur les deux serveurs :

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

Vérification

Si les étapes ont été suivies correctement, le syslog est configuré à distance. Pour vérifier ceci :

Sur le serveur distant :

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

De l'expéditeur :

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

Le serveur distant doit avoir reçu ce message :

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

Dépannage

Dans les cas où le relais échoue, vous devez vérifier à nouveau les fichiers de configuration.

Il est également utile de confirmer le statut de l'ONS et 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.

Vous pouvez vérifier les règles de pare-feu ou les configurations SELinux. Ils peuvent bloquer le transfert du journal vers la destination distante.

1. systemctl status firewalld.service
2. sestatus

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.