Configurar Syslog para registros de Network Services Orchestrator 5.X

Contenido

Introducción

Este documento describe cómo configurar servidores syslog para Network Services Orchestrator (NSO) 5.x.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Requisitos de configuración

Una vez finalizada la instalación, se necesitan estos archivos:

- El archivo de configuración es /etc/rsyslog.conf .
- El directorio definido con los archivos de configuración específicos es **/etc/rsyslog.d/**.

Para esta configuración, utilice el servicio rsyslog que está disponible de forma predeterminada en varias distribuciones de Linux. En caso de que no esté disponible en el servidor, descárguelo de la siguiente manera (RHEL/CentOS):

```
yum install rsyslog
```

Con NSO 5.1, los elementos syslog-server que formaban parte del ncs.conf que se ha vuelto obsoleto.

> **Nota:** El soporte para el syslog a través de UDP ha sido eliminado para cumplir con los requisitos de seguridad de Cisco. El valor predeterminado syslog mediante el libc syslog(3) todavía está disponible.

Para redirigir los registros de NSO a un servidor remoto, consulte el archivo NSO Syslog Relay Readme y utilice la configuración de syslog daemon relay.

Configuración

Se necesitan dos conjuntos de archivos de configuración para la configuración. Uno está en el servidor donde se ejecuta NSO, el remitente en este caso, y el otro está en el receptor (servidor remoto) que almacena todos los registros.

Paso 1: Compruebe que el ncs.conf tiene esta sección:

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

Paso 2: Configure el /etc/rsyslog.conf como sigue:

- Bajo #### RULES ####; sección add:

```
*.* @remote_ip
```

Por ejemplo:

```
*.* @10.127.200.61
```

Esta línea indica al servicio rsyslog que también redirija 'todos' los registros de daemon al host remoto en la IP especificada.

Paso 3: Agregue un nuevo archivo en el /etc/rsyslog.d/ como se muestra en el siguiente ejemplo.

- El nuevo archivo es un archivo de configuración para indicarle alsyslog daemon detalles acerca de qué archivos se enviarán a través de la red al servidor remoto.

Por ejemplo:

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

- Una vez que todos los archivos están definidos y contienen detalles, puede especificar dónde se envían los archivos a través del protocolo:

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

Por ejemplo:

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

Paso 4: Reinicie el rsyslog servicio:

```
service rsyslog restart
```

> **Nota:** Los pasos 2 a 4 deben ejecutarse en el remitente, es decir, el servidor en el que está activo el servicio NSO.

Paso 5: Quite los comentarios de la sección para UDP/TCP según los requisitos del /etc/rsyslog.conf archivo:

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

> **Nota:** 514 es el puerto utilizado para esta transferencia.

Paso 6: Modifique el **/etc/rsyslog.conf** archivo. Agregue las líneas situadas debajo de ###MODULES### sección:

```
$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:** Puede utilizar el nombre ncs-server para el directorio.

En este paso, se definen las reglas para almacenar los registros específicamente en NSO en una ubicación designada.

Paso 7: Reinicie el rsyslog servicio:

```
service rsyslog restart
```

> **Nota:** Los pasos 5 a 7 deben ejecutarse en el receptor, el servidor remoto, donde se deben almacenar los registros.

Configuraciones adicionales

La funcionalidad de syslog daemon relay se debe configurar con estos pasos. Sin embargo, en un entorno de producción, el servicio Firewall y SELinux suelen estar habilitados. Si están habilitados, los registros no se almacenan de forma remota. Para asegurarse de que esto no cause ningún problema, debe agregar estas configuraciones en ambos servidores:

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

Verificación

Si los pasos se han seguido correctamente, el syslog el servidor se configura de forma remota. Para verificar esto:

En el servidor remoto:

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

Del remitente:

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

El servidor remoto debe haber recibido este mensaje:

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

Troubleshoot

En situaciones en las que la retransmisión no es exitosa, debe verificar los archivos de configuración nuevamente.

También es útil confirmar el estado de NSO y 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.

Puede verificar si hay reglas de firewall o configuraciones de SELinux. Esto puede bloquear la transferencia del registro al destino remoto.

1. systemctl status firewalld.service
2. sestatus

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).