Configurar Syslog para Logs do Network Services Orchestrator 5.X

Contents

Introdução

Este documento descreve como configurar servidores syslog para o Network Services Orchestrator (NSO) 5.x.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Requisitos de configuração

Após a conclusão da instalação, estes arquivos são necessários:

- O arquivo de configuração é /etc/rsyslog.conf .
- O diretório definido com arquivos de configuração específicos é **/etc/rsyslog.d/.**

Para esta configuração, use o serviço rsyslog que está disponível por padrão em várias distribuições Linux. Caso não esteja disponível no servidor, baixe-o da seguinte forma (RHEL/CentOS):

```
yum install rsyslog
```

Com o NSO 5.1, os elementos syslog-server que faziam parte do ncs.conf arquivo que se tornou obsoleto.

✎ Observação: o suporte para o syslog via UDP foi removido para atender aos requisitos de segurança da Cisco. O padrão syslog por meio do libc syslog(3) ainda está disponível.

Para redirecionar os logs NSO para um servidor remoto, consulte o arquivo NSO Syslog Relay Readme e use a configuração de relay do daemon de syslog.

Configuração

São necessários dois conjuntos de arquivos de configuração para a configuração. Um está no servidor onde o NSO é executado, o remetente nesse caso, e o outro está no receptor (servidor remoto) que armazena todos os logs.

Etapa 1: Verifique se o ncs.conf arquivo tem esta seção:

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

Etapa 2: Configure o /etc/rsyslog.conf do seguinte modo:

- Sob #### RULES ####; seção aditar:

```
*.* @remote_ip
```

Por exemplo:

```
*.* @10.127.200.61
```

Essa linha direciona o serviço rsyslog para também redirecionar todos os logs de daemon para o host remoto no IP especificado.

Etapa 3: adicione um novo arquivo no /etc/rsyslog.d/ como mostrado no próximo exemplo.

- O novo arquivo é um arquivo de configuração para informar ao usuáriosyslog daemon detalhes sobre quais arquivos devem ser enviados pela rede ao servidor remoto.

Por exemplo:

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

- Quando todos os arquivos estiverem definidos e contiverem detalhes, você poderá especificar para onde os arquivos serão enviados por meio do protocolo:

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

Por exemplo:

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

Etapa 4: reinicie o rsyslog serviço:

```
service rsyslog restart
```

Observação: as etapas 2 a 4 devem ser executadas no remetente, ou seja, no servidor em que o serviço NSO está ativo.

Etapa 5: Remova o comentário da seção para UDP/TCP com base em seu requisito no /etc/rsyslog.conf arquivo:

<#root>

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

Observação: 514 é a porta usada para essa transferência.

Passo 6: Modifique o /etc/rsyslog.conf arquivo. Adicione as linhas abaixo de ###MODULES### seção:

```
$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
```

Observação: você pode usar o nome ncs-server para seu diretório.

Nesta etapa, as regras são definidas para armazenar os logs especificamente para NSO no local designado.

Etapa 7: reinicie o rsyslog serviço:

```
service rsyslog restart
```

Observação: as etapas de 5 a 7 devem ser executadas no receptor, o servidor remoto, onde os logs devem ser armazenados.

Configurações adicionais

A funcionalidade do daemon relay de syslog deve ser configurada com estas etapas. No entanto, em um ambiente de produção, o serviço de firewall e o SELinux geralmente são ativados. Se

estiverem ativados, os logs não serão armazenados remotamente. Para garantir que isso não cause problemas, você precisa adicionar estas configurações em ambos os servidores:

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

Verificação

Se as etapas tiverem sido seguidas corretamente, o syslog o servidor está configurado remotamente. Para verificar isso:

No servidor remoto:

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

Do remetente:

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

O servidor remoto deve ter recebido esta mensagem:

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

Troubleshooting

Em situações em que a retransmissão não é bem-sucedida, você precisa verificar os arquivos de configuração novamente.

É igualmente útil confirmar o estatuto de NSO e de 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.

Você pode verificar as regras de firewall ou as configurações do SELinux. Eles podem bloquear a transferência de registro para o destino remoto.

1. systemctl status firewalld.service
2. sestatus

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.