

# Syslog für Network Services Orchestrator 5.x- Protokolle konfigurieren

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurationsanforderungen](#)

[Konfiguration](#)

[Zusätzliche Konfigurationen](#)

[Verifizierung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird die Konfiguration von Syslog-Servern für Network Services Orchestrator (NSO) 5.x beschrieben.

## Voraussetzungen

### Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Hintergrundinformationen

### Konfigurationsanforderungen

Nach Abschluss der Installation werden folgende Dateien benötigt:

- Konfigurationsdatei ist `/etc/rsyslog.conf` .
- Verzeichnis, das mit bestimmten Konfigurationsdateien definiert ist `/etc/rsyslog.d/`.

Verwenden Sie für diese Konfiguration den Dienst rsyslog, der standardmäßig in mehreren Linux-Distributionen verfügbar ist. Falls es auf dem Server nicht verfügbar ist, laden Sie es wie folgt herunter (RHEL/CentOS):

```
yum install rsyslog
```

Mit NSO 5.1 können die Syslog-Server-Elemente, die `ncs.conf` Datei, die veraltet ist.

**Anmerkung:** Die Unterstützung für das Syslog über UDP wurde entfernt, um die Sicherheitsanforderungen von Cisco zu erfüllen. Der Standardwert `syslog` über die `libc syslog(3)` ist noch verfügbar.

Um NSO-Protokolle an einen Remote-Server umzuleiten, lesen Sie die [Readme](#)-Datei für das [NSO-Syslog-Relay](#), und verwenden Sie die Syslog-Daemon-Relay-Konfiguration.

## Konfiguration

Für die Konfiguration werden zwei Gruppen von Konfigurationsdateien benötigt. Einer befindet sich auf dem Server, auf dem der NSO ausgeführt wird, in diesem Fall der Sender, der andere auf dem Empfänger (Remote-Server), auf dem alle Protokolle gespeichert werden.

**Schritt 1:** Prüfen Sie, ob `ncs.conf`-Datei hat diesen Abschnitt:

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

**Phase 2:** Konfigurieren Sie `/etc/rsyslog.conf` wie folgt:

- Unter `#### RULES ####`; Abschnitt hinzufügen:

```
*.* @remote_ip
```

**Beispiele:**

```
*.* @10.127.200.61
```

Diese Zeile weist den rsyslog-Dienst an, ebenfalls alle Daemon-Protokolle an den Remote-Host mit der angegebenen IP umzuleiten.

**Schritt 3:** Neue Datei hinzufügen im `/etc/rsyslog.d/` Pfad, wie im nächsten Beispiel gezeigt.

- Die neue Datei ist eine Konfigurationsdatei, die dem `rsyslog daemon` Details darüber, welche Dateien über das Netzwerk an den Remote-Server gesendet werden.

**Beispiele:**

```
$ModLoad imfile
```

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

- Sobald alle Dateien definiert sind und Details enthalten, können Sie angeben, wohin die Dateien über das Protokoll gesendet werden:

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

### Beispiele:

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

### Schritt 4: Starten Sie den rsyslog Dienst:

```
service rsyslog restart
```

**Anmerkung:** Die Schritte 2 bis 4 müssen für den Absender ausgeführt werden, d. h. den Server, auf dem der NSO-Service aktiv ist.

### Schritt 5: Kommentieren Sie den Abschnitt für UDP/TCP aus, basierend auf Ihren Anforderungen im `/etc/rsyslog.conf` Datei:

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

**Anmerkung:** Der Port 514 wird für diese Übertragung verwendet.

### Schritt 6: Ändern Sie `/etc/rsyslog.conf` Datei. Fügen Sie die Posten unter `###MODULES###` Abschnitt:

```
$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
```

**Anmerkung:** Sie können den Namen `ncs-server` für Ihr Verzeichnis verwenden.

In diesem Schritt werden die Regeln zum Speichern der Protokolle speziell für den NSO an einem festgelegten Standort definiert.

### Schritt 7: Starten Sie den rsyslog Dienst:

```
service rsyslog restart
```

**Anmerkung:** Die Schritte 5 bis 7 müssen auf dem Empfänger, dem Remote-Server, ausgeführt werden, auf dem die Protokolle gespeichert werden sollen.

## Zusätzliche Konfigurationen

Die Relay-Funktion des Syslog-Daemons muss wie folgt eingerichtet werden: In einer Produktionsumgebung sind jedoch normalerweise der Firewall-Service und SELinux aktiviert. Wenn sie aktiviert sind, werden die Protokolle nicht remote gespeichert. Um sicherzustellen, dass keine Probleme auftreten, müssen Sie die folgenden Konfigurationen auf beiden Servern hinzufügen:

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

## Verifizierung

Wenn die Schritte ordnungsgemäß durchgeführt wurden, `syslog` Server remote eingerichtet wird. So überprüfen Sie Folgendes:

Auf dem Remote-Server:

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

Vom Absender:

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

Der Remoteserver muss folgende Nachricht erhalten haben:

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

## Fehlerbehebung

In Fällen, in denen das Relay nicht erfolgreich ist, müssen Sie die Konfigurationsdateien erneut überprüfen.

Es ist auch nützlich, den Status des NSO zu bestätigen und `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 (running) 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 Logging Service Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled) Active: active (running) since Wed 2022-05-11 01:12:08 EDT; 21h ago ... No other lines in red in the status output.

Sie können nach Firewall-Regeln oder SELinux-Konfigurationen suchen. Diese können die Protokollübertragung an das Remote-Ziel blockieren.

1. `systemctl status firewalld.service`
2. `sestatus`

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.