Network Services Orchestrator 5.X口グのSyslogの設定

内容

概要

このドキュメントでは、Network Services Orchestrator(NSO)5.xのsyslogサーバを設定する方法について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

設定要件

インストールが完了したら、次のファイルが必要です。

- コンフィギュレーションファイルは /etc/rsyslog.conf を参照。
- 特定のコンフィギュレーションファイルで定義されたディレクトリは、 **/etc/rsyslog.d/**を参照。

この設定では、いくつかのLinuxディストリビューションでデフォルトで利用可能なrsyslogサービスを使用します。サーバで使用できない場合は、次の手順でダウンロードします (RHEL/CentOS)。

```
yum install rsyslog
```

NSO 5.1では、 ncs.conf 古いファイルに置き換えられます。

注：シスコのセキュリティ要件に準拠するため、UDP経由のsyslogのサポートは削除されました。デフォルト syslog 機能を提供します libc syslog(3) まだ利用できます。

NSOログをリモートサーバにリダイレクトするには、『NSO Syslog Relay Readme』ファイルを参照し、syslogデーモンリレー設定を使用してください。

コンフィギュレーション

設定には2つの設定ファイルのセットが必要です。1つはNSOが実行されているサーバ（この場合は送信側）、もう1つは、すべてのログを保存するレシーバ（リモートサーバ）にあります。

ステップ1：次のことを確認します。 ncs.conf ファイルには次のセクションがあります。

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

ステップ2:WLCで /etc/rsyslog.conf 次の手順に従います。

- 通常の #### RULES #### ; セクション追加：

```
*.* @remote_ip
```

例：

```
*.* @10.127.200.61
```

この行は、指定されたIPのリモートホストに「all」デーモンログをリダイレクトするように syslogサービスに指示します。

ステップ3：新しいファイルを /etc/rsyslog.d/ 次の例に示すようにパスを設定します。

- 新しいファイルは設定ファイルであり、このファイルを使ってrsyslog daemon どのファイルをネットワーク経由でリモートサーバーに送信するかについての詳細。

例：

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

- すべてのファイルを定義して詳細を含めた後、プロトコルを介してファイルを送信する場所を指定できます。

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

例：

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

ステップ4：ルータを rsyslog service：

```
service rsyslog restart
```

注：ステップ2 ~ 4は、送信側、つまりNSOサービスが稼働しているサーバで実行する必要があります。

ステップ5:UDP/TCPに関するセクションのコメントを、 /etc/rsyslog.conf DSN エントリの例：

<#root>

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

注:514は、この転送に使用されるポートです。

ステップ 6： 次の項目を変更します /etc/rsyslog.conf 出力を提供してください。下に行を追加します。 ###MODULES### セクション：

```
$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
```

注：ディレクトリにはncs-serverという名前を使用できます。

この手順では、NSO専用のログを指定された場所に保存するためのルールを定義します。

ステップ7：ルータを rsyslog service：

```
service rsyslog restart
```

注：ステップ5 ~ 7は、ログを保存する受信側のリモートサーバで実行する必要があります。

その他の設定

syslogデーモンリレー機能は、次の手順で設定する必要があります。ただし、実稼働環境では通常、ファイアウォールサービスとSELinuxが有効になっています。有効になっている場合、ログはリモートに保存されません。これが問題を引き起こさないようにするため、両方のサーバに次

の設定を追加する必要があります。

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

検証

手順に正しく従っている場合は、 syslog サーバはリモートでセットアップされます。これを確認するには、次のようにします。

リモートサーバで次のコマンドを実行します。

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

送信者から：

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

リモートサーバは次のメッセージを受信している必要があります。

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

トラブルシュート

リレーが成功しない状況では、設定ファイルをもう一度確認する必要があります。

また、NSOのステータスを確認し、 rsyslog：を入力します。

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.

ファイアウォールルールまたはSELinux設定を確認できます。これにより、リモート接続先へのログ転送がブロックされる場合があります。

1. systemctl status firewalld.service
2. sestatus

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。