配置网络服务协调器5.X日志的系统日志

目录

简介

本文档介绍如何为网络服务协调器(NSO)5.x配置系统日志服务器。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

配置要求

安装完成后，需要以下文件：

- 配置文件为 /etc/rsyslog.conf .
- 使用特定配置文件定义的目录为 **/etc/rsyslog.d/.**

对于此配置，请使用多个Linux发行版中默认提供的rsyslog服务。如果服务器上没有该功能，请按如下所示下载该功能(RHEL/CentOS):

```
yum install rsyslog
```

在NSO 5.1中，系统日志服务器元素是 ncs.conf 已过时文件。

注意：为符合思科安全要求，已取消通过UDP对系统日志的支持。默认值 syslog 功能通过 libc syslog(3) 仍然可用。

要将NSO日志重定向到远程服务器，请参阅NSO系统日志中继自述文件，并使用系统日志后台守护程序中继配置。

配置

配置需要两组配置文件。一个位于运行NSO的服务器上（本例中为发送方），另一个位于存储所有日志的接收方（远程服务器）上。

第1步：检查 ncs.conf 文件包含此部分：

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

第2步：配置 /etc/rsyslog.conf 如下所示：

- 低于 #### RULES #### ；部分添加：

```
*.* @remote_ip
```

例如：

```
*.* @10.127.200.61
```

此行指示rsyslog服务也将“所有”守护程序日志重定向到指定IP上的远程主机。

第3步：在中添加新文件 /etc/rsyslog.d/ 路径，如下一示例所示。

- 新文件是一个配置文件，用于告知rsyslog daemon 有关通过网络将哪些文件发送到远程服务器的详细信息。

例如：

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

- 定义所有文件并包含详细信息后，您可以指定通过协议发送文件的位置：

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

例如：

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

第4步：重新启动 rsyslog 服务：

```
service rsyslog restart
```

注意：必须在发送方（即NSO服务所在的服务器）上执行步骤2到步骤4。

第5步：根据您在UDP/TCP上的要求取消对UDP/TCP一节的注释 /etc/rsyslog.conf 文件:

<#root>

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

注意：514是此传输使用的端口。

步骤 6： 修改 /etc/rsyslog.conf 文件.在下面添加行 ###MODULES### 部分：

```
$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：您可以将名称ncs-server用于目录。

在此步骤中，定义规则以将日志专门存储到指定位置的NSO。

第7步：重新启动 rsyslog 服务：

```
service rsyslog restart
```

注：必须在接收方（即远程服务器）上执行步骤5到7，以便存储日志。

其他配置

必须按照以下步骤设置syslog守护程序中继功能。但是，在生产环境中，通常启用防火墙服务和SELinux。如果启用，则不会远程存储日志。为了确保这不会导致任何问题，您需要在两个服务器上添加以下配置：

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

确认

如果正确执行了步骤， syslog 远程设置服务器。要验证这一点，请执行以下操作：

在远程服务器上：

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

发件人：

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

远程服务器必须已收到以下消息：

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

故障排除

在中继不成功的情况下，您需要再次检查配置文件。

确认NSO和NSO的状态也非常有用 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.

您可以检查防火墙规则或SELinux配置。这些命令可以阻止日志传输到远程目标。

1. systemctl status firewalld.service
2. sestatus

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。