為網路服務協調器5.X日誌配置系統日誌

目錄

簡介

本檔案介紹如何為網路服務協調器(NSO)5.x設定系統日誌伺服器。

必要條件

需求

本文件沒有特定需求。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

配置要求

安裝完成後，需要以下檔案：

- 配置檔案為 /etc/rsyslog.conf .
- 使用特定配置檔案定義的目錄為 **/etc/rsyslog.d/.**

對於此配置，請使用多個Linux發行版中預設提供的rsyslog服務。如果伺服器上沒有該軟體，請按如下方式下載(RHEL/CentOS):

```
yum install rsyslog
```

在NSO 5.1中，系統日誌伺服器元素是 ncs.conf 已過時檔案。

註：為符合思科安全要求，已取消通過UDP對系統日誌的支援。預設值 syslog 功能通過 libc syslog(3) 仍然可用。

要將NSO日誌重定向到遠端伺服器，請參閱NSO系統日誌中繼自述檔案並使用syslog守護程式中繼配置。

組態

配置需要兩組配置檔案。一個位於運行NSO的伺服器上（本例中為傳送方），另一個位於儲存所有日誌的接收器（遠端伺服器）上。

第1步：檢查 ncs.conf 檔案中有以下區段：

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

第2步：配置 /etc/rsyslog.conf 如下所示：

- 在 #### RULES ####；節新增：

```
*.* @remote_ip
```

舉例來說：

```
*.* @10.127.200.61
```

此行指示rsyslog服務也將「所有」守護程式日誌重定向到指定IP上的遠端主機。

步驟3：在 /etc/rsyslog.d/ 路徑，如下例所示。

- 新檔案是一個配置檔案，用於告知rsyslog daemon 有關通過網路傳送到遠端伺服器的檔案的詳細資訊。

舉例來說：

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

- 定義所有檔案並包含詳細資訊後，您可以指定通過協定傳送檔案的位置：

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

舉例來說：

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

第4步：重新啟動 rsyslog 服務：

```
service rsyslog restart
```

注意：必須在傳送方（即NSO服務所在的伺服器）上執行步驟2到步驟4。

第5步：根據您在UDP/TCP中的要求取消對UDP/TCP一節的註釋 /etc/rsyslog.conf 檔案：

<#root>

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

註:514是此傳輸使用的埠。

步驟 6: 修改 /etc/rsyslog.conf 檔案。在下方新增行 ###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
```

註：您可以將名稱ncs-server用於目錄。

在此步驟中，定義規則以將日誌專門儲存到指定位置的NSO。

第7步：重新啟動 rsyslog 服務：

```
service rsyslog restart
```

註：必須在接收方（即要儲存日誌的遠端伺服器）上執行步驟5至7。

其他配置

必須按照以下步驟設定syslog守護程式中繼功能。但是，在生產環境中通常啟用防火牆服務和SELinux。如果啟用，則不會遠端儲存日誌。要確保這不會導致任何問題，您需要在兩個伺服器上新增以下配置：

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

驗證

如果步驟正確執行， syslog 伺服器是遠端設定的。要驗證這一點，請執行以下操作：

在遠端伺服器上：

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

發件人：

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

遠端伺服器必須已收到以下消息：

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

疑難排解

如果中繼不成功，則需要再次檢查配置檔案。

此外，還可用於確認NSO和NSO的狀態 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.

您可以檢查防火牆規則或SELinux配置。它們可以阻止日誌傳輸到遠端目標。

1. systemctl status firewalld.service
2. sestatus

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。