配置CSPC以將Syslog轉發到Syslog伺服器

目錄

簡介

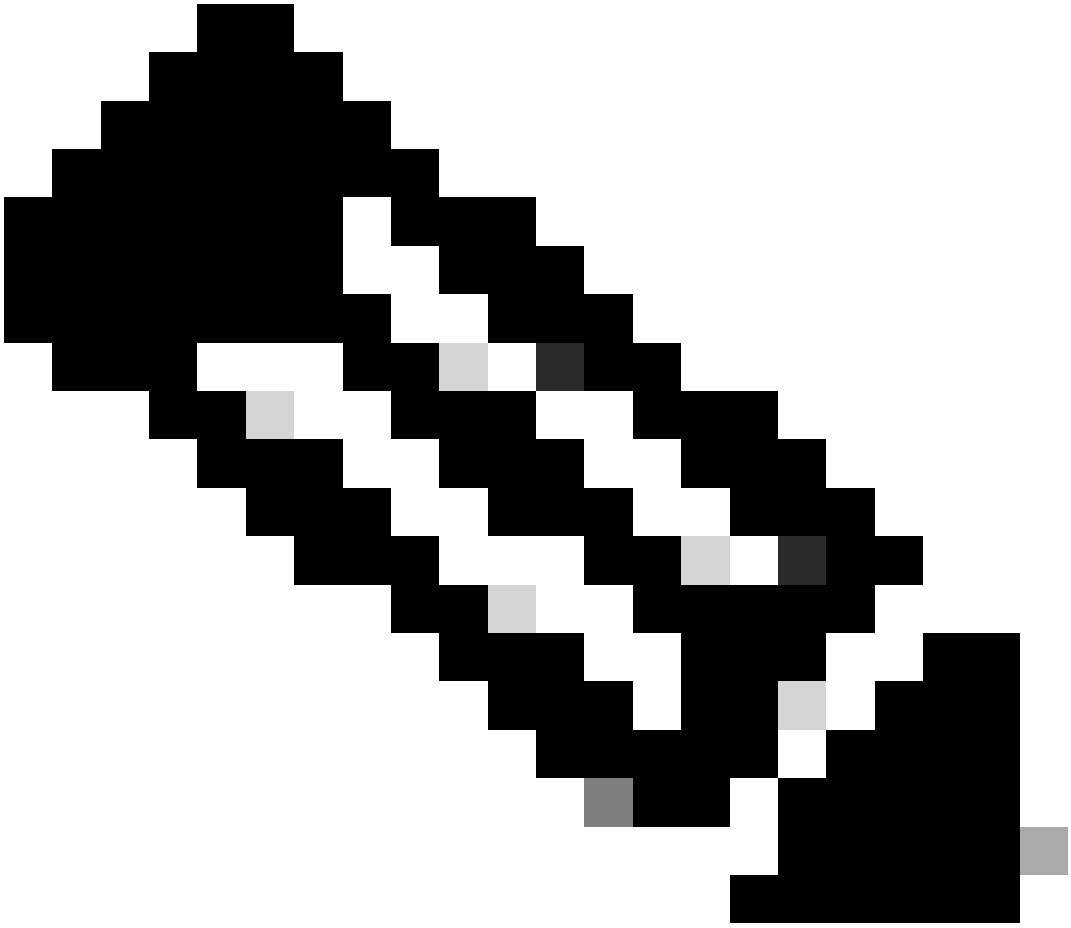
本文檔介紹如何配置CSPC以將系統日誌轉發到系統日誌伺服器。

問題

雖然BCS和NP支援系統日誌分析，但有些人已經有了其他解決方案，並且喜歡使用Splunk等系統日誌伺服器。但是在這種情況下，您要求CSPC將系統日誌從CSPC轉發到syslog伺服器。

解決方案

判斷需要使用的通訊協定(TCP/UDP)和IP/連線埠。預設埠為514。



註：必須可以從CSPC訪問Syslog伺服器。

使用rsyslog

1. 備份/etc/rsyslog.conf。

```
cp /etc/rsyslog.conf /etc/rsyslog.confbkup<date>
```

2. 增加轉發規則。

```
# ### begin forwarding rule ###
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
```

```
# Remote Logging (we use TCP for reliable delivery)
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$WorkDirectory /var/lib/rsyslog # where to place spool files
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
Add here
# ### end of the forwarding rule ###
```

2.1.例如TCP：

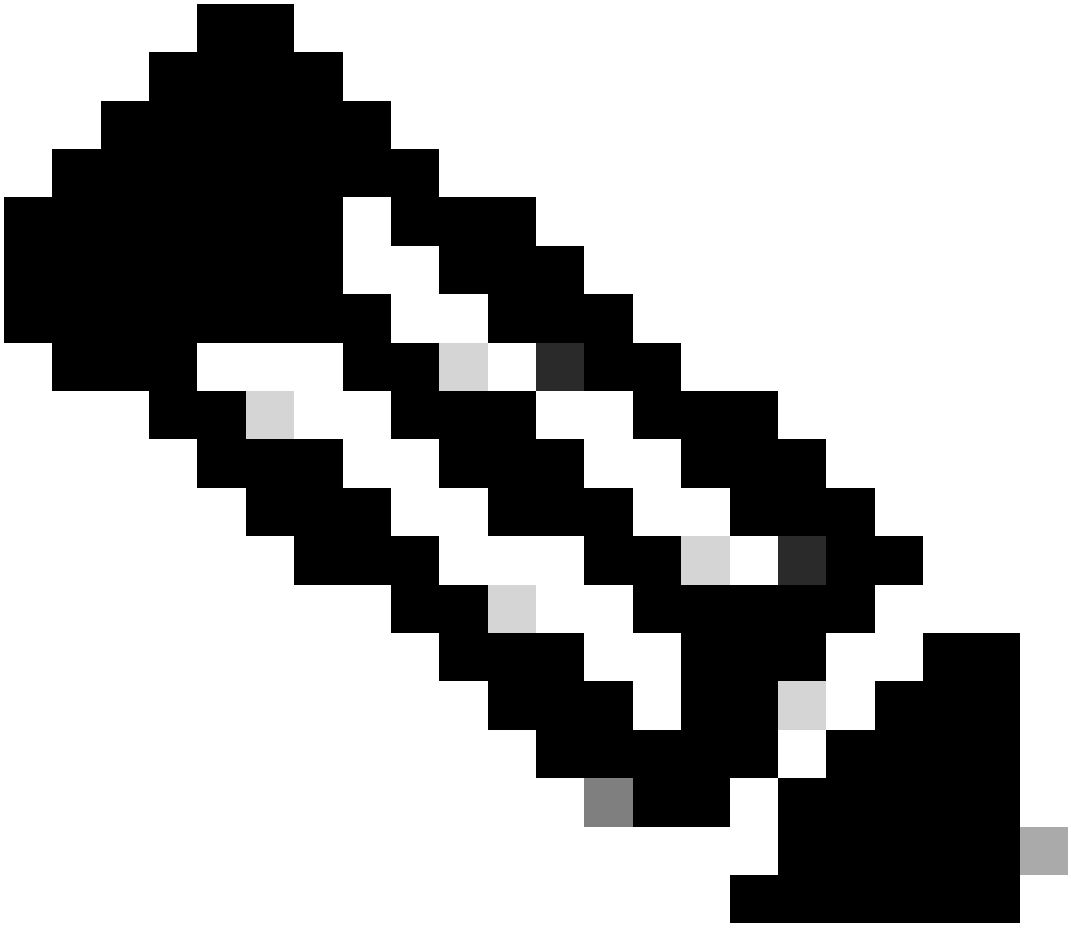
```
*.* @@138.25.253.132:514
```

2.2.例如UDP：

```
*.* @138.25.253.132:514
```

3. 重新啟動rsyslog。

```
service rsyslog restart
```



注意：如果配置錯誤的協定，則會顯示錯誤消息rsyslogd： cannot connect to ： ： Connection rejected ... 。如果發生此錯誤，請修改（請轉至步驟2.1和2.2）。

我們可利用下列專案產生用於測試的syslog：

```
logger "Your message for testing here"
```

4. 確認是否正在接收系統日誌。

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）。