SyslogをSyslogサーバに転送するためのCSPCの設定

内容

はじめに

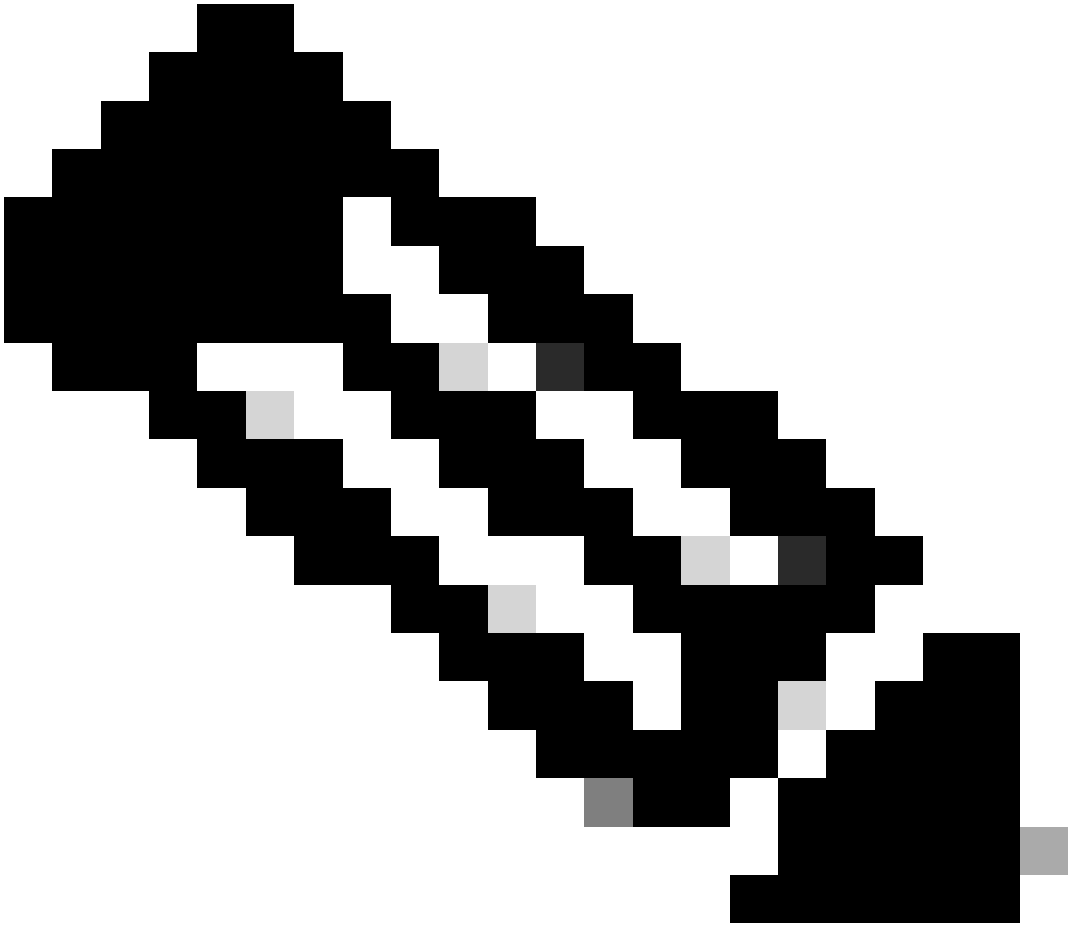
このドキュメントでは、syslogをsyslogサーバに転送するようにCSPCを設定する方法について説明します。

問題

BCSとNPはsyslog分析をサポートしますが、すでに別のソリューションを使用していて、Splunkのようなsyslogサーバを使用したいと考えている人もいます。ただし、この場合、CSPCがCSPCからsyslogサーバにsyslogを転送する必要があります。

解決方法

使用する必要があるプロトコル(TCP/UDP)とIP/ポートを決定します。デフォルトのポートは514です。



注:Syslogサーバには、CSPCから到達できる必要があります。

rsyslogの使用

1. /etc/rsyslog.confをバックアップします。

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

2. 転送ルールを追加します。

```
# ### 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. TCPの例：

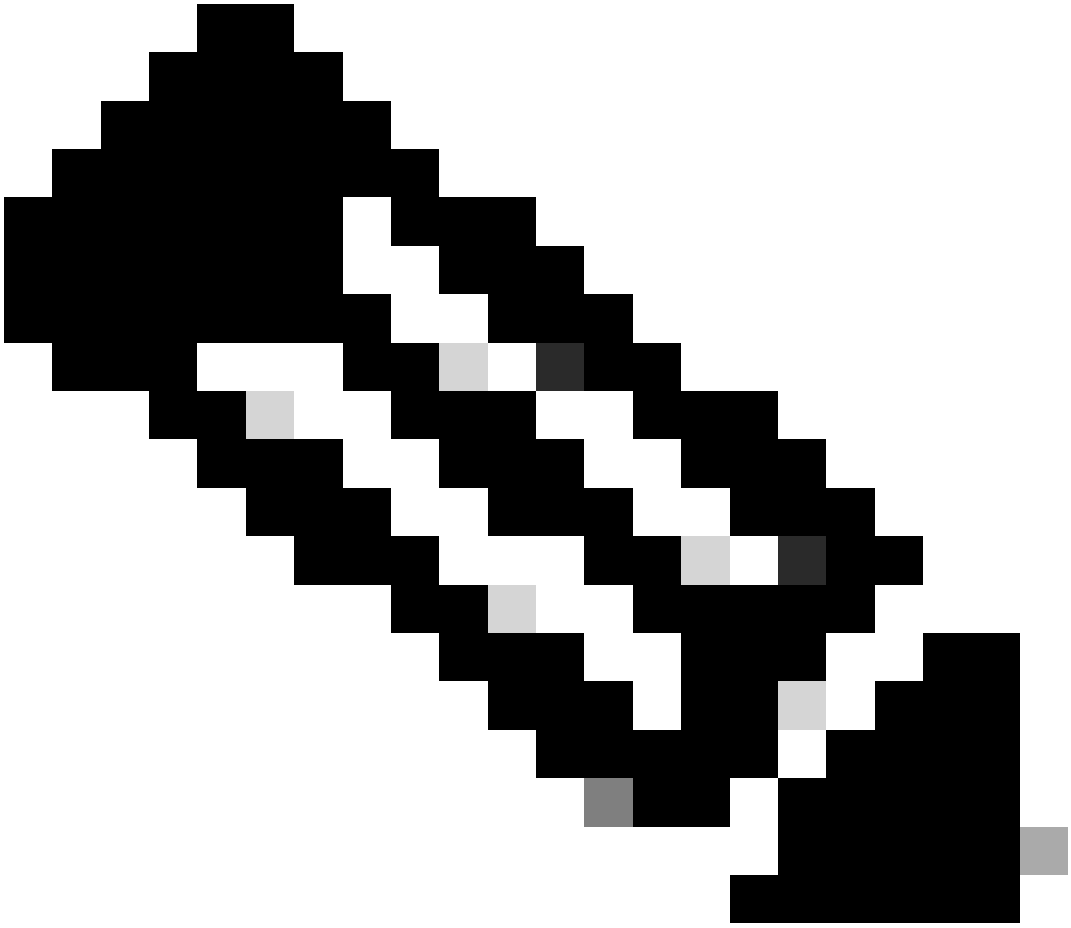
```
*.* @@138.25.253.132:514
```

2.2. UDPの例：

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

3. rsyslogを再起動します。

```
service rsyslog restart
```



注：誤ったプロトコルを設定すると、エラーメッセージrsyslogd: cannot connect to : : Connection refused ...が表示されます。このエラーが発生した場合は、変更します（ステップ2.1および2.2に進みます）。

テスト用にsyslogを生成するには、次のコマンドを使用します。

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

4. syslogが受信されているかどうかを確認します。

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。