Konfigurieren von CSPC zum Weiterleiten von Syslog an Syslog-Server

Inhalt

Einleitung

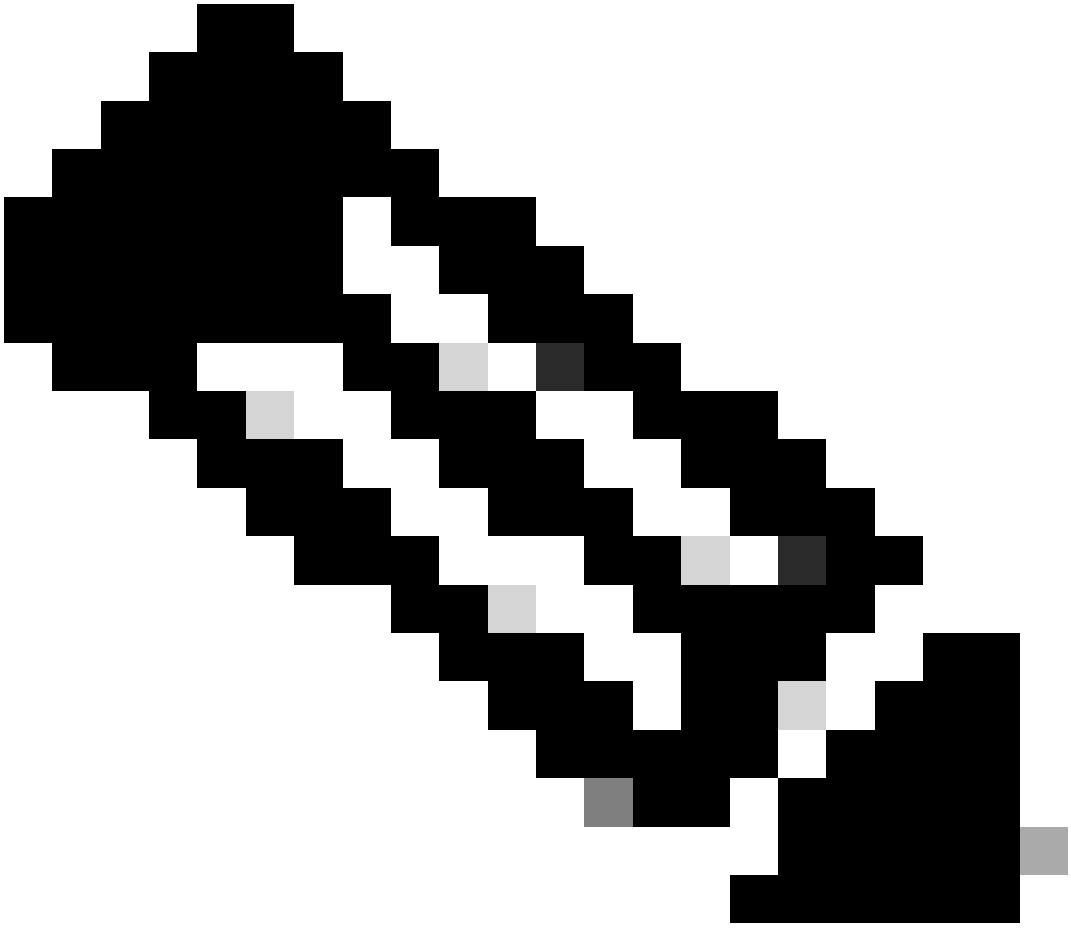
Dieses Dokument beschreibt die Konfiguration des CSPC für die Weiterleitung von Syslogs an einen Syslog-Server.

Problem

BCS und NP unterstützen zwar die Syslog-Analyse, einige Benutzer haben jedoch bereits eine andere Lösung und möchten einen Syslog-Server wie Splunk verwenden. In diesem Fall muss der CSPC die Syslogs jedoch vom CSPC an den Syslog-Server weiterleiten.

Lösung

Bestimmen Sie, welches Protokoll (TCP/UDP) und welche IP-Adresse/Port Sie verwenden müssen. Der Standard-Port ist 514.



Hinweis: Der Syslog-Server muss vom CSPC aus erreichbar sein.

Verwenden von rsyslog

1. Erstellen Sie ein Backup von /etc/rsyslog.conf.

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

2. Eine Weiterleitungsregel hinzufügen.

```
# ### 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. Beispiel für TCP:

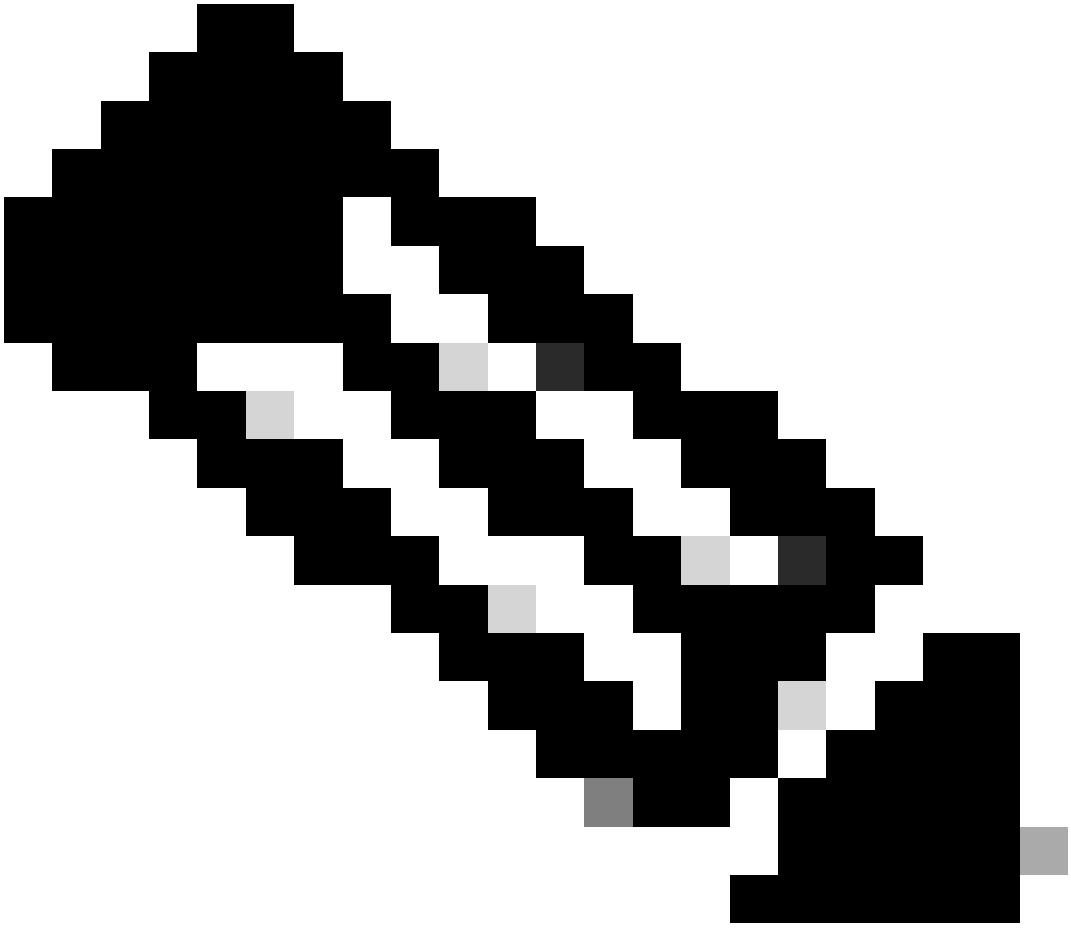
```
*.* @@138.25.253.132:514
```

2.2. Beispiel für UDP:

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

3. Starten Sie rsyslog neu.

```
service rsyslog restart
```



Hinweis: Wenn Sie das falsche Protokoll konfigurieren, wird eine Fehlermeldung angezeigt: rsyslogd: cannot connect to : : Connection rejected ... . Wenn dieser Fehler auftritt, ändern Sie ihn (gehen Sie zu den Schritten 2.1 und 2.2).

Wir können Syslogs zu Testzwecken generieren mit:

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

4. Bestätigen Sie, ob Syslogs empfangen werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.