CSPC configureren om Syslog door te sturen naar Syslog Server

Inhoud

Inleiding

Probleem

Oplossing

- Het gebruik van rsyslog

Inleiding

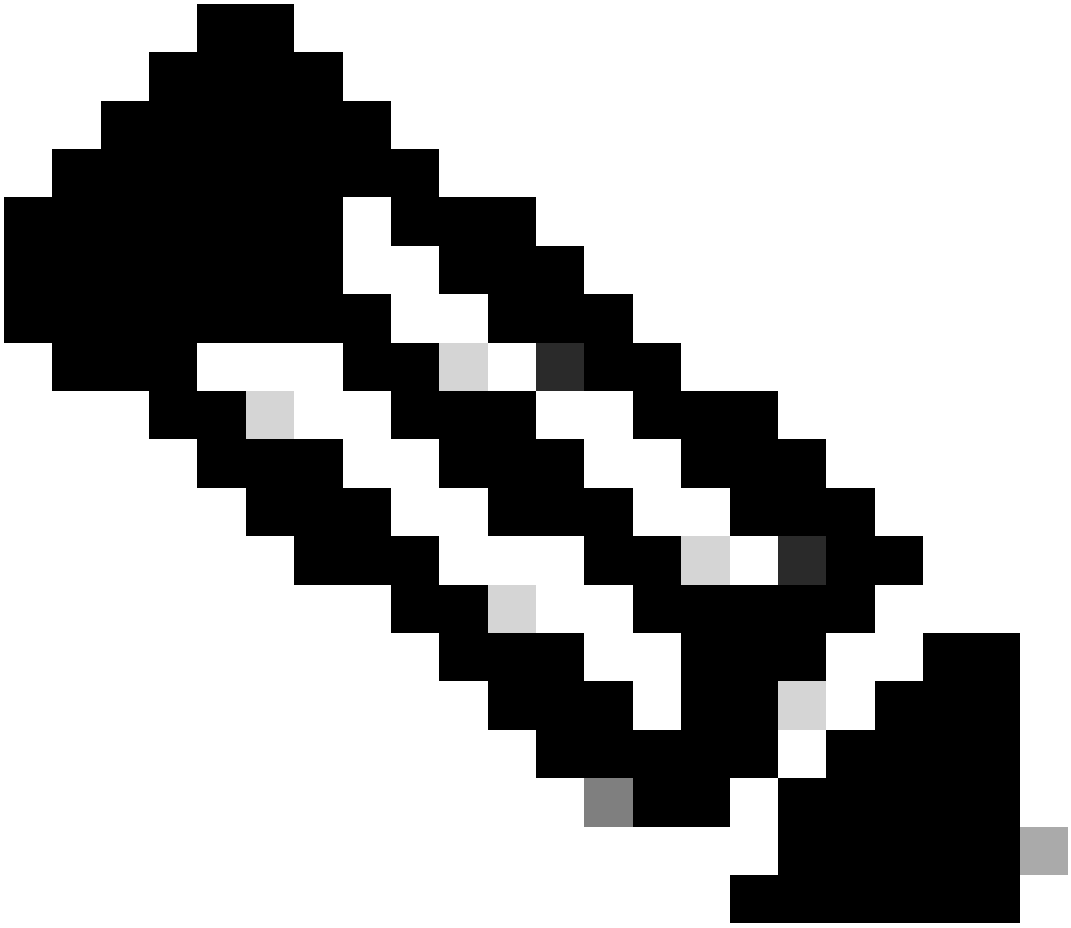
Dit document beschrijft hoe de CSPC moet worden geconfigureerd om syslogs naar een syslogserver te sturen.

Probleem

Hoewel de BCS en NP syslog analyse ondersteunen, hebben sommige mensen al een andere oplossing en willen ze graag een syslog server zoals Splunk gebruiken. Maar in dit geval, vereist u CSPC om de syslogs van CSPC aan de syslogserver door te sturen.

Oplossing

Bepaal welk protocol (TCP/UDP) en welke IP/poort u moet gebruiken. De standaardpoort is 514.



Opmerking: Syslog-server moet bereikbaar zijn vanuit de CSPC.

Het gebruik van rsyslog

1. Back-up /etc/rsyslog.conf.

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

2. Voeg een verzendregel toe.

```
# ### 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. Voorbeeld van TCP:

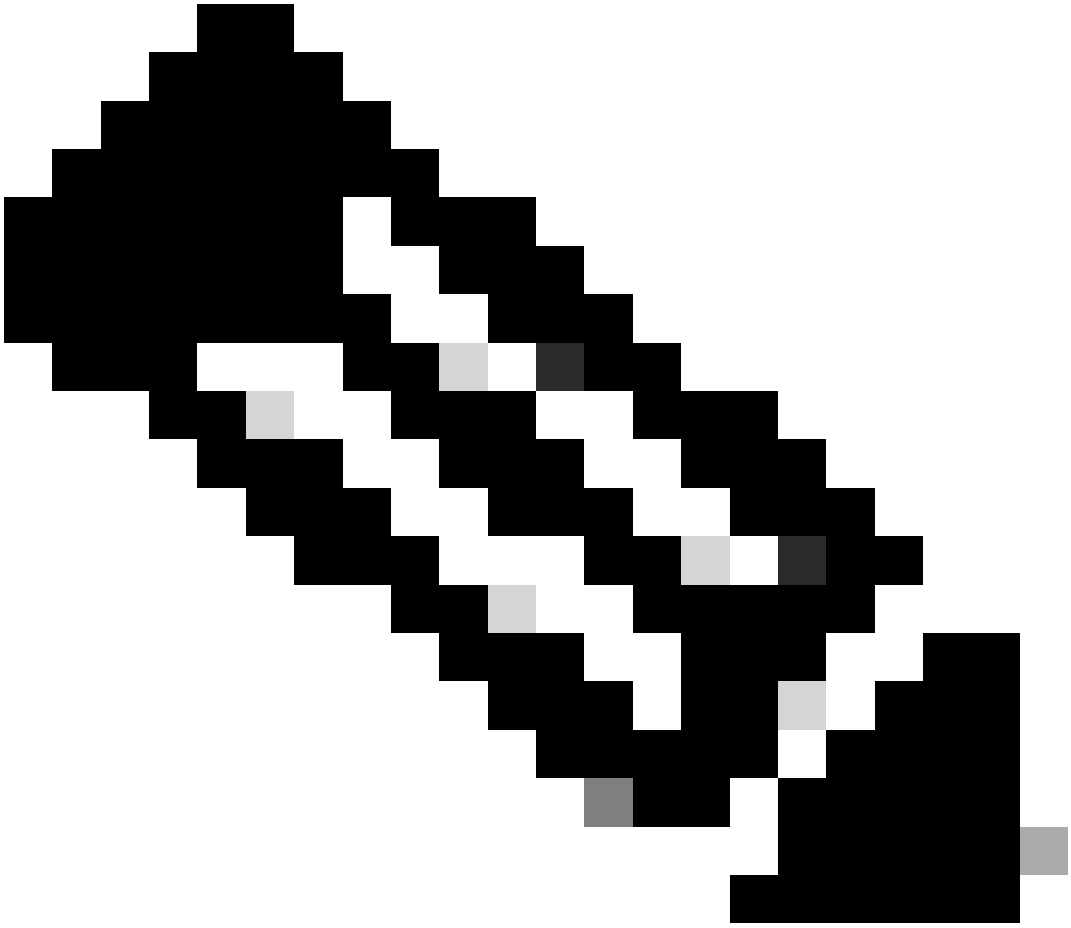
```
*.* @@138.25.253.132:514
```

2.2. Voorbeeld van UDP:

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

3. Start rsyslog opnieuw.

```
service rsyslog restart
```



Opmerking: Als u het verkeerde protocol configureert, verschijnt er een foutmelding rsyslogd: kan geen verbinding maken met: : Verbinding geweigerd ... . Als deze fout optreedt, wijzigt u (ga naar stap 2.1 en 2.2).

We kunnen systemen voor testdoeleinden genereren met:

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

4. Controleer of er syslogs worden ontvangen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.