Configuración de CSPC para reenviar Syslog al servidor Syslog

Contenido

Introducción

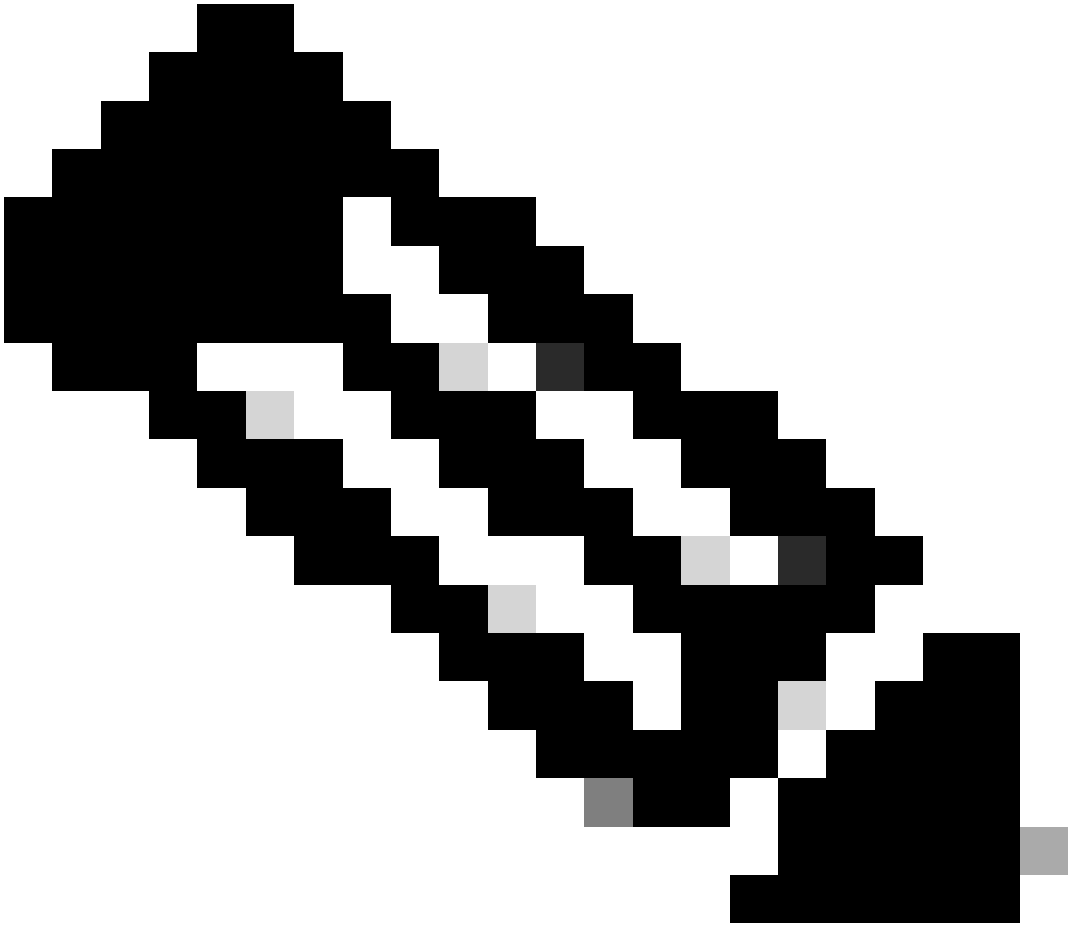
Este documento describe cómo configurar el CSPC para reenviar registros del sistema a un servidor syslog.

Problema

Aunque BCS y NP admiten el análisis de syslog, algunas personas ya tienen otra solución y les gusta utilizar un servidor de syslog como Splunk. Pero en este caso, usted requiere que el CSPC reenvíe los syslogs desde el CSPC al servidor syslog.

Solución

Determine qué protocolo (TCP/UDP) y qué IP/puerto debe utilizar. El puerto predeterminado es 514.



Nota: el servidor Syslog debe ser accesible desde el CSPC.

Uso de rsyslog

1. Haga una copia de seguridad de /etc/rsyslog.conf.

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

2. Agregue una regla de reenvío.

```
# ### 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. Ejemplo de TCP:

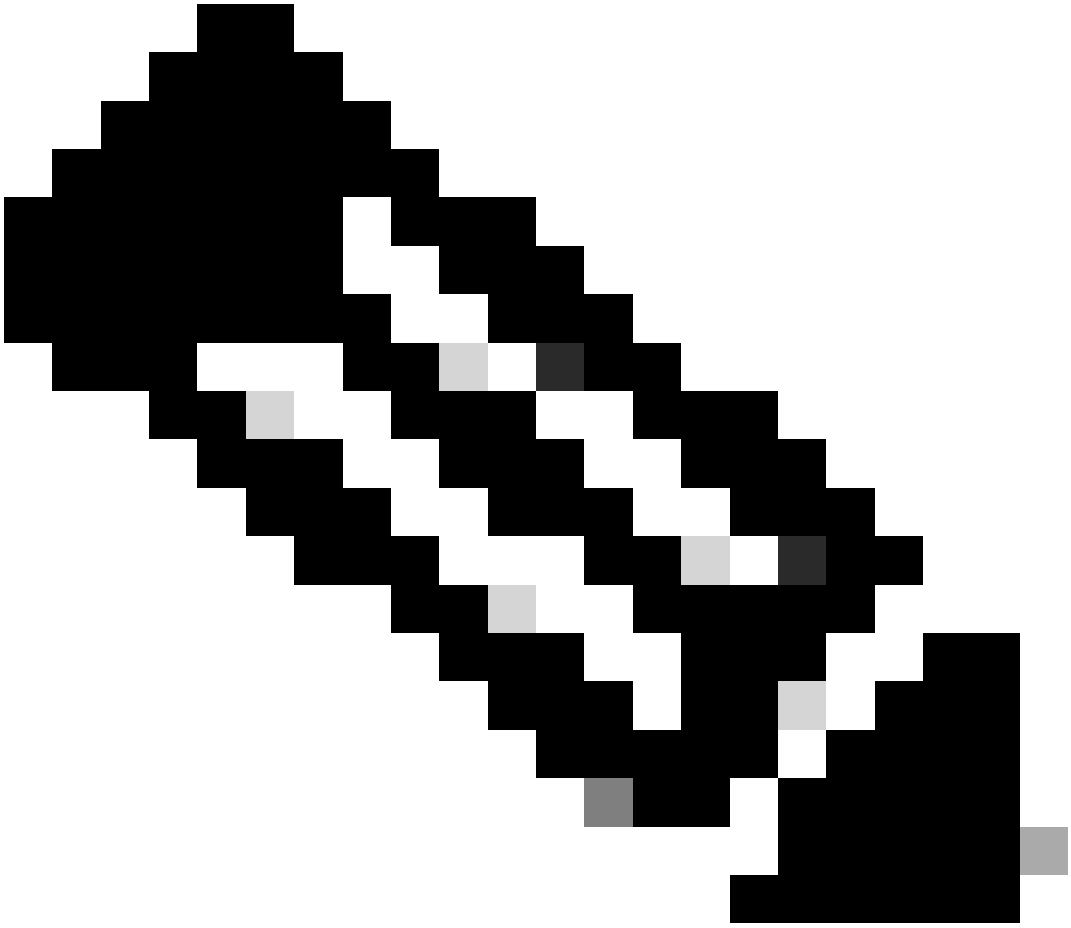
```
*.* @@138.25.253.132:514
```

2.2. Ejemplo de UDP:

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

3. Reinicie rsyslog.

```
service rsyslog restart
```



Nota: Si configura el protocolo incorrecto, aparece un mensaje de error rsyslogd: cannot connect to : Connection denied ... . Si se produce este error, modifíquelo (vaya a los pasos 2.1 y 2.2).

Podemos generar registros del sistema con fines de prueba con:

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

4. Confirme si se están recibiendo registros del sistema.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).