配置CSPC将系统日志转发到系统日志服务器

目录

简介

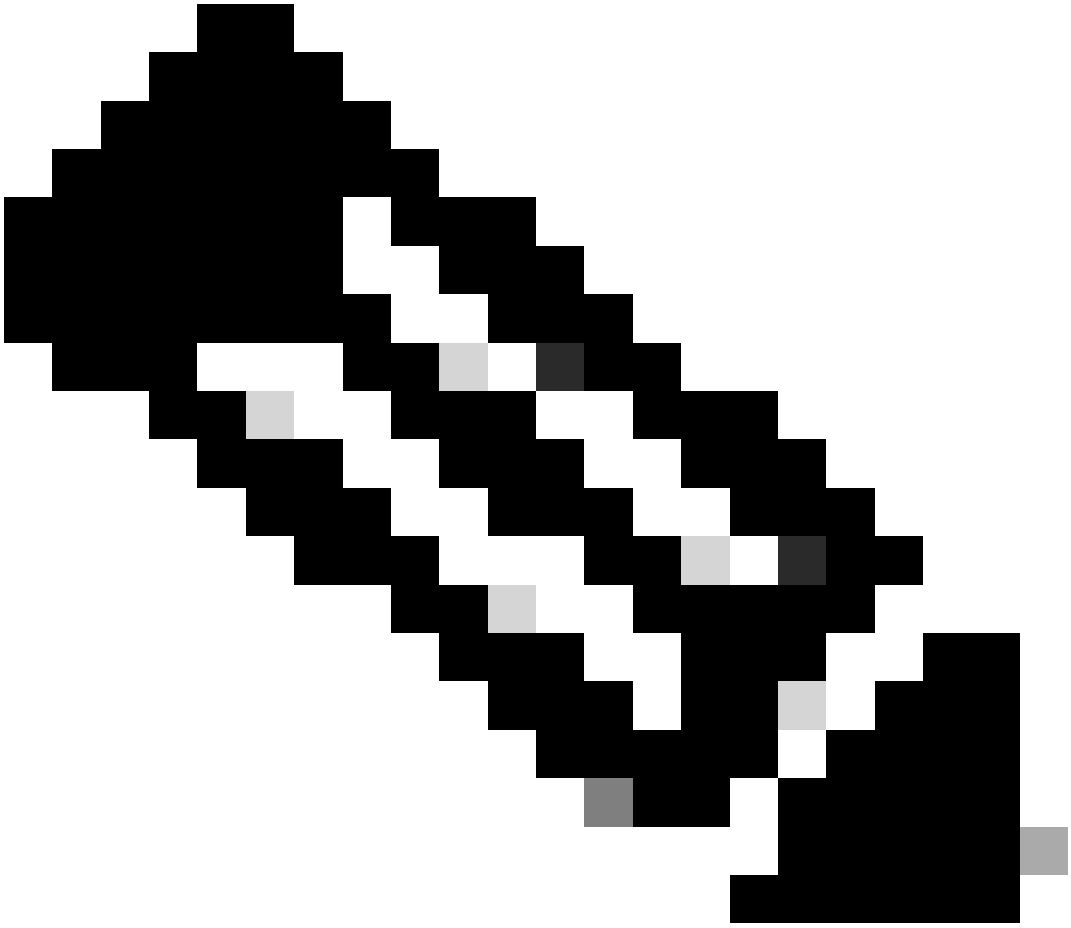
本文档介绍如何配置CSPC以将系统日志转发到系统日志服务器。

问题

虽然BCS和NP支持系统日志分析，但有些人已经有其他解决方案，并且喜欢使用Splunk等系统日志服务器。但是，在这种情况下，您需要CSPC将系统日志从CSPC转发到系统日志服务器。

解决方案

确定需要使用的协议(TCP/UDP)和IP/端口。默认端口为514。



注意：必须可以从CSPC访问系统日志服务器。

使用rsyslog

1. 备份/etc/rsyslog.conf。

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

2. 添加转发规则。

```
# ### 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示例：

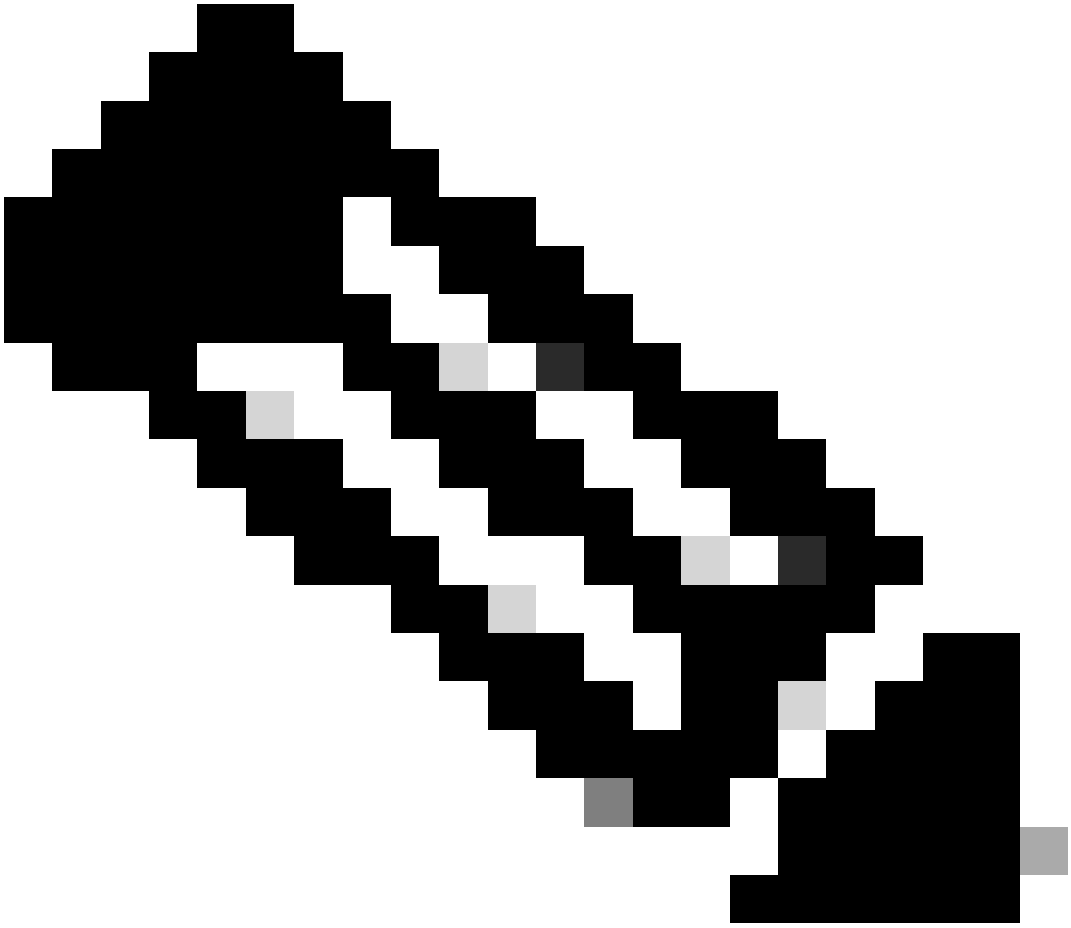
```
*.* @@138.25.253.132:514
```

2.2. UDP示例：

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

3. 重新启动rsyslog。

```
service rsyslog restart
```



注意：如果配置错误的协议，则会显示错误消息rsyslogd： cannot connect to ： ： Connection refused ... 。如果发生此错误，请进行修改（转到步骤2.1和2.2）。

我们可以通过以下方式生成用于测试的系统日志：

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

4. 确认是否正在接收系统日志。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。