Syslog 서버에 Syslog를 전달하도록 CSPC 구성

목차

소개

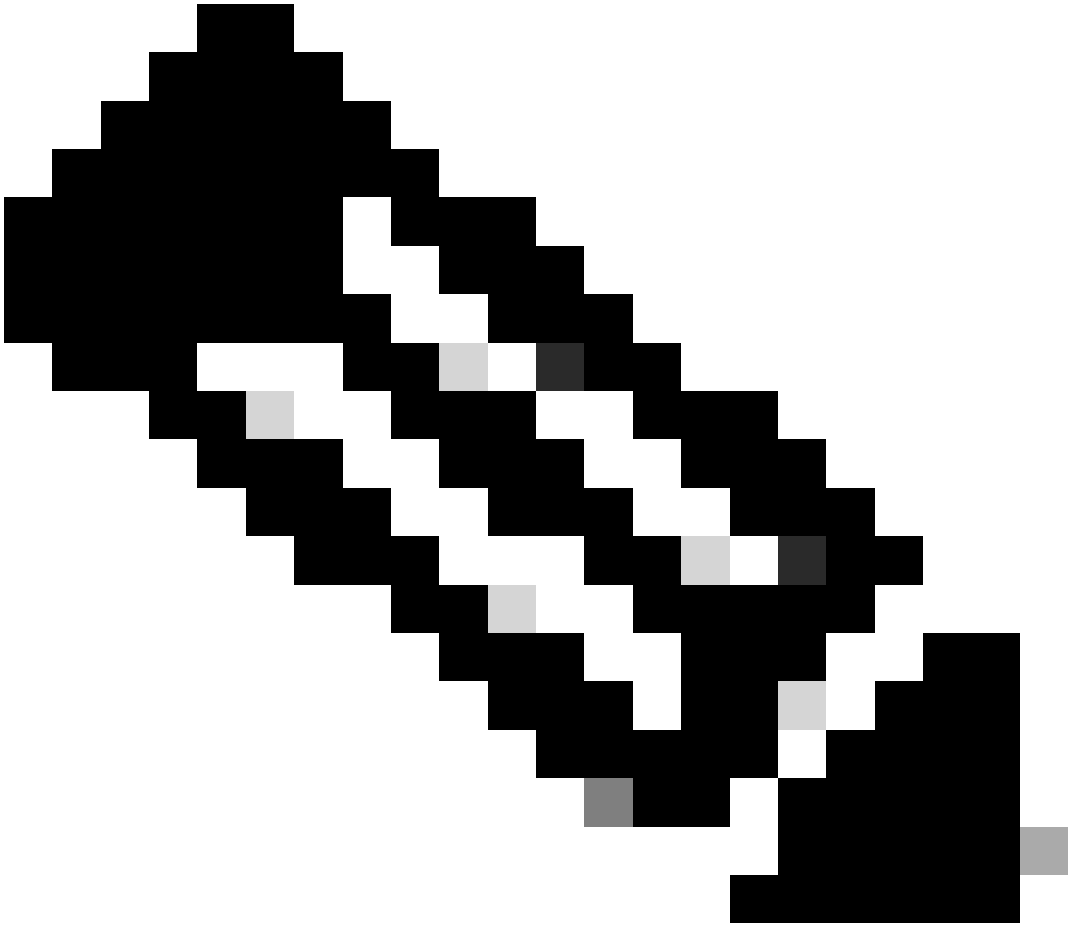
이 문서에서는 syslog를 syslog 서버에 전달하도록 CSPC를 구성하는 방법에 대해 설명합니다.

문제

BCS 및 NP는 syslog 분석을 지원하지만, 이미 다른 솔루션을 보유하고 있으며 Splunk와 같은 syslog 서버를 사용하는 경우도 있습니다. 그러나 이 경우 CSPC에서 syslog를 CSPC에서 syslog 서버로 전달해야 합니다.

솔루션

사용해야 할 프로토콜(TCP/UDP) 및 IP/포트를 결정합니다. 기본 포트는 514입니다.



참고: CSPC에서 Syslog 서버에 연결할 수 있어야 합니다.

rsyslog 사용

1. /etc/rsyslog.conf을 백업합니다.

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

2. 전달 규칙을 추가합니다.

```
# ### 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. TCP의 예:

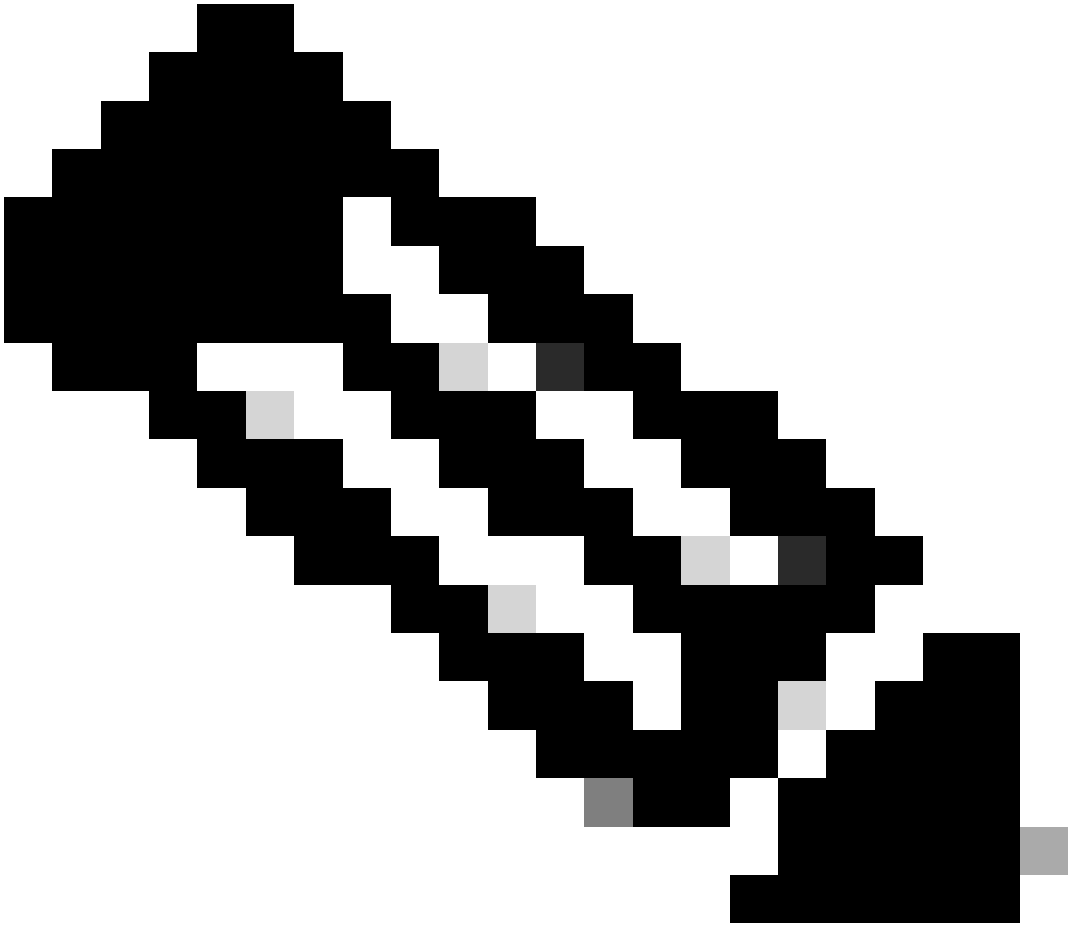
```
*.* @@138.25.253.132:514
```

2.2. UDP 예:

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

3. rsyslog를 다시 시작합니다.

```
service rsyslog restart
```



참고: 잘못된 프로토콜을 구성하면 rsyslogd: cannot connect to : : : Connection refused ... . 이 오류가 발생하면 수정합니다(단계 2.1 및 2.2로 이동).

테스트 목적으로 다음을 사용하여 syslog를 생성할 수 있습니다.

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

4. syslog를 수신하는지 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.