Configurar o CSPC para encaminhar o Syslog ao Servidor Syslog

Contents

Introdução

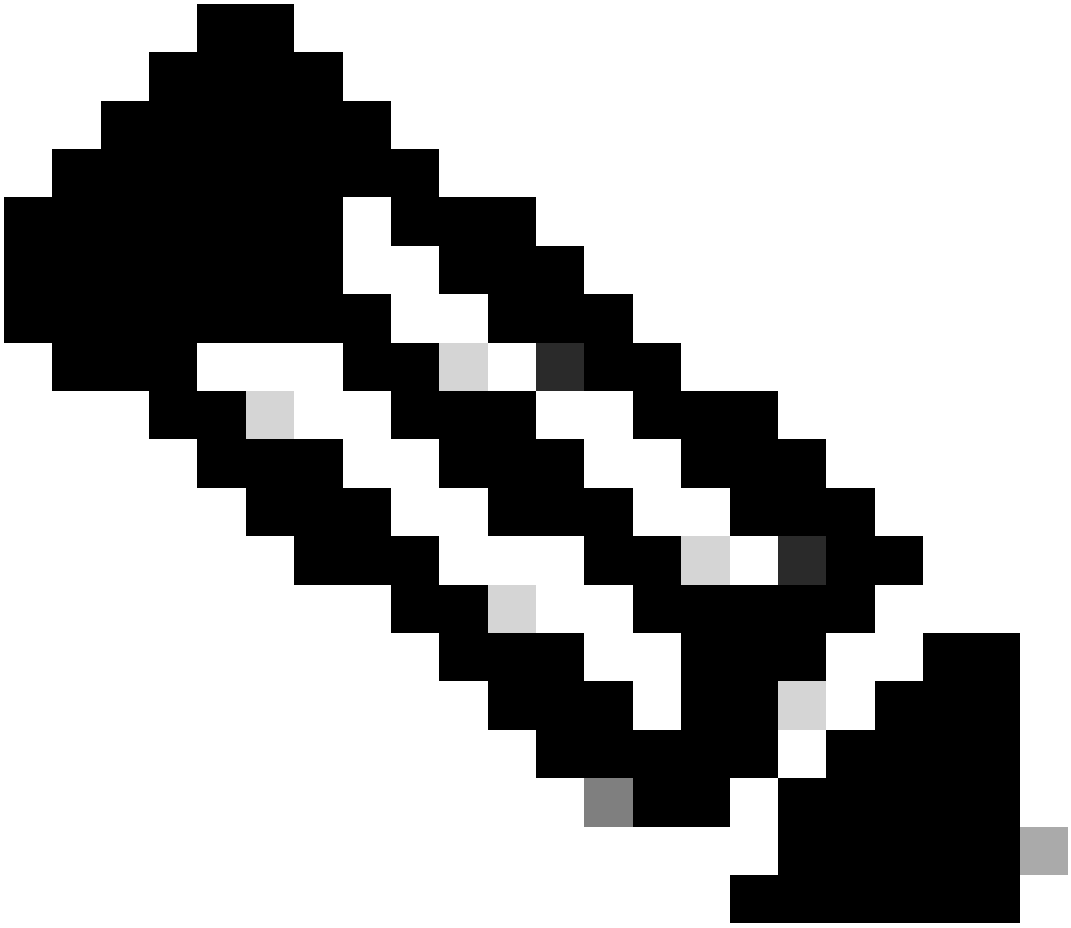
Este documento descreve como configurar o CSPC para encaminhar syslogs a um Servidor syslog.

Problema

Embora o BCS e o NP suportem a análise de syslog, algumas pessoas já têm outra solução e gostam de usar um servidor de syslog como o Splunk. Mas, nesse caso, você exige que o CSPC encaminhe os syslogs do CSPC para o servidor syslog.

Solução

Determine que protocolo (TCP/UDP) e que IP/porta você precisa usar. A porta padrão é 514.



Observação: o Servidor syslog deve estar acessível no CSPC.

Usando o rsyslog

1. Faça backup de /etc/rsyslog.conf.

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

2. Adicione uma regra de encaminhamento.

```
# ### 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. Exemplo de TCP:

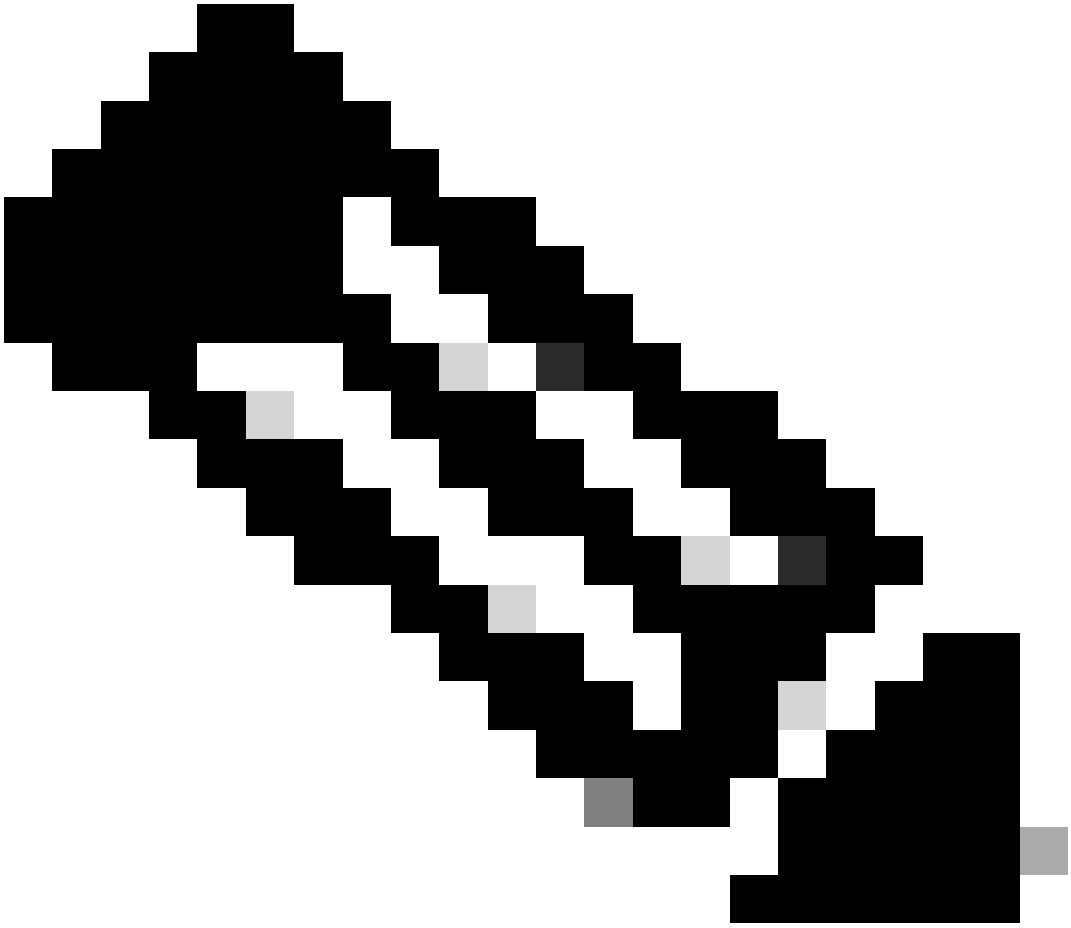
```
*.* @@138.25.253.132:514
```

2.2. Exemplo para o UDP:

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

3. Reinicie o rsyslog.

```
service rsyslog restart
```



Observação: se você configurar o protocolo errado, uma mensagem de erro será exibida rsyslogd: cannot connect to : : Connection rejected ... . Se esse erro ocorrer, modifique (vá para as etapas 2.1 e 2.2).

Podemos gerar syslogs para fins de teste com:

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

4. Confirme se os syslogs estão sendo recebidos.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.