Configurazione di CSPC per l'inoltro del syslog al server syslog

Sommario

Introduzione

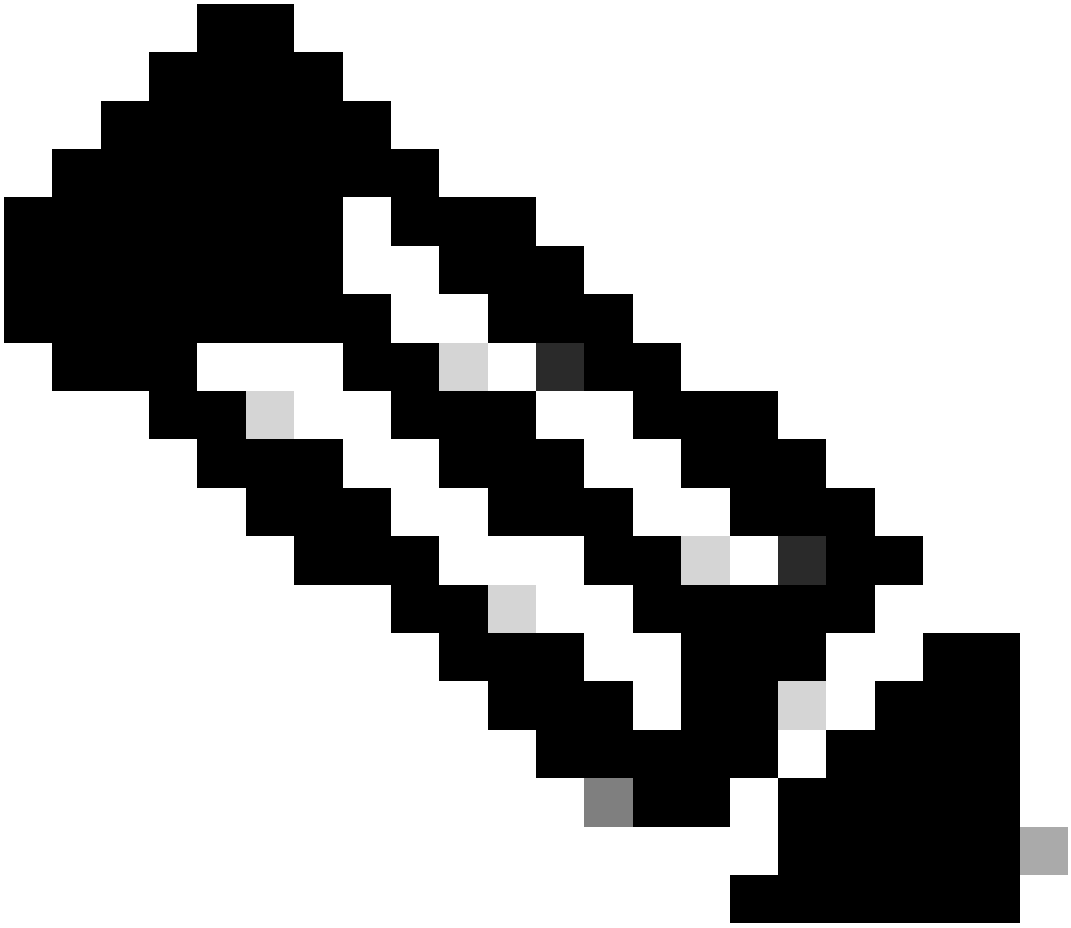
In questo documento viene descritto come configurare CSPC per l'inoltro dei syslog a un server syslog.

Problema

Sebbene BCS e NP supportino l'analisi syslog, alcuni utenti dispongono già di un'altra soluzione e preferiscono utilizzare un server syslog come Splunk. Tuttavia, in questo caso è necessario che il CSPC inoltri i syslog da CSPC al server syslog.

Soluzione

Determinare il protocollo (TCP/UDP) e la porta/IP da utilizzare. La porta predefinita è 514.



Nota: Il server Syslog deve essere raggiungibile dal CSPC.

Uso di rsyslog

1. Eseguire il backup di /etc/rsyslog.conf.

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

2. Aggiungere una regola di inoltro.

```
# ### 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. Esempio di TCP:

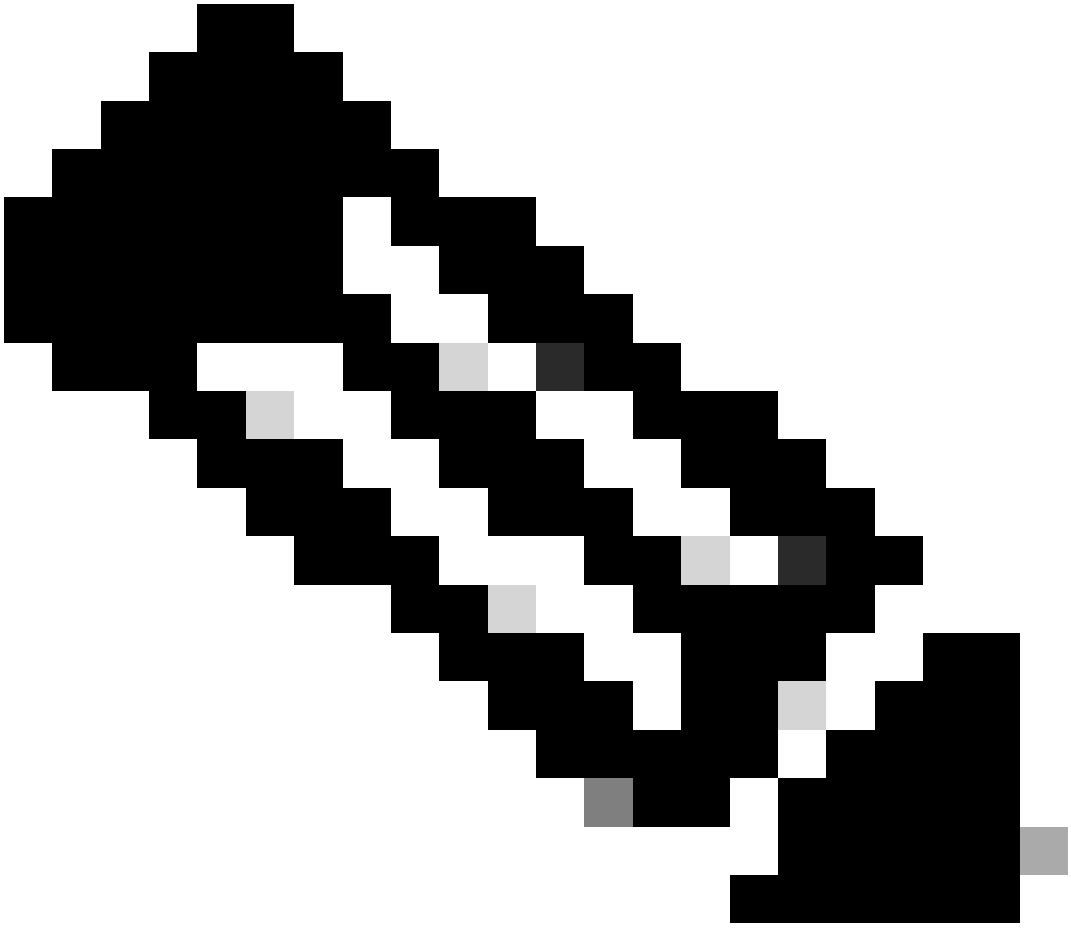
```
*.* @@138.25.253.132:514
```

2.2. Esempio di UDP:

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

3. Riavviare rsyslog.

```
service rsyslog restart
```



Nota: Se si configura il protocollo errato, viene visualizzato un messaggio di errore rsyslogd: impossibile connettersi a: : Connessione rifiutata... . Se si verifica questo errore, modificare (andare ai punti 2.1 e 2.2).

Possiamo generare syslog a scopo di test con:

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

4. Verificare che i syslog siano stati ricevuti.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).