Configurer CSPC pour transférer Syslog vers le serveur Syslog

Table des matières

Introduction

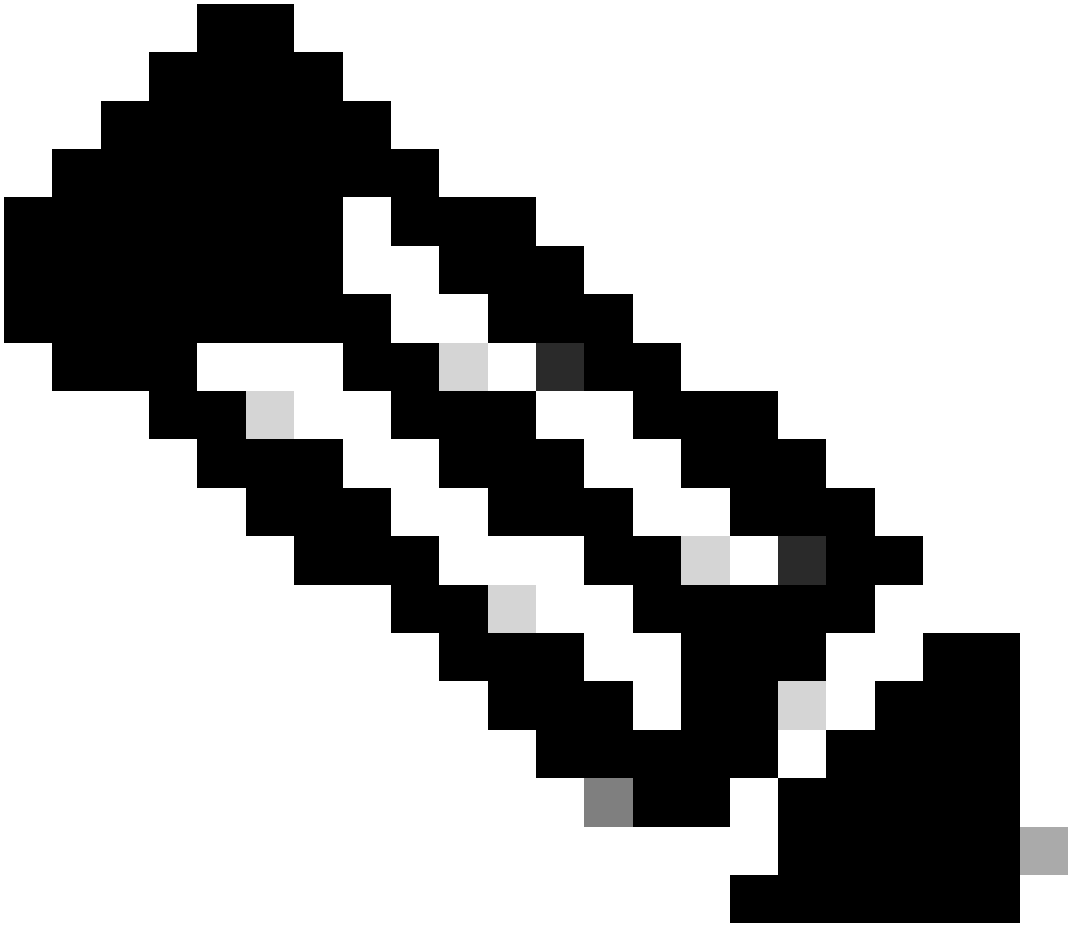
Ce document décrit comment configurer le CSPC pour transférer les syslogs à un serveur syslog.

Problème

Bien que le BCS et le NP prennent en charge l'analyse syslog, certaines personnes disposent déjà d'une autre solution et aiment utiliser un serveur syslog comme Splunk. Mais dans ce cas, vous exigez que le CSPC transfère les syslogs du CSPC au serveur syslog.

Solution

Déterminez le protocole (TCP/UDP) et le port IP/IP que vous devez utiliser. Le port par défaut est 514.



Remarque : Le serveur Syslog doit être accessible à partir du CSPC.

Utilisation de rsyslog

1. Sauvegardez /etc/rsyslog.conf.

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

2. Ajoutez une règle de transfert.

```
# ### 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. Exemple pour TCP :

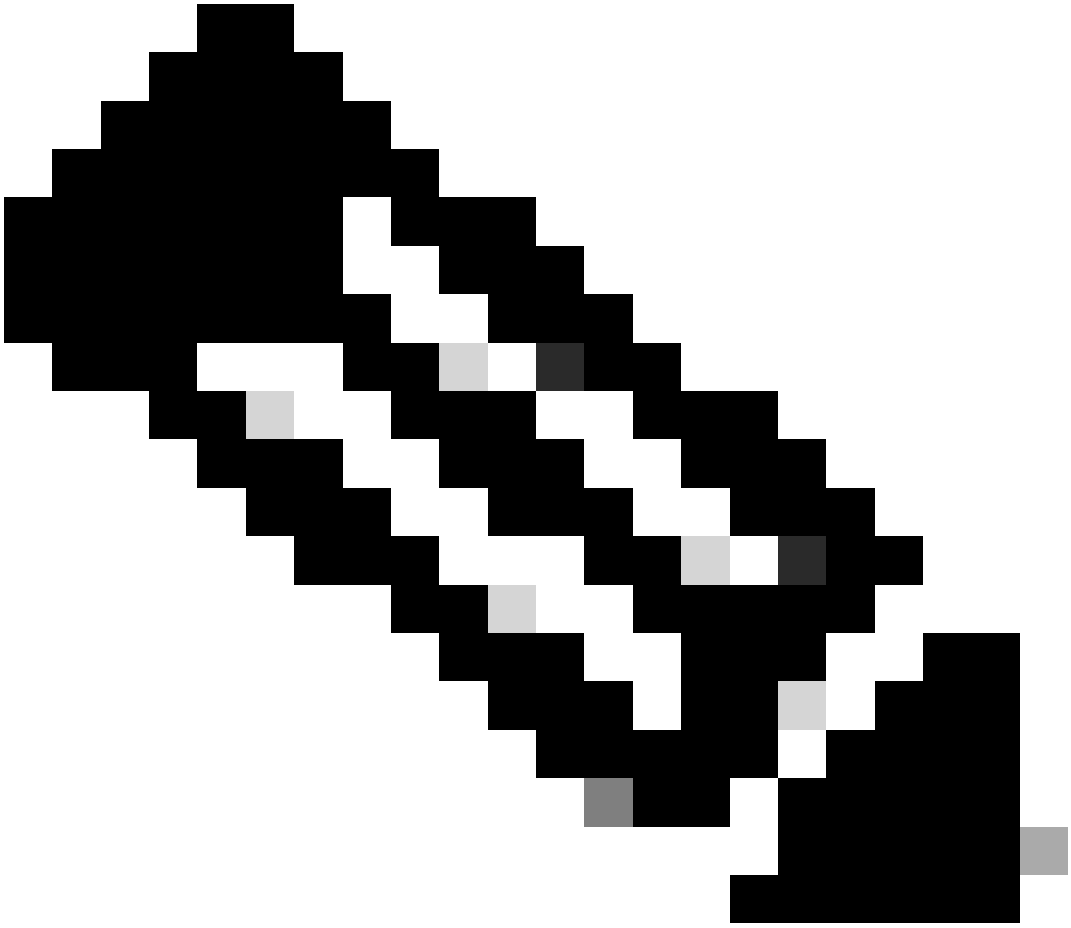
```
*.* @@138.25.253.132:514
```

2.2. Exemple de protocole UDP :

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

3. Redémarrez rsyslog.

```
service rsyslog restart
```



Remarque : Si vous configurez le mauvais protocole, un message d'erreur apparaît rsyslogd: impossible de se connecter à : : Connexion refusée... . Si cette erreur se produit, modifiez (passez aux étapes 2.1 et 2.2).

Nous pouvons générer des syslogs à des fins de test avec :

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

4. Vérifiez si des syslogs sont reçus.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.