تكوين CSPC لإعادة توجيه Syslog إلى خادم Syslog

المحتويات

المقدمة

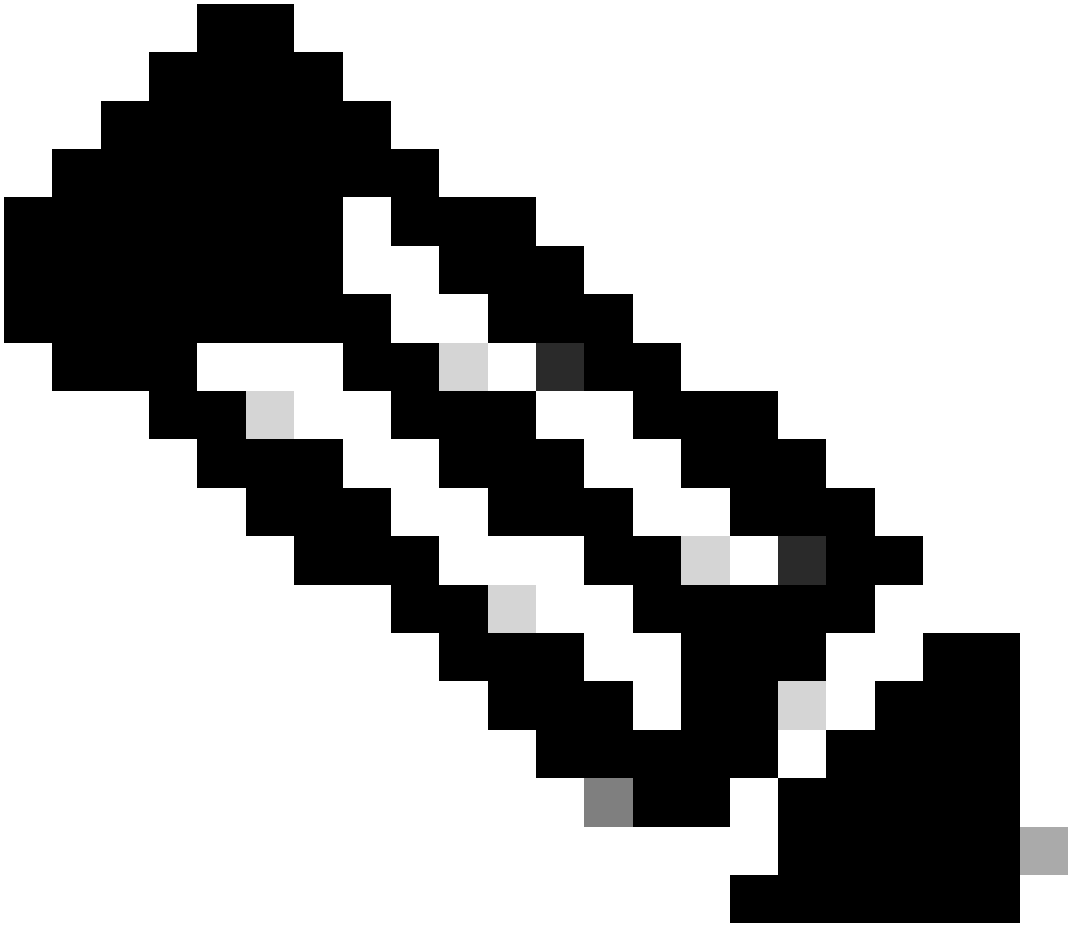
يصف هذه الوثيقة كيفية أن يشكل CSPC أن يرسل syslog إلى syslog نادل.

المشكلة

على الرغم من تحليل الدخول إلى النظام (BCS) و NP، إلا أن بعض الأشخاص لديهم حل آخر ويحبون إستخدام خادم syslog مثل Splunk. غير أن في هذه الحالة، يتطلب أنت ال CSPC أن يرسل ال syslogs من CSPC إلى ال syslog نادل.

الحل

حدد أي بروتوكول (TCP/UDP) وأي بروتوكول/منفذ تحتاج إلى إستخدامه. المنفذ البديل هو 514.



ملاحظة: يجب أن يكون خادم syslog قابل للوصول إليه من CSPC.

إستخدام rsyslog

1. النسخ الاحتياطي على /etc/rsyslog.conf.

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

2. أضف قاعدة إعادة توجيه.

```
# ### 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. مثال على بروتوكول TCP:

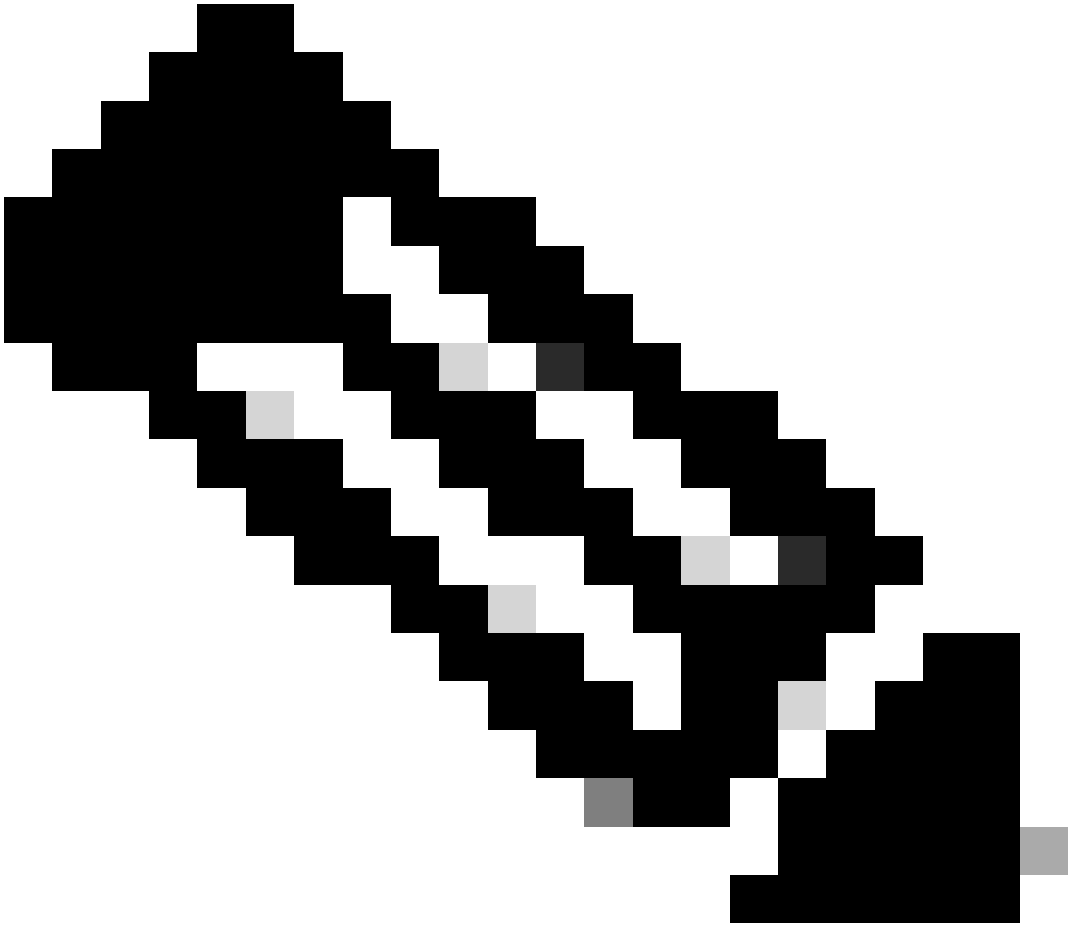
```
*.* @@138.25.253.132:514
```

2.2. مثال ل UDP:

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

3. قم بإعادة تشغيل rsyslog.

```
service rsyslog restart
```



ملاحظة: إذا قمت بتكوين البروتوكول الخطأ، تظهر رسالة خطأ في الوضع: لا يمكن الاتصال ب : تم رفض الاتصال ... . إذا حدث هذا الخطأ، فقم بالتعديل (انتقل إلى الخطوات 2.1 و 2.2).

يمكنك إنشاء syslog لأغراض الاختبار باستخدام:

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

4. تأكد مما إذا كانت تتم تلقي syslogs.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).