Por que há uns erros de rede quando o ESA se comunica com o servidor de SYSLOG?

Índice

Introdução

Este documento descreve porque a ferramenta de segurança do email (ESA) é incapaz de enviar dados a um servidor de SYSLOG.

Por que há uns erros de rede quando o ESA se comunica com o servidor de SYSLOG?

O ESA foi configurado para empurrar assinaturas do log para um servidor de SYSLOG. **Os arquivos puderam ou não puderam com sucesso ser empurrados para o servidor de SYSLOG.** Em todo caso, pode haver uns erros de rede no arquivo de registro do correio similar a este:

```
Log Error: Subscription Mail_Log: Network error while sending log data
to syslog server
```

Uma captura de pacote de informação entre o ESA e o servidor de SYSLOG mostra as gotas da conexão iniciadas pelo servidor de SYSLOG, que neste exemplo é 10.44.167.30.

Se você segue o córrego TCP na captura de pacote de informação você verá este:

```
<22>Jun 25 08:50:03 example.com: Info: Begin Logfile
<22>Jun 25 08:50:03 example.com: Info: Version: 8.0.1-023 SN: A4BADB4712A9-511AA1E
<22>Jun 25 08:50:03 example.com: Info: Time offset from UTC: 7200 seconds
<22>Jun 25 08:50:03 example.com: Info: A System/Critical alert was sent to
alerts@ironport.com with subject "Critical <System> mail.example.com: Log Error:
Subscription Mail_Log: Network error while sending l...".
```

Os erros indicam que há um Firewall ou Intrusion Prevention System (IPS) que obstrua o acesso ao servidor de SYSLOG no endereço IP de Um ou Mais Servidores Cisco ICM NT. Se todos os dispositivos in-between têm sido examinados e confirmados a fim permitir o tráfego, a seguir este poderia igualmente significar que o servidor de SYSLOG é demasiado ocupado e recusou as conexões. Quando o ESA é configurado para enviar um arquivo de registro a um servidor de SYSLOG, a seguir à revelia usará a porta de SYSLOG 514 UDP a menos que configurado para usar o TCP. Uma vez que o dispositivo é configurado, a única coisa que faz com que a conexão seja alistada como recusado é se recebe os pacotes que fecham a conexão quando são abertos.