ESA與syslog伺服器通訊時為什麼會出現網路錯誤？

目錄

簡介

本文檔說明為什麼郵件安全裝置(ESA)無法將資料傳送到系統日誌伺服器。

ESA與syslog伺服器通訊時為什麼會出現網路錯誤？

ESA已配置為將日誌訂閱推送到系統日誌伺服器。**檔案可能成功推送到syslog伺服器，也可能未成功推送到。**在任何情況下，郵件日誌檔案中都可能存在類似以下所示的網路錯誤：

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

ESA和syslog伺服器之間的資料包捕獲顯示syslog伺服器發起的連線丟棄，在本例中為10.44.167.30。

o.	Time	Source	Destination	Protocol	Info
278	2015-06-25 08:50:04.111689	10.229.24.230	10.44.167.30	TCP	26040 > shell [SYN] Seq=0 Win=16384 Len=0 MSS=1460 WS=8 SACK_P
279	2015-06-25 08:50:04.114360	10.44.167.30	10.229.24.230	TCP	shell > 26040 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1350
280	2015-06-25 08:50:04.114375	10.229.24.230	10.44.167.30	TCP	26040 > shell [ACK] Seq=1 Ack=1 Win=17550 Len=0
281	2015-06-25 08:50:04.114518	10.229.24.230	10.44.167.30	RSH	Client -> Server data
282	2015-06-25 08:50:04.114877	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=48 Win=32073 Len=0
283	2015-06-25 08:50:04.114883	10.229.24.230	10.44.167.30	RSH	Client -> Server data
284	2015-06-25 08:50:04.115362	10.44.167.30	10.229.24.230	TCP	shell > 26040 [ACK] Seq=1 Ack=413 Win=31755 Len=0
285	2015-06-25 08:50:04.116192	10.44.167.30	10.229.24.230	TCP	shell > 26040 [RST, ACK] Seq=1 Ack=413 Win=32120 Len=0

如果您在封包擷取中追蹤TCP資料流，將會看到以下內容：

```
<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...".
```

錯誤表示存在阻止訪問IP地址處的系統日誌伺服器的防火牆或入侵防禦系統(IPS)。如果介於兩者之間的所有裝置都已檢查並確認以允許流量，則這也可能表示系統日誌伺服器太忙且拒絕連線。當ESA配置為將日誌檔案傳送到系統日誌伺服器時，預設情況下，它將使用UDP系統日誌埠514，除非配置為使用TCP。配置裝置後，導致連線被列為拒絕的唯一原因就是該裝置接收到在開啟連線時關閉連線的資料包。