

O Encaminhador de Lixo Eletrônico não está enviando eventos à Nuvem de Lixo Eletrônico

Aplicabilidade

Nuvem Splunk

Descrição

Um encaminhador de Splunk não está mais enviando eventos para a Splunk Cloud. Isso pode afetar um encaminhador universal, um encaminhador pesado ou um nível de encaminhamento intermediário.

O seguinte erro é exibido no `splunkd.log`:

```
ERROR TcpOutputFd - Connection to host=1.22.122.222:9997 failed. sock_error = 104. SSL  
Error = No error
```

A mensagem `sock_error = 104` indica que a conexão TCP foi redefinida enquanto o encaminhador tentava se comunicar com o ponto de extremidade de recebimento do Splunk Cloud.

Investigação

Verifique a conectividade de rede básica do encaminhador afetado para o endpoint de entrada do Splunk Cloud:

```
telnet inputs1.<stack_id>.splunkcloud.com 9997
```

Uma conexão `telnet` bem-sucedida confirma que a porta está acessível. No entanto, ele não

valida totalmente a conexão SSL/TLS nem confirma se o tráfego não está sendo redefinido por um dispositivo de rede intermediário.

Para validar ainda mais a conexão, execute um dos seguintes comandos do encaminhador afetado:

```
openssl s_client -connect inputs1.<stack_id>.splunkcloud.com:9997
```

OU

```
$SPLUNK_HOME/bin/splunk cmd openssl s_client -connect inputs1.<stack_id>.splunkcloud.com
```

Se a seguinte saída for retornada, a conexão será redefinida:

```
CONNECTED(00000003)  
write:errno=104
```

Isso confirma que o encaminhador pode inicialmente estabelecer uma conexão TCP, mas a conexão é forçada antes que a sessão SSL/TLS seja concluída.

Reveja também a configuração de encaminhamento no encaminhador afetado, incluindo `outputs.conf`, para confirmar se o encaminhador está usando o ponto final e a porta de recebimento corretos do Splunk Cloud.

Resolução

O erro 104 é `ECONNRESET`, que significa "Connection reset by peer." Isso indica que a conexão foi forçada a fechar com um pacote de redefinição TCP. A redefinição pode ser enviada pelo endpoint de destino ou por um dispositivo de rede intermediário, como um firewall, proxy, balanceador de carga, IDS/IPS, dispositivo de inspeção SSL ou dispositivo de rede.

Revise o caminho de rede completo entre o encaminhador afetado e a Splunk Cloud. Confirme se:

- O tráfego de saída para o ponto de extremidade de entrada do Splunk Cloud é permitido na porta 9997.
- Firewalls, proxies ou dispositivos de rede não estão redefinindo sessões TCP.
- A inspeção SSL não está interferindo na conexão de encaminhamento de Splunk.
- Todas as alterações recentes relacionadas a rede, firewall, proxy, roteamento ou certificado são analisadas.
- O aplicativo e os certificados do encaminhador Splunk Cloud estão atualizados e corretamente implantados.
- Os encaminhadores intermediários podem se comunicar com o Splunk Cloud e não estão descartando ou bloqueando o tráfego encaminhado.

Após corrigir a configuração de rede, firewall ou certificado, reinicie o encaminhador afetado, se necessário, ou permita que ele se reconecte automaticamente. Em seguida, confirme se os eventos estão sendo indexados com êxito no Splunk Cloud.

Links relacionados

[Problemas de conexão com o Universal Forwarder para Linux ARM e Splunk Cloud \(erro SSL\)](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.