Erro de Validação do Certificado de Acesso Seguro com Carregamentos de Log do Cliente de Splunk

Contents

Problema

Os clientes Windows que executam o cliente Splunk não puderam carregar logs na nuvem Splunk devido a erros de validação de certificado quando o tráfego foi descriptografado pelo Cisco Secure Access. Mais de 5.000 fontes de log do Windows falharam ao enviar dados para a nuvem Splunk, afetando a ingestão de logs. O erro específico observado nos logs do cliente Splunk foi:

```
02-27-2026 16:51:54.830 +0530 ERROR X509Verify [15668 TcpOutEloop] - Server X509 certificate failed val
```

O tráfego para o destino *.splunkcloud.com estava fluindo pelo firewall, mas a validação do certificado no nível do aplicativo estava falhando. A navegação na Web para sites nos quais a descriptografia SSL estava habilitada continuou a funcionar normalmente.

Ambiente

- Cisco Secure Access com descriptografia SSL/TLS ativada
- Clientes Windows com Splunk Universal Forwarder instalado
- Destino da nuvem de tronco: *.splunkcloud.com
- Mais de 5.000 origens de log do Windows afetadas
- O cliente Splunk usa seu próprio armazenamento de certificados, não o armazenamento de certificados do sistema Microsoft

Resolução

O problema foi resolvido com a implementação de uma política de desvio de descriptografia para tráfego de nuvem Splunk no Cisco Secure Access.

Foram dados vários passos.

Passo 1: Identificar o problema

Durante uma sessão do WebEx, o comportamento foi confirmado e reproduzido. Os testes mostraram que, quando a descriptografia de Acesso seguro foi desabilitada para um cliente ou quando o serviço SWG foi desabilitado no cliente, os carregamentos de log de Splunk tiveram êxito. Isso confirmou que o processo de descriptografia SSL/TLS estava causando a falha de validação do certificado.

Passo 2: Criar lista de destinos

Uma lista de destinos foi criada contendo os FQDNs e os endereços IP da nuvem de Splunk para direcionar especificamente o tráfego destinado aos serviços de nuvem de Splunk.

Passo 3: Implementar Política de Desvio de Descriptografia

Uma política do Cisco Secure Access foi implementada para desabilitar a descriptografia SSL/TLS para o tráfego correspondente à lista de destinos da nuvem Splunk. Essa política de desvio permitiu que os clientes Splunk estabelecessem conexões criptografadas diretas com a nuvem Splunk sem interceptação de certificado pelo Secure Access.

Passo 4: Validação

Após implementar a política de desvio de descriptografia, a validação confirmou que:

- Os clientes Splunk puderam carregar logs com êxito
- O número geral de clientes relatando na nuvem Splunk aumentou substancialmente
- Nenhum outro erro de validação de certificado foi observado

A gravidade do caso foi reduzida de 1 para 3 e colocada no status de monitoramento para observar a ingestão contínua e bem-sucedida de registros.

Causa

A causa raiz foi que o cliente Splunk usa seu próprio armazenamento de certificados e não confia no certificado SubCA Primário do Cisco Secure Access que estava sendo apresentado durante a descriptografia SSL/TLS. Quando o Cisco Secure Access interceptou e descriptografou o tráfego SSL para a nuvem Splunk, ele criptografou novamente o tráfego usando sua própria autoridade de certificação. O processo de validação do certificado do cliente Splunk rejeitou este certificado porque não pôde verificar a cadeia de certificados de volta para uma autoridade de certificado raiz confiável em seu próprio repositório de certificados.

O erro de validação X.509 específico "não é possível obter o certificado do emissor local" (código de erro 20) indica que o processo de validação do certificado não pôde localizar a autoridade de certificação emissora no repositório de certificados confiáveis do cliente, causando a falha da conexão.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

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.