

Resolver o tempo limite de conexão LDAP de migração para nuvem do AWS Secure Email Gateway

Contents

Problema

Após migrar o ambiente Cisco Secure Email Gateway (SEG) para a plataforma SEG hospedada na nuvem da Amazon Web Services (AWS), os administradores passam por problemas persistentes de login e desempenho.

Os sintomas incluíram:

- Atrasos significativos ao acessar o SEG nas interfaces GUI e CLI
- Excesso de tempo necessário para autenticação após inserir nome de usuário e senha
- Carregamento muito lento do painel/página principal
- A capacidade de resposta geral da plataforma foi extremamente lenta
- Os problemas mais perceptíveis durante o acesso autenticado por LDAP

A análise de captura de pacotes revela que as sessões SEG TCP para servidores LDAP estão sendo fechadas pelo GWLB (Gateway Load Balancer) após aproximadamente 350 segundos de tempo ocioso, causando atrasos e timeouts de autenticação.

Ambiente

- Cisco Secure Email Gateway (SEG) migrado para a plataforma hospedada na nuvem da AWS
- Versão do AsyncOS: 16.0.4-016

- Autenticação LDAP configurada com o Active Directory
- Balanceador de Carga do Gateway AWS (GWLB) no caminho de rede
- Cisco Secure Email e Web Manager também afetados pelo mesmo problema
- Criptografia SSL/TLS habilitada para conexões LDAP na porta 3269

Resolução

Ajuste as configurações de tempo de vida da conexão LDAP para evitar tempos limite de sessão ociosos causados pelo Balanceador de Carga do Gateway AWS com estas etapas:

1. Conecte-se ao SEG CLI e acesse a configuração LDAP:

```
device# ldapconfig
```

2. Localize o perfil do servidor LDAP e modifique a configuração "Maximum lifetime per connection to the server (in seconds)" (Tempo de vida máximo por conexão com o servidor (em segundos)). Altere esse valor para 300 segundos para garantir que as conexões sejam atualizadas antes do limite de tempo ocioso de 350 segundos do Balanceador de Carga do Gateway.

Configuração original:

```
Max lifetime per connection: 1800
```

Configuração atualizada:

```
Max lifetime per connection: 300
```

3. Confirme as alterações de configuração e permita que o sistema aplique as novas configurações.

4. Aplique a alteração idêntica do tempo de vida da conexão LDAP ao Cisco Secure Email e Web Manager usando a mesma configuração de 300 segundos.
5. Teste a funcionalidade de login da GUI e CLI. Depois de implementar as alterações, os tempos de login devem ser reduzidos para aproximadamente 5 segundos e os atrasos de autenticação não devem mais ocorrer.
6. Monitore o ambiente para verificar se há recorrência do problema e colete capturas de pacotes se os problemas persistirem.

Causa

A análise de captura de pacotes mostrou que o GWLB (AWS Gateway Load Balancer) estava encerrando sessões TCP ociosas após aproximadamente 350 segundos. O tempo de vida padrão da conexão LDAP do SEG é de 1800 segundos, o que excede o limite de tempo ocioso do GWLB de 350 segundos. Quando as conexões LDAP permaneceram ociosas por mais de 350 segundos, o GWLB interromperia as sessões TCP, causando atrasos de autenticação e timeouts quando os usuários tentavam fazer login. Reduzindo o tempo de vida da conexão LDAP para 300 segundos, o SEG atualiza as conexões de forma proativa antes que o tempo limite de GWLB ocorra e evite atrasos de autenticação.

Conteúdo relacionado

- [Guia do usuário do AsyncOS 16.5 para Cisco Secure Email Cloud Gateway - GD \(implantação geral\)](#)
- [Guia do usuário do AsyncOS 16.5 para Cisco Secure Email e Web Manager - GD \(General Deployment, Implementação geral\)](#)

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.