

Resolver tiempo de espera de conexión LDAP de migración a nube de AWS de gateway de correo electrónico seguro

Contenido

Problema

Después de migrar el entorno de Cisco Secure Email Gateway (SEG) a la plataforma SEG alojada en la nube de Amazon Web Services (AWS), los administradores experimentan problemas persistentes de inicio de sesión y rendimiento.

Los síntomas incluyeron:

- Retrasos significativos al acceder a SEG en interfaces GUI y CLI
- Se requiere demasiado tiempo para la autenticación después de introducir el nombre de usuario y la contraseña
- Carga muy lenta del panel/página principal
- La respuesta general de la plataforma fue extremadamente lenta
- Los problemas fueron más notables durante el acceso autenticado LDAP

El análisis de captura de paquetes revela que el equilibrador de carga de gateway (GWLB) cierra las sesiones TCP de SEG a los servidores LDAP después de aproximadamente 350 segundos de inactividad, lo que causa retrasos y tiempos de espera de autenticación.

Entorno

- Cisco Secure Email Gateway (SEG) migró a la plataforma alojada en la nube de AWS
- Versión de AsyncOS: 16.0.4-016

- Autenticación LDAP configurada con Active Directory
- Equilibrador de carga de gateway de AWS (GWLB) en la ruta de red
- Cisco Secure Email and Web Manager también se ve afectado por el mismo problema
- Cifrado SSL/TLS habilitado para conexiones LDAP en el puerto 3269

Resolución

Ajuste la configuración de duración de la conexión LDAP para evitar los tiempos de espera de sesión inactivos causados por el equilibrador de carga de gateway de AWS con estos pasos:

1. Conéctese a la CLI de SEG y acceda a la configuración de LDAP:

```
device# ldapconfig
```

2. Busque el perfil de servidor LDAP y modifique la configuración "Vigencia máxima por conexión al servidor (en segundos)". Cambie este valor a 300 seconds para asegurarse de que las conexiones se actualizan antes del umbral de tiempo de espera de inactividad de 350 segundos del equilibrador de carga de gateway.

Configuración original:

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

Configuración actualizada:

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

3. Realice los cambios de configuración y permita que el sistema aplique los nuevos parámetros.

4. Aplique el mismo cambio de duración de la conexión LDAP a Cisco Secure Email and Web Manager con la misma configuración de 300 segundos.

5. Pruebe la funcionalidad de inicio de sesión de GUI y CLI. Después de implementar los cambios, los tiempos de inicio de sesión deben reducirse a aproximadamente 5 segundos y los retrasos de autenticación ya no deben ocurrir.

6. Supervise el entorno para detectar cualquier recurrencia del problema y recopile capturas de paquetes si persisten los problemas.

Causa

El análisis de captura de paquetes mostró que el equilibrador de carga de gateway de AWS (GWLB) estaba terminando las sesiones TCP inactivas después de aproximadamente 350 segundos. La duración de la conexión LDAP predeterminada del SEG es de 1800 segundos, lo que excede el umbral de tiempo de espera inactivo del GWLB de 350 segundos. Cuando las conexiones LDAP permanecían inactivas durante más de 350 segundos, el GWLB desactivaba las sesiones TCP, lo que provocaba retrasos de autenticación y tiempos de espera cuando los usuarios intentaban iniciar sesión. Al reducir la duración de la conexión LDAP a 300 segundos, el SEG actualiza las conexiones de forma proactiva antes de que se agote el tiempo de espera de GWLB y evita retrasos en la autenticación.

Contenido relacionado

- [Guía del usuario de AsyncOS 16.5 para Cisco Secure Email Cloud Gateway - GD \(implementación general\)](#)
- [Guía del usuario de AsyncOS 16.5 para Cisco Secure Email and Web Manager - GD \(implementación general\)](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).