

Resolve Secure Email Gateway AWS Cloud Migration LDAP Connection Timeout

Contents

Issue

After migrating Cisco Secure Email Gateway (SEG) environment to the Amazon Web Services (AWS) Cloud-hosted SEG platform, administrators experience persistent login and performance issues.

Symptoms included:

- Significant delays while accessing the SEG in both GUI and CLI interfaces
- Excessive time required for authentication after entering username and password
- Very slow loading of the main dashboard/page
- Overall platform responsiveness was extremely slow
- Issues were most noticeable during LDAP-authenticated access

Packet capture analysis reveals that SEG TCP sessions to LDAP servers are being closed by the Gateway Load Balancer (GWLB) after approximately 350 seconds of idle time, causing authentication delays and timeouts.

Environment

- Cisco Secure Email Gateway (SEG) migrated to AWS Cloud-hosted platform
- AsyncOS Version: 16.0.4-016
- LDAP authentication configured with Active Directory
- AWS Gateway Load Balancer (GWLB) in the network path
- Cisco Secure Email and Web Manager also affected by the same issue
- SSL/TLS encryption enabled for LDAP connections on port 3269

Resolution

Adjust the LDAP connection lifetime settings to prevent idle session timeouts caused by the AWS Gateway Load Balancer with these steps:

1. Connect to the SEG CLI and access the LDAP configuration:

```
device# ldapconfig
```

2. Locate the LDAP server profile and modify the "Maximum lifetime per connection to the server (in seconds)" setting. Change this value to **300 seconds** to ensure connections are refreshed before the Gateway Load Balancer's 350-second idle timeout threshold.

Original configuration:

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

Updated configuration:

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

3. Commit the configuration changes and allow the system to apply the new settings.
4. Apply the identical LDAP connection lifetime change to the Cisco Secure Email and Web Manager using the same 300-second configuration.
5. Test the GUI and CLI login functionality. After implementing the changes, login times should be reduced to approximately 5 seconds, and the authentication delays should no longer occur.
6. Monitor the environment for any recurrence of the issue and collect packet captures if problems persist.

Cause

Packet capture analysis showed that the AWS Gateway Load Balancer (GWLb) was terminating idle TCP

sessions after approximately 350 seconds. The SEG's default LDAP connection lifetime is 1800 seconds, which exceeds the GWLB's idle timeout threshold of 350 seconds. When LDAP connections remained idle for more than 350 seconds, the GWLB would tear down the TCP sessions, causing authentication delays and timeouts when users attempted to log in. By reducing the LDAP connection lifetime to 300 seconds, the SEG proactively refreshes connections before the GWLB timeout occurs and prevents authentication delays.

Related Content

- [User Guide for AsyncOS 16.5 for Cisco Secure Email Cloud Gateway - GD \(General Deployment\)](#)
- [User Guide for AsyncOS 16.5 for Cisco Secure Email and Web Manager - GD \(General Deployment\)](#)