

解决安全邮件网关AWS云迁移LDAP连接超时

目录

问题

将Cisco Secure Email Gateway(SEG)环境迁移到Amazon Web Services(AWS)云托管SEG平台后，管理员会遇到持续的登录和性能问题。

症状包括：

- 在GUI和CLI界面中访问SEG时出现严重延迟
- 输入用户名和密码后，身份验证所需的时间过长
- 主控制面板/页面的加载非常缓慢
- 整体平台响应速度极慢
- 问题在LDAP身份验证访问期间最明显

数据包捕获分析显示，在大约350秒的空闲时间后，网关负载均衡器(GWLB)将关闭到LDAP服务器的SEG TCP会话，从而导致身份验证延迟和超时。

环境

- Cisco Secure Email Gateway(SEG)迁移至AWS云托管平台
- AsyncOS版本：16.0.4-016
- 使用Active Directory配置的LDAP身份验证
- 网络路径中的AWS网关负载均衡器(GWLB)
- Cisco Secure Email和Web Manager也受到相同问题的影响
- 为端口3269上的LDAP连接启用SSL/TLS加密

分辨率

使用以下步骤调整LDAP连接生存期设置，以防止AWS网关负载均衡器导致的空闲会话超时：

1. 连接到SEG CLI并访问LDAP配置：

```
device# ldapconfig
```

2. 找到LDAP服务器配置文件，并修改“每次连接到服务器时的最长生命期（秒）”设置。将此值更改为300秒，以确保在网关负载均衡器的350秒空闲超时阈值之前刷新连接。

原始配置：

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

更新后的配置：

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

3. 提交配置更改并允许系统应用新设置。

4. 使用相同的300秒配置将相同的LDAP连接生命周期更改应用到Cisco Secure Email and Web Manager。

5. 测试GUI和CLI登录功能。实施更改后，登录时间应缩短至约5秒，并且不会再出现身份验证延迟。

6. 监控环境以确定问题是否再次出现，如果问题依然存在，则收集数据包捕获。

原因

数据包捕获分析表明，AWS网关负载均衡器(GWLB)在大约350秒后终止空闲TCP会话。SEG的默认LDAP连接生存时间为1800秒，超过了GWLB的空闲超时阈值350秒。当LDAP连接闲置超过350秒时，GLB将中断TCP会话，导致身份验证延迟和用户尝试登录时超时。通过将LDAP连接生存时间缩短至300秒，SEG会在GWLB超时发生之前主动刷新连接，并防止身份验证延迟。

相关内容

- [思科安全邮件云网关AsyncOS 16.5用户指南 — GD \(通用部署 \)](#)
- [思科安全邮件和网络管理器AsyncOS 16.5用户指南 — GD \(通用部署 \)](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。