

Lösen des Timeouts für sichere E-Mail-Gateways AWS Cloud-Migration LDAP-Verbindung

Inhalt

Problem

Nach der Migration der Cisco Secure Email Gateway (SEG)-Umgebung auf die Cloud-gehostete Amazon Web Services (AWS) SEG-Plattform treten für Administratoren dauerhafte Anmelde- und Leistungsprobleme auf.

Symptome:

- Erhebliche Verzögerungen beim Zugriff auf SEG sowohl über die grafische Benutzeroberfläche als auch über die Kommandozeile
- Zu viel Zeit für die Authentifizierung nach Eingabe von Benutzername und Passwort
- Sehr langsames Laden des Haupt-Dashboards/der Hauptseite
- Die Reaktionsfähigkeit der Plattform insgesamt war extrem langsam.
- Probleme traten vor allem beim LDAP-authentifizierten Zugriff auf.

Die Paketerfassungsanalyse zeigt, dass SEG TCP-Sitzungen mit LDAP-Servern vom Gateway Load Balancer (GWLB) nach ca. 350 Sekunden Inaktivitätszeit geschlossen werden, was zu Authentifizierungsverzögerungen und Zeitüberschreitungen führt.

Umwelt

- Cisco Secure Email Gateway (SEG) auf Cloud-gehostete AWS-Plattform migriert
- AsyncOS-Version 16.0.4-016

- Mit Active Directory konfigurierte LDAP-Authentifizierung
- AWS Gateway Load Balancer (GWLB) im Netzwerkpfad
- Cisco Secure Email und Web Manager sind ebenfalls vom gleichen Problem betroffen.
- SSL-/TLS-Verschlüsselung aktiviert für LDAP-Verbindungen auf Port 3269

Auflösung

Passen Sie die Einstellungen für die Lebensdauer der LDAP-Verbindung an, um Zeitüberschreitungen bei Inaktivitätssitzungen zu vermeiden, die durch den AWS Gateway Load Balancer verursacht werden. Gehen Sie dazu wie folgt vor:

1. Stellen Sie eine Verbindung mit der SEG-CLI her, und greifen Sie auf die LDAP-Konfiguration zu:

```
device# ldapconfig
```

2. Suchen Sie das LDAP-Serverprofil, und ändern Sie die Einstellung "Maximale Lebensdauer pro Verbindung zum Server (in Sekunden)". Ändern Sie diesen Wert auf 300 Sekunden, um sicherzustellen, dass die Verbindungen vor dem Timeout-Schwellenwert des Gateway Load Balancer für Leerlaufzeiten von 350 Sekunden aktualisiert werden.

Originalkonfiguration:

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

Aktualisierte Konfiguration:

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

3. Bestätigen Sie die Konfigurationsänderungen, und erlauben Sie dem System, die neuen Einstellungen zu übernehmen.

4. Wenden Sie die identische Änderung der Lebensdauer der LDAP-Verbindung unter Verwendung derselben 300-Sekunden-Konfiguration auf Cisco Secure Email und Web Manager an.
5. Testen Sie die GUI- und CLI-Anmeldefunktionen. Nach der Implementierung der Änderungen sollten die Anmeldezeiten auf ca. 5 Sekunden reduziert werden, und die Authentifizierungsverzögerungen sollten nicht mehr auftreten.
6. Überwachen Sie die Umgebung auf ein Wiederauftreten des Problems und erfassen Sie die Paketerfassung, wenn das Problem weiterhin besteht.

Ursache

Die Paketerfassungsanalyse zeigte, dass der AWS Gateway Load Balancer (GWLB) inaktive TCP-Sitzungen nach ca. 350 Sekunden beendete. Die standardmäßige LDAP-Verbindungslebensdauer der SEG beträgt 1800 Sekunden und überschreitet damit den Timeout-Schwellenwert des GWLB für Leerlaufzeiten von 350 Sekunden. Wenn LDAP-Verbindungen länger als 350 Sekunden inaktiv waren, hat der GWLB die TCP-Sitzungen abgebrochen, was zu Authentifizierungsverzögerungen und Zeitüberschreitungen beim Anmeldeversuch von Benutzern führte. Durch die Reduzierung der LDAP-Verbindungslebensdauer auf 300 Sekunden aktualisiert die SEG Verbindungen proaktiv, bevor das GWLB-Timeout eintritt, und verhindert Authentifizierungsverzögerungen.

Verwandte Inhalte

- [Benutzerhandbuch für AsyncOS 16.5 für Cisco Secure Email Cloud Gateway - GD \(Allgemeine Bereitstellung\)](#)
- [Benutzerhandbuch für AsyncOS 16.5 für Cisco Secure Email und Web Manager - GD \(Allgemeine Bereitstellung\)](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.