

Secure Email Gateway AWS Cloud Migration

LDAP 연결 시간 초과 확인

목차

문제

Cisco SEG(Secure Email Gateway) 환경을 Amazon Web Services(AWS) 클라우드 호스팅 SEG 플랫폼으로 마이그레이션한 후 관리자는 지속적인 로그인 및 성능 문제를 경험하게 됩니다.

증상은 다음과 같습니다.

- GUI 및 CLI 인터페이스에서 SEG에 액세스하는 동안 상당한 지연
- 사용자 이름 및 비밀번호 입력 후 인증에 과도한 시간 필요
- 기본 대시보드/페이지의 로딩이 매우 느림
- 전반적인 플랫폼 응답성이 매우 느림
- LDAP 인증 액세스 시 문제가 가장 많이 나타남

패킷 캡처 분석 결과, 유휴 시간이 약 350초 후에 GWLB(Gateway Load Balancer)가 LDAP 서버에 대한 SEG TCP 세션을 닫아 인증 지연 및 시간 초과가 발생하는 것으로 나타났습니다.

환경

- Cisco SEG(Secure Email Gateway)가 AWS 클라우드 호스팅 플랫폼으로 마이그레이션됨
- AsyncOS 버전 16.0.4-016
- Active Directory로 구성된 LDAP 인증
- 네트워크 경로의 AWS GWLB(Gateway Load Balancer)
- Cisco Secure Email 및 Web Manager도 동일한 문제의 영향을 받습니다

- 포트 3269의 LDAP 연결에 대해 SSL/TLS 암호화 사용

해결

LDAP 연결 수명 설정을 조정하여 다음 단계를 통해 AWS 게이트웨이 로드 밸런서로 인한 유휴 세션 시간 제한을 방지합니다.

1. SEG CLI에 연결하고 LDAP 컨피그레이션에 액세스합니다.

```
device# ldapconfig
```

2. LDAP 서버 프로필을 찾아 "서버에 대한 연결당 최대 수명(초)" 설정을 수정합니다. 게이트웨이 로드 밸런서의 350초 유휴 시간 제한 임계값 이전에 연결을 새로 고치려면 이 값을 300초로 변경합니다.

원래 구성:

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

업데이트된 구성:

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

3. 컨피그레이션 변경 사항을 커밋하고 시스템에서 새 설정을 적용하도록 허용합니다.

4. 동일한 300초 컨피그레이션을 사용하여 Cisco Secure Email and Web Manager에 동일한 LDAP 연결 수명 변경을 적용합니다.

5. GUI 및 CLI 로그인 기능을 테스트합니다. 변경 사항을 구현한 후에는 로그인 시간을 약 5초로 줄이고 인증 지연을 더 이상 발생시키지 않아야 합니다.

6. 환경의 문제 재발을 모니터링하고 문제가 지속되면 패킷 캡처를 수집합니다.

원인

패킷 캡처 분석 결과, AWS GWLB(Gateway Load Balancer)가 약 350초 후에 유휴 TCP 세션을 종료하는 것으로 나타났습니다. SEG의 기본 LDAP 연결 수명은 1800초이며, 이는 GWLB의 유휴 시간 제한 임계값인 350초를 초과합니다. LDAP 연결이 350초 이상 유휴 상태로 유지되면 GWLB에서 TCP 세션을 해제하여 사용자가 로그인을 시도할 때 인증이 지연되고 시간이 초과됩니다. LDAP 연결 수명을 300초로 줄임으로써 SEG는 GWLB 시간 초과가 발생하기 전에 연결을 사전 대응적으로 새로 고치고 인증 지연을 방지합니다.

관련 콘텐츠

- [AsyncOS 16.5 for Cisco Secure Email Cloud Gateway - GD 사용 설명서\(일반 배포\)](#)
- [AsyncOS 16.5 for Cisco Secure Email and Web Manager 사용 설명서 - GD\(일반 배포\)](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.