CUCM 10.5(2)SU2로 업그레이드 후 보안 LDAP 문제

목차

소개

이 문서에서는 Cisco CUCM(Unified Communications Manager) 10.5(2)SU2 또는 9.1(2)SU3으로 업그레이드한 후 LDAP(Secure Lightweight Directory Access Protocol)의 문제와 이 문제를 해결하는 데 필요한 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 CUCM 버전 10.5(2)SU2를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

보안 LDAP 인증을 위해 IP 주소 또는 FQDN(Fully Qualified Domain Name)을 사용하도록 CUCM을 구성할 수 있습니다.FQDN이 제공됩니다.CUCM의 기본 동작은 FQDN을 사용하는 것입니다.IP 주

소를 사용하려는 경우 CUCM Publisher의 **CLI**(Command Line Interface)에서 utils ldap config ipaddr 명령을 실행할 수 있습니다.

10.5(2)SU2 및 9.1(2)SU3에 도입된 CSCun63825의 수정 전에 CUCM은 LDAP에 대한 TLS(Transport Layer Security) 연결에 대해 FQDN 검증을 엄격하게 시행하지 않았습니다. FQDN 검증은 MM(CUCM Admin > System > LDAP > CUCM)에 구성된 호스트 이름을 비교해야 합니다. 인증) 및 LDAP 서버에 대한 TLS 연결 중에 LDAP 서버에서 제공하는 LDAP 인증서의 CN(Common Name) 또는 SAN(Subject Alternative Name) 필드따라서 LDAP 인증이 활성화되고(**SSL 사용** 확인) LDAP 서버/서버가 IP 주소로 정의되는 경우 **utils ldap config ipaddr** 명령이 실행되지 않더라도 인증이 성공합니다.

CUCM을 10.5(2)SU2, 9.1(2)SU3 이상 버전으로 업그레이드한 후 FQDN 검증이 적용되며 utils ldap config를 사용하는 모든 변경 사항은 FQDN을 사용하는 기본 동작으로 돌아갑니다.이 변경 결과로 CSCux83666을 열었습니다. 또한 CLI 명령 **utils ldap config 상태**가 추가되어 IP 주소 또는 FQDN이 사용되고 있는지 확인합니다.

시나리오 1

업그레이드 LDAP 인증이 활성화되기 전에 서버/서버가 IP 주소로 정의되면 CUCM Publisher의 CLI에서 utils ldap config ipaddr 명령이 구성됩니다.

업그레이드 LDAP 인증이 실패하고 CUCM Publisher의 CLI에서 **utils ldap config status** 명령을 실행하면 FQDN이 인증에 사용됨을 보여줍니다.

시나리오 2

업그레이드 LDAP 인증이 활성화되기 전에 서버/서버가 IP 주소로 정의되면 CUCM Publisher의 CLI에서 utils ldap config ipaddr 명령이 구성되지 않습니다.

업그레이드 LDAP 인증이 실패하고 CUCM Publisher의 CLI에서 **utils ldap config status** 명령을 실행하면 FQDN이 인증에 사용됨을 보여줍니다.

문제

CUCM에서 SSL(Secure Sockets Layer)을 사용하도록 LDAP 인증이 구성되어 있고 업그레이드 전에 IP 주소를 사용하여 LDAP 서버/서버가 구성된 경우 보안 LDAP 인증이 실패합니다.

LDAP 인증 설정을 확인하려면 CUCM **Admin(CUCM 관리) 페이지 > System(시스템) > LDAP > LDAP Authentication(LDAP 인증)으로 이동하고** LDAP 서버가 FQDN이 아닌 IP 주소로 정의되었는지 확인합니다.LDAP 서버가 FQDN으로 정의되고 CUCM이 FQDN을 사용하도록 구성된 경우(확인은 아래 명령 참조) 이 문제가 발생할 가능성이 높습니다.

업그레이드 후 CUCM이 IP 주소 또는 FQDN을 사용하도록 구성되었는지 확인하려면 CUCM 게시자의 CLI에서 **utils ldap config status** 명령을 사용합니다.

```
admin:utils ldap config status
utils ldap config fqdn configured
```

이 문제가 발생했는지 확인하려면 CUCM DirSync 로그에서 이 오류를 확인할 수 있습니다.이 오류는 LDAP 서버가 CUCM의 LDAP 인증 컨피그레이션 페이지에서 IP 주소를 사용하여 구성되었으며 LDAP 인증서의 CN 필드와 일치하지 않음을 나타냅니다.

```
2016-02-09 14:08:32,718 DEBUG [http-bio-443-exec-1] impl.AuthenticationLDAP -
URL contains IP Address
```

솔루션

The CUCM **Admin(CUCM 관리) > System(시스템) > LDAP > LDAP Authentication(LDAP 인증)** 페이지로 이동하고 LDAP 서버의 IP 주소에서 LDAP 서버의 FQDN으로 LDAP 서버 컨피그레이션을 변경합니다.LDAP 서버의 IP 주소를 사용해야 하는 경우 CUCM 게시자의 CLI에서 이 명령을 사용합니다

```
admin:utils ldap config ipaddr
Now configured to use IP address
admin:
```

FQDN 유효성 검사 실패가 발생할 수 있는 기타 이유는 이 특정 문제와 관련이 없습니다.

1. CUCM에 구성된 LDAP 호스트 이름이 LDAP 인증서의 CN 필드(LDAP 서버의 호스트 이름)와 일치하지 않습니다.

이 문제를 해결하려면 The CUCM **Admin(CUCM 관리) > System(시스템) > LDAP > LDAP Authentication(LDAP 인증)** 페이지로 이동하여 LDAP 인증서의 CN 필드에서 호스트 이름/FQDN을 사용하도록 LDAP **서버 정보**를 수정합니다.또한 사용된 이름이 라우팅 가능하며 CUCM 게시자의 CLI에서 **네트워크 ping을** 사용하여 CUCM에서 연결할 수 있는지 확인합니다.

2. DNS 로드 밸런서는 네트워크에 구축되며 CUCM에 구성된 LDAP 서버는 DNS 로드 밸런서를 사용합니다.예를 들어, 이 컨피그레이션은 adaccess.example.com을 가리키며, 이는 지역 또는 기타 요소를 기반으로 여러 LDAP 서버 간에 로드 밸런싱을 수행합니다.요청에 응답하는 LDAP 서버는 adaccess.example.com 이외의 FQDN을 가질 수 있습니다.호스트 이름 불일치가 있으므로 유효성 검사에 실패합니다.

```
2016-02-06 09:19:51,702 ERROR [http-bio-443-exec-23] impl.AuthenticationLDAP -
verifyHostName:Exception.javax.net .ssl.SSLPeerUnverifiedException: hostname of the server
'adlab.testing.cisco.local' does not match the hostname in the server's certificate.
```

이 문제를 해결하려면 LDAP 서버 자체가 아닌 로드 밸런서에서 TLS 연결이 종료되도록 LDAP 로드 밸런서 체계를 변경합니다.이것이 불가능한 경우 유일한 옵션은 FQDN 검증을 비활성화하고 대신 IP 주소를 사용하여 검증하는 것입니다.