# CUCM 10.5(2)SU2へのアップグレード後のLDAP問題の保護

## 内容



## 概要

このドキュメントでは、Cisco Unified Communications Manager(CUCM)10.5(2)SU2または9.1(2)SU3にアップグレードした後のSecure Lightweight Directory Access Protocol(LDAP)に関する問題と、この問題を解決するために実行できる手順について説明します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、CUCMバージョン10.5(2)SU2に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 背景説明

CUCMは、IPアドレスまたは完全修飾ドメイン名(FQDN)を使用してセキュアLDAP認証を行うよ

うに設定できます。FQDNが入力されています。CUCMのデフォルトの動作は、FQDNを使用することです。IPアドレスの使用が望ましい場合は、**utils ldap config ipaddrコマンド**をCUCMパブリッシャのコマンドラインインターフェイス(CLI)から実行できます。

10.5(2)SU2および9.1(2)SU3で導入されたCSCun63825の修正に先立ち、CUCMはLDAPへのTransport Layer Security(TLS)接続のFQDN検証を厳密に実施していませんでしたcucm(**[CUCM Admin] > [System] > [LDAP] > [LDAP Authentication])**、およびCUCMからLDAPサーバへのTLS接続時にLDAPサーバによって提示されるLDAP証明書の[Common Name (CN)]または[Subject Alternative Name (SAN)]フィールド。したがって、LDAP認証が有効で(**use SSLを使用する**)と、LDAPサーバ/サーバがIPアドレスで定義されている場合、**utils ldap config ipaddrコマンドが発行されていなくても認証は成功します。**

CUCMを10.5(2)SU2、9.1(2)SU3、またはそれ以降のバージョンにアップグレードした後、FQDNの検証が実施され、**utils ldap configを使用した変更はデフォルトの動作に戻され、FQDNを使用します。**この変更の結果、CSCux83666が開かれました。また、CLIコマンド**utils ldap config statusが追加さ**れ、IPアドレスまたはFQDNが使用されているかどうかを表示します。

**シナリオ 1**

アップグレードLDAP認証を有効にする前に、サーバ/サーバをIPアドレスで定義し、**utils ldap config ipaddrコマンドをCUCMパブリッシャのCLIで設定します。**

LDAP認証のアップグレードが失敗し、CUCMパブリッシャのCLIで**utils ldap config statusコマンドを実行**すると、認証にFQDNが使用されていることが示されます。

**シナリオ 2**

アップグレードLDAP認証が有効になる前は、サーバ/サーバがIPアドレスで定義され、CUCMパブリッシャのCLIで**utils ldap config ipaddrコマンドが設定されませ**ん。

LDAP認証のアップグレードが失敗し、CUCMパブリッシャのCLIで**utils ldap config statusコマンドを実行**すると、認証にFQDNが使用されていることが示されます。

# 問題

LDAP認証がCUCMでSecure Sockets Layer(SSL)を使用するように設定され、LDAPサーバ/サーバがアップグレード前にIPアドレスを使用して設定されている場合、セキュアLDAP認証は失敗します。

LDAP認証設定を確認するには、**[CUCM Admin page] > [System] > [LDAP] > [LDAP Authentication]に移動**して、LDAPサーバがFQDNではなくIPアドレスで定義されていることを確認します。LDAPサーバがFQDNで定義され、CUCMがFQDNを使用するように設定されている場合（確認のため、次のコマンドを参照）、これが問題である可能性は低くなります。


アップグレード後にCUCMがIPアドレスまたはFQDNを使用するように設定されているかどうか

を確認するには、CUCMパブリッシャのCLIから**utils ldap config statusコマンドを使用**します。

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

この問題が発生していることを確認するには、CUCM DirSyncログでこのエラーを確認します。このエラーは、LDAPサーバがCUCMの[LDAP Authentication]設定ページのIPアドレスを使用して設定されており、LDAP証明書の[CN]フィールドと一致していないことを示します。

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

# 解決方法

[CUCM Admin] > [**System] > [LDAP] > [LDAP Authentication]ページに移動**し、LDAPサーバの設定をLDAPサーバのIPアドレスからLDAPサーバのFQDNに変更します。LDAPサーバのIPアドレスを使用する必要がある場合は、CUCMパブリッシャのCLIからこのコマンドを使用します

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

この特定の問題に関連しないFQDN検証エラーが発生する可能性があるその他の理由(FQDN):

1. CUCMで設定されているLDAPホスト名が、LDAP証明書のCNフィールド（LDAPサーバのホスト名）と一致しません。

この問題に対処するために、**[CUCM Admin] > [System] > [LDAP] > [LDAP Authentication]ページに移動**し、LDAP証明書のCNフィールドのホスト名/FQDNを使用するように**[LDAP Server Information]を変更します。**また、使用する名前がルーティング可能であり、CUCMパブリッシャのCLIから**utils network pingを使用**してCUCMから到達できることを確認します。

2. DNSロードバランサがネットワークに展開され、CUCMで設定されたLDAPサーバがDNSロードバランサを使用します。たとえば、この設定ではadaccess.example.comがポイントされ、その後、地域やその他の要因に基づいて複数のLDAPサーバ間のロードバランシングが行われます。要求に応答するLDAPサーバには、adaccess.example.com以外のFQDNを使用できます。ホスト名が一致しないため、検証に失敗します。

```
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.
```

この問題に対処するには、LDAPサーバ自体ではなく、TLS接続がロードバランサで終端するように、LDAPロードバランサ方式を変更します。これが不可能な場合は、FQDN検証を無効にし、代わりにIPアドレスを使用して検証する方法しかありません。