CUCM 10.5(2)SU2 にアップグレードの後で LDAP 問題を保護して下さい

目次

概要

この資料は 10.5(2)SU2 Cisco Unified Communications Manager （CUCM）へのアップグレードした後で問題を解決するために踏むことができるステップおよびセキュア Lightweight Directory Access Protocol （LDAP）における問題、または 9.1(2)SU3 記述したものです。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報は CUCM バージョン 10.5(2)SU2 に基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

CUCM はセキュア LDAP認証のために IP アドレスか完全修飾ドメイン名 （FQDN）を使用する

ために設定することができます。 FQDN は preffered。 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れれば **utils LDAP 構成 ip-addr** コマンドは CUCM パブリッシャの Command Line Interface （ CLI ）から実行することができます。

10.5(2)SU2 および 9.1(2)SU3 で導入される CSCun63825 のための修正前に、CUCM は厳しく LDAP への Transport Layer Security （ TLS ）接続のための FQDN 検証を実施しませんでした。 FQDN 検証は CUCM （ **CUCM Admin > システム > LDAP > LDAP認証** ）で設定されるホスト名の比較、および CUCM からの LDAPサーバへの TLS 接続の間に LDAPサーバによって示される LDAP 認証の Common Name （ CN ）または認証対象代替名（ SAN ）フィールド含みます。 このように LDAP認証が（ チェック **使用 SSL** ）有効に なり、**utils LDAP 構成 ip-addr** コマンドが発行されなくても LDAPサーバ/サーバは IP アドレスによって定義されます、認証は成功します。

10.5(2)SU2 への CUCM アップグレードが、9.1(2)SU3、またはそれ以降 バージョン、FQDN 検証実施され、FQDN を使用することであるデフォルトの動作への **utils LDAP 構成**を使用してどの変更でも戻る後。 この変更の結果は CSCux83666 の開始でした。 また、CLI コマンド **utils LDAP config ステータスは** IP アドレスか FQDN が使用されるかどうか示すために追加されます。

シナリオ 1

アップグレード LDAP認証が有効に なる前に、サーバ/サーバは IP アドレスによって、**utils** 定義されます **LDAP 構成 ip-addr** コマンドが CUCM パブリッシャの CLI で設定される。

アップグレード LDAP認証が失敗した後、CUCM パブリッシャの CLI の **utils LDAP config status コマンドは** FQDN が認証のために使用されることを示し。

シナリオ 2

アップグレード LDAP認証が有効に なる前に、サーバ/サーバは IP アドレスによって、**utils** 定義されます **LDAP 構成 ip-addr** コマンドが CUCM パブリッシャの CLI で設定されない。

アップグレード LDAP認証が失敗した後、CUCM パブリッシャの CLI の **utils LDAP config status コマンドは** FQDN が認証のために使用されることを示し。

問題

セキュア LDAP認証は CUCM の Secure Sockets Layer （ SSL ）を使用するために LDAP認証が設定され、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たら場合失敗します。

LDAP認証設定を確認するために **CUCM 管理者ページ > システム > LDAP > LDAP認証**にナビゲート し、ない FQDN LDAPサーバが IP アドレスによって定義されることを確認して下さい。 LDAPサーバが FQDN によって定義されればおよび FQDN を使用するために CUCM が設定されれば（ 確認については下記のコマンドを参照して下さい ）これは問題であることはまずない。

IP アドレスか FQDN 使用を使用するために CUCM が（アップグレードことをの後で） CUCM パブリッシャの CLI からの **utils LDAP config status コマンド**設定されればかどうか確認するため。

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

この問題に直面していること確認することはこのエラーがあるかどうか CUCM DirSync ログを点検できます。 このエラーは LDAPサーバが CUCM の LDAP認証 設定 ページの IP アドレスを使用して設定され、LDAP 認証の CN フィールドを一致することを示します。

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

解決策

CUCM Admin > システム > LDAP > LDAP認証 ページにナビゲート し、LDAPサーバの IP アドレスから LDAPサーバの FQDN に LDAPサーバ 設定を変更して下さい。 CUCM パブリッシャの CLI からのこのコマンド LDAPサーバ 使用の IP アドレスを使用する必要があれば

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

できる他の原因はこの特定の isuse に関しない FQDN 検証エラーという結果に終る場合があります:

1. CUCM で設定される LDAP ホスト名は LDAP 認証（LDAPサーバのホスト名）の CN フィールドを一致する。

この問題に対処するために **CUCM Admin > システム > LDAP > LDAP認証** ページにナビゲート し、LDAP 認証で CN フィールドからのホスト名 /FQDN を使用するために **LDAPサーバ 情報を**修正して下さい。 また使用される名前がルーティング可能で、CUCM から CUCM パブリッシャの CLI からの **utils ネットワーク PING** を使用して達することができることを、確認して下さい。

2. DNS ロードつりあい機はネットワークで配置され、CUCM で設定される LDAPサーバは DNS ロードつりあい機を使用します。 たとえば、設定は adaccess.example.com 地理学に基づいて複数の LDAPサーバ間のバランスをロードするまたは他のファクタを指します。 要求に応える LDAPサーバは adaccess.example.com 以外 FQDN がある場合があります。 これは検証エラーという結果にホスト名ミスマッチがあるので終ります。

```
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.
```

TLS 接続が LDAPサーバ自体よりもむしろ loadbalancer で、終了することこの問題に対処するために LDAP loadbalancer 方式をそのような物変更して下さい。 これが可能性のあるではない場合唯一のオプションは FQDN 検証をディセーブルにし、IP アドレスを使用して代りに検証することです。