Secure LDAP-problemen na een upgrade naar CUCM 10.5(2)SU2

Inhoud

Inleiding

Dit document beschrijft problemen met het Secure Lichtgewicht Directory Access Protocol (LDAP) na het verbeteren naar Cisco Unified Communications Manager (CUCM) 10.5(2)SU2, of 9.1(2)SU3 en de stappen die kunnen worden genomen om het probleem op te lossen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op CUCM versie 10.5(2)SU2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

CUCM kan worden ingesteld om IP-adres of FQDN-naam (Full Qualified Domain Name, FQDN) te

gebruiken voor beveiligde LDAP-verificatie. FQDN is aangedaan. Het standaardgedrag van CUCM is het gebruik van FQDN. Als het gebruik van IP-adres wordt gewenst kan de opdracht **utils ldap-bestandsindeling** worden uitgevoerd vanuit de Opdracht Line Interface (CLI) van de CUCM Publisher.

Voorafgaand aan de vaststelling voor CSCun63825, die is geïntroduceerd in 10.5(2)SU2 en 9.1(2)SU3, heeft CUCM niet strikt FQDN-validatie voor TLS-verbindingen (Transport Layer Security) met LDAP afgedwongen. FQDN-validatie omvat een vergelijking van de hostnaam in CUCM (**CUCM min > Systeem > LDAP > LDAP - verificatie)**, en het veld Gemeenschappelijke naam (CN) of Onderwerp Alternative Name (SAN) van het LDAP-certificaat dat door de LDAP-server wordt aangeboden tijdens de TLS-verbinding van CUCM naar de LDAP-server. Dus als LDAP-verificatie is ingeschakeld (controleer **gebruik van SSL)** en de LDAP server/servers zijn gedefinieerd door IP-adres, zal de authenticatie slagen zelfs als de **utils ldap configuratie ipaddr**-opdracht niet wordt uitgegeven.

Na een CUCM-upgrade naar 10.5(2)SU2, 9.1(2)SU3, of latere versies, wordt FQDN-validatie afgedwongen en alle veranderingen die **utils ldap-configuratie** gebruiken, worden teruggebracht naar het standaardgedrag, dat wil zeggen het gebruik van FQDN. Het resultaat van deze verandering was het openen van CSCux83666. Tevens wordt de CLI opdracht **utils ldap configuratie status** toegevoegd om aan te tonen of IP adres of FQDN wordt gebruikt.

Scenario 1

Voordat de upgrade LDAP verificatie is ingeschakeld, worden server/servers gedefinieerd door IP-adres, wordt de opdracht **utils** ldap-**bestand** op de CLI van de CUCM Publisher ingesteld.

Nadat de upgrade LDAP verificatie mislukt, en de opdracht **titer ldap-configuratie** op de CLI van de CUCM Publisher aantoont dat FQDN voor verificatie wordt gebruikt.

Scenario 2

Voordat de upgrade LDAP verificatie is ingeschakeld, worden server/servers gedefinieerd door IP-adres, wordt de opdracht utils **ldap-id** niet ingesteld op de CLI van de CUCM-uitgever.

Nadat de upgrade LDAP verificatie mislukt, en de opdracht **titer ldap-configuratie** op de CLI van de CUCM Publisher aantoont dat FQDN voor verificatie wordt gebruikt.

Probleem

Secure LDAP-verificatie faalt indien de authenticatie van de LMP is ingesteld om Secure Socket Layer (SSL) op CUCM te gebruiken en de LDAP server/servers zijn ingesteld met behulp van IP-adres voorafgaand aan de upgrade.

Om de verificatie-instellingen van de LDAP te bevestigen, navigeer naar de **CUCM Admin-pagina > Systeem > LDAP > LDAP-verificatie** en controleer of de LDAP-servers zijn gedefinieerd door IP-adres, niet door FQDN. Als uw LDAP server wordt gedefinieerd door FQDN en de CUCM is ingesteld om FQDN te gebruiken (zie opdracht hieronder voor verificatie) is het onwaarschijnlijk dat dit uw probleem is.

Om te verifiëren of CUCM (na een upgrade) is geconfigureerd om IP-adres te gebruiken of FQDN gebruikt de opdracht **utils-lidap-configuratie** van de CLI van de CUCM-uitgever.

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

Om te controleren of u dit probleem ondervindt kunt u de logbestanden van CUCM DirSync op deze fout controleren. Deze fout geeft aan dat de LDAP-server is ingesteld met behulp van een IP-adres op de LBP-verificatiepagina in CUCM en niet overeenkomt met het GN-veld in het LDAP-certificaat.

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

Oplossing

Navigeer naar de pagina **CUCM Admin > System > LDAP > LDAP verificatie** en wijzig de configuratie van de LDAP server van het IP-adres van de LDAP server naar de FQDN van de LDAP server. Als u het IP-adres van de LDAP-server moet gebruiken, gebruikt u deze opdracht vanuit de CLI van de CUCM Publisher

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

Andere redenen die kunnen resulteren in FQDN-validatie die geen verband houdt met dit specifieke probleem:

1. De LGO-hostname die in CUCM is ingesteld, komt niet overeen met het GN-veld in het LDAP-certificaat (hostname van de LDAP-server).

Om deze kwestie aan te pakken navigeer naar de **CUCM Admin > System > LDAP > LDAP verificatiepagina** en wijzig de **LDAP serverinformatie** om de hostname/FQDN te gebruiken vanuit het GN-veld in het LDAP-certificaat. Controleer ook dat de gebruikte naam routeerbaar is en vanuit CUCM kan worden bereikt door gebruik te maken van **utils Network ping** van de CLI van de CUCM-uitgever.

2. Er wordt een DNS-taakverdeling in het netwerk geïmplementeerd en de LDAP-server in CUCM gebruikt de DNS-taakverdeling. De configuratie wijst bijvoorbeeld op adaccess.voorbeeld.com, dat dan de balansen tussen verschillende LDAP-servers vult op basis van geografie of andere factoren. De LDAP server die het verzoek beantwoordt kan een FQDN anders dan adaccess.voorbeeld.com hebben. Dit resulteert in een validatie-storing omdat er een hostname-fout optreedt.

```
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.
```

Om deze kwestie aan te pakken, moet het LVP-belastingsysteem zodanig worden gewijzigd dat de TLS-verbinding bij de loadstabilisator wordt afgesloten in plaats van de LDAP-server zelf. Als dit niet mogelijk is, is de enige optie om FQDN-validatie uit te schakelen en in plaats daarvan het gebruik van IP-adres te valideren.