Problemi LDAP sicuri dopo un aggiornamento a CUCM 10.5(2)SU2

Sommario

Introduzione

In questo documento vengono descritti i problemi relativi al protocollo LDAP (Lightweight Directory Access Protocol) sicuro dopo l'aggiornamento a Cisco Unified Communications Manager (CUCM) versione 10.5(2)SU2 o 9.1(2)SU3 e le operazioni che è possibile eseguire per risolvere il problema.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il riferimento delle informazioni contenute in questo documento è CUCM versione 10.5(2)SU2.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

CUCM può essere configurato per utilizzare l'indirizzo IP o il nome di dominio completo (FQDN) per l'autenticazione LDAP sicura. FQDN preferito. Il comportamento predefinito di CUCM prevede l'utilizzo di FQDN. Se si desidera utilizzare l'indirizzo IP, è possibile eseguire il comando **utils ldap config ipaddr** dall'interfaccia della riga di comando (CLI) di CUCM Publisher.

Prima della correzione per CSCun63825 introdotta nelle versioni 10.5(2)SU2 e 9.1(2)SU3, CUCM non applicava rigorosamente la convalida FQDN per le connessioni Transport Layer Security (TLS) a LDAP. La convalida FQDN implica un confronto tra il nome host configurato in CUCM (**CUCM Admin > Sistema > LDAP > Autenticazione LDAP)** e il campo Nome comune (CN) o Nome alternativo soggetto (SAN) del certificato LDAP presentato dal server LDAP durante la connessione TLS da CUCM al server LDAP. Pertanto, se l'autenticazione LDAP è abilitata (selezionare **Usa SSL)** e i server LDAP sono definiti dall'indirizzo IP, l'autenticazione avrà esito positivo anche se il comando **utils ldap config ipaddr** non è stato emesso.

Dopo l'aggiornamento di CUCM alla versione 10.5(2)SU2, 9.1(2)SU3 o successive, viene applicata la convalida del nome di dominio completo e tutte le modifiche che utilizzano la **configurazione ldap** vengono ripristinate al comportamento predefinito, ovvero utilizzare il nome di dominio completo. Il risultato di questa modifica è stata l'apertura di CSCux83666. Inoltre, il comando CLI **utilizza lo stato di configurazione ldap** per visualizzare se è in uso un indirizzo IP o un FQDN.

Scenario 1

Prima di abilitare l'autenticazione LDAP per l'aggiornamento, i server sono definiti dall'indirizzo IP, il comando **utils ldap config ipaddr** viene configurato sulla CLI dell'editore CUCM.

Se l'aggiornamento dell'autenticazione LDAP ha esito negativo e il comando **ldap config status** nella CLI dell'autore CUCM indica che per l'autenticazione viene utilizzato il nome di dominio completo (FQDN).

Scenario 2

Prima di abilitare l'autenticazione LDAP per l'aggiornamento, i server sono definiti dall'indirizzo IP, il comando **utils ldap config ipaddr** non è configurato sulla CLI dell'editore CUCM.

Se l'aggiornamento dell'autenticazione LDAP ha esito negativo e il comando **ldap config status** nella CLI dell'autore CUCM indica che per l'autenticazione viene utilizzato il nome di dominio completo (FQDN).

Problema

L'autenticazione LDAP sicura non riesce se l'autenticazione LDAP è configurata per l'utilizzo di Secure Sockets Layer (SSL) su CUCM e se i server LDAP sono stati configurati utilizzando l'indirizzo IP prima dell'aggiornamento.

Per confermare le impostazioni di autenticazione LDAP, passare alla **pagina Amministratore CUCM > Sistema > LDAP > Autenticazione LDAP** e verificare che i server LDAP siano definiti dall'indirizzo IP e non da FQDN. Se il server LDAP è definito da FQDN e CUCM è configurato per l'utilizzo di FQDN (vedere il comando seguente per la verifica), è improbabile che si tratti di un problema.

Per verificare se CUCM (dopo un aggiornamento) è configurato per utilizzare l'indirizzo IP o il nome di dominio completo, usare il comando **utils ldap config status** dalla CLI dell'editore CUCM.

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

Per verificare se il problema si è verificato, è possibile controllare la presenza di questo errore nei registri DirSync di CUCM. Questo errore indica che il server LDAP è configurato utilizzando un indirizzo IP nella pagina di configurazione dell'autenticazione LDAP in CUCM e non corrisponde al campo CN nel certificato LDAP.

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

Soluzione

Passare alla pagina **CUCM Admin > Sistema > LDAP > Autenticazione LDAP** e modificare la configurazione del server LDAP dall'indirizzo IP del server LDAP al nome FQDN del server LDAP. Se è necessario utilizzare l'indirizzo IP del server LDAP, utilizzare questo comando dalla CLI di CUCM Publisher

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

Altri motivi che possono causare errori di convalida del nome di dominio completo non correlati a questo problema specifico:

1. Il nome host LDAP configurato in CUCM non corrisponde al campo CN nel certificato LDAP (nome host del server LDAP).

Per risolvere questo problema, passare alla pagina **CUCM Admin > Sistema > LDAP >Autenticazione LDAP** e modificare **LDAP Server Information** per utilizzare il nome host/FQDN dal campo CN nel certificato LDAP. Verificare inoltre che il nome utilizzato sia instradabile e possa essere raggiunto da CUCM utilizzando **utils network ping** from the CLI of the CUCM publisher.

2. Nella rete viene distribuito un load balancer DNS e il server LDAP configurato in CUCM utilizza il load balancer DNS. Ad esempio, la configurazione punta a adaccess.example.com, che quindi carica i bilanciamenti tra diversi server LDAP in base alla geografia o ad altri fattori. Il server LDAP che risponde alla richiesta può avere un FQDN diverso da adaccess.example.com. La convalida non riesce in quanto il nome host non corrisponde.

```
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.
```

Per risolvere questo problema, modificare lo schema del loadbalancer LDAP in modo che la connessione TLS termini nel loadbalancer, anziché nel server LDAP stesso. Se non è possibile, l'unica opzione è disabilitare la convalida del nome di dominio completo e convalidare utilizzando l'indirizzo IP.