Problemas LDAP seguros después de una actualización a CUCM 10.5(2)SU2

Contenido

Introducción

Este documento describe los problemas con el protocolo ligero de acceso a directorios (LDAP) seguro después de actualizar a Cisco Unified Communications Manager (CUCM) 10.5(2)SU2 o 9.1(2)SU3 y los pasos que se pueden realizar para resolver el problema.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en la versión 10.5(2)SU2 de CUCM.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

CUCM se puede configurar para utilizar la dirección IP o el nombre de dominio completo (FQDN) para la autenticación LDAP segura. Se prefiere FQDN. El comportamiento predeterminado de

CUCM es utilizar FQDN. Si se desea utilizar la dirección IP, el comando **utils ldap config ipaddr** se puede ejecutar desde la interfaz de línea de comandos (CLI) del editor de CUCM.

Antes de la corrección para CSCun63825 que se introduce en 10.5(2)SU2 y 9.1(2)SU3, CUCM no aplicaba estrictamente la validación FQDN para las conexiones de seguridad de la capa de transporte (TLS) a LDAP. La validación de FQDN implica una comparación del nombre de host configurado en CUCM (**CUCM Admin > System > LDAP > LDAP Authentication)**, y el campo Common Name (CN) o Subject Alternative Name (SAN) del certificado LDAP presentado por el servidor LDAP durante la conexión TLS de CUCM al servidor LDAP. Por lo tanto, si la autenticación LDAP está habilitada (verifique **utilizar SSL)** y el servidor/servidores LDAP están definidos por la dirección IP, la autenticación se realizará correctamente incluso si el **comando utils ldap config ipaddr** no se ejecuta.

Después de una actualización de CUCM a 10.5(2)SU2, 9.1(2)SU3 o versiones posteriores, se aplica la validación de FQDN y cualquier cambio que use **utils ldap config** se revierte al comportamiento predeterminado, que es utilizar FQDN. El resultado de este cambio fue la apertura de CSCux83666. Además, el comando CLI **utils ldap config status** se agrega para mostrar si se está utilizando la dirección IP o el FQDN.

Escenario 1

Antes de que se active la autenticación LDAP de actualización, los servidores/servidores se definen por dirección IP, el comando **utils ldap config ipaddr** se configura en la CLI del editor de CUCM.

Después de que la actualización de la autenticación LDAP falle, y el **comando utils ldap config status** en la CLI del editor de CUCM muestra que el FQDN se utiliza para la autenticación.

Escenario 2

Antes de que se active la autenticación LDAP de actualización, los servidores/servidores se definen por dirección IP, el comando **utils ldap config ipaddr** no se configura en la CLI del editor de CUCM.

Después de que la actualización de la autenticación LDAP falle, y el **comando utils ldap config status** en la CLI del editor de CUCM muestra que el FQDN se utiliza para la autenticación.

Problema

La autenticación LDAP segura falla si la autenticación LDAP se configura para utilizar Secure Sockets Layer (SSL) en CUCM y el servidor/servidores LDAP se configuró usando la dirección IP antes de la actualización.

Para confirmar la configuración de autenticación LDAP, navegue a la **página de administración de CUCM > Sistema > LDAP > Autenticación LDAP** y verifique que los servidores LDAP estén definidos por la dirección IP, no por FQDN. Si el FQDN define su servidor LDAP y CUCM está configurado para utilizar FQDN (consulte el siguiente comando para la verificación), es poco probable que este sea su problema.

Para verificar si CUCM (después de una actualización) está configurado para utilizar la dirección IP o el FQDN, utilice el comando **utils ldap config status** de la CLI del editor de CUCM.

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

Para verificar que está experimentando este problema, puede verificar los registros de CUCM DirSync para este error. Este error indica que el servidor LDAP está configurado usando una dirección IP en la página de configuración de autenticación LDAP en CUCM y no coincide con el campo CN en el certificado LDAP.

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

Solución

Navegue hasta la página **CUCM Admin > System > LDAP > LDAP Authentication** y cambie la configuración del servidor LDAP desde la dirección IP del servidor LDAP al FQDN del servidor LDAP. Si debe utilizar la dirección IP del servidor LDAP, utilice este comando desde la CLI del editor de CUCM

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

Otras razones que pueden dar lugar a una falla de validación de FQDN no relacionada con este problema en particular :

1. El nombre de host LDAP configurado en CUCM no coincide con el campo CN en el certificado LDAP (nombre de host del servidor LDAP).

Para resolver este problema, navegue a la **página** de **CUCM Admin > System > LDAP > LDAP Authentication** y modifique la **Información del Servidor LDAP** para utilizar el nombre de host/FQDN del Campo CN en el certificado LDAP. Además, verifique que el nombre utilizado sea enrutable y se pueda alcanzar desde CUCM usando **ping de red de utilidades** desde la CLI del editor de CUCM.

2. Un equilibrador de carga DNS se implementa en la red y el servidor LDAP configurado en CUCM utiliza el equilibrador de carga DNS. Por ejemplo, la configuración apunta a adaccess.example.com, que luego equilibra la carga entre varios servidores LDAP basados en la geografía, u otros factores. El servidor LDAP que responde a la solicitud puede tener un FQDN que no sea adaccess.example.com. Esto produce un error de validación, ya que hay una discordancia de nombre de host.

```
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.
```

Para resolver este problema, cambie el esquema de balanceador de carga LDAP de tal manera que la conexión TLS termine en el balanceador de carga, en lugar del servidor LDAP mismo. Si esto no es posible, la única opción es inhabilitar la validación de FQDN y, en su lugar, validar usando la dirección IP.