Asegure los problemas LDAP después de una actualización a CUCM 10.5(2)SU2

Contenido

Introducción

Este documento describe los problemas con el Lightweight Directory Access Protocol (LDAP) seguro después de actualizar a las Comunicaciones unificadas de Cisco al administrador (CUCM) 10.5(2)SU2, o 9.1(2)SU3 y las medidas que se puedan tomar para resolver el problema.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

CUCM se puede configurar para utilizar la dirección IP o el nombre de dominio completo (FQDN)

para la autenticación ldap segura. Se prefiere el FQDN. El comportamiento predeterminado de CUCM es utilizar el FQDN. Si el uso de la dirección IP se desea el **comando ipaddr de los config del ldap del utils** puede ser funcionado con del comando line interface(cli) del CUCM Publisher.

Antes del arreglo para CSCun63825 que se introduce en 10.5(2)SU2 y 9.1(2)SU3, CUCM no aplicó estrictamente la validación FQDN para las conexiones de Transport Layer Security (TLS) al LDAP. La validación FQDN implica una comparación del nombre de host configurado en CUCM (**CUCM Admin > sistema > LDAP > autenticación ldap)**, y el Common Name (CN) o el campo alternativo sujeto del nombre (SAN) del certificado LDAP presentado por el servidor LDAP durante la conexión TLS de CUCM al servidor LDAP. Así pues, si se habilita la autenticación ldap (el **uso SSL del** control) y la dirección IP define al servidor LDAP/los servidores, la autenticación tendrá éxito incluso si no publican el **comando ipaddr de los config del ldap del utils**.

Después de que una actualización CUCM a 10.5(2)SU2, 9.1(2)SU3, o versiones posteriores, validación FQDN se aplique y cualquier cambio usando los **config del ldap del utils** se invierte al comportamiento predeterminado, que es utilizar el FQDN. El resultado de este cambio era la apertura de CSCux83666. También, el **estatus de los config del ldap del utils del** comando CLI se agrega para mostrar si se está utilizando la dirección IP o el FQDN.

Escenario 1

Antes de que se habilite la autenticación ldap de la actualización, el servidor/los servidores es definido por la dirección IP, el **comando ipaddr de los config del ldap del utils** se configura en el CLI del CUCM Publisher.

Después de que la autenticación ldap de la actualización falle, y el **comando status de los config del ldap del utils** en el CLI del CUCM Publisher muestra que el FQDN está utilizado para la autenticación.

Escenario 2

Antes de que se habilite la autenticación ldap de la actualización, el servidor/los servidores es definido por la dirección IP, el **comando ipaddr de los config del ldap del utils** no se configura en el CLI del CUCM Publisher.

Después de que la autenticación ldap de la actualización falle, y el **comando status de los config del ldap del utils** en el CLI del CUCM Publisher muestra que el FQDN está utilizado para la autenticación.

Problema

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

Para confirmar las configuraciones de la autenticación ldap navegue a la **página de administración > al sistema > al LDAP > a la autenticación ldap CUCM** y verifique que la dirección IP definen a los servidores LDAP, no FQDN. Si el FQDN define a su servidor LDAP y el CUCM se configura para utilizar el FQDN (véase el comando abajo para la verificación) que es inverosímil que éste es su problema.

Para verificar si CUCM (después de una actualización) se configura para utilizar la dirección IP o el uso FQDN el **comando status de los config del ldap del utils del** CLI del editor CUCM.

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

Para verificarle que usted esté experimentando este problema puede marcar los registros CUCM DirSync para este error. Este error indica que configuran al servidor LDAP usando una dirección IP en la página de configuración de la autenticación ldap en CUCM y no hace juego 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 Al **CUCM Admin > sistema > LDAP >** página de la **autenticación ldap** y cambie la configuración de servidor LDAP de la dirección IP del servidor LDAP al FQDN del servidor LDAP. Si usted debe utilizar la dirección IP del uso del servidor LDAP este comando del CLI del CUCM Publisher

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

Otras razones que pueden poder el resultado en error de la validación FQDN no relacionado con este isuse determinado:

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

Para abordar este problema navegue Al **CUCM Admin > sistema > LDAP >** página de la **autenticación ldap** y modifique la **información del servidor LDAP** para utilizar el hostname/FQDN del campo CN en el certificado LDAP. También, verifique que el nombre usado sea routable y se pueda alcanzar de CUCM usando el **ping de la red del utils del** CLI del editor CUCM.

2. Un balanceador de la carga DNS se despliega en la red y el servidor LDAP configurado en CUCM utiliza el balanceador de la carga DNS. Por ejemplo, la configuración señala a adaccess.example.com, que entonces cargan los equilibrios entre varios servidores LDAP basados en la geografía, o a otros factores. El servidor LDAP que contesta a la petición puede tener un FQDN con excepción de adaccess.example.com. Esto da lugar a un error de la validación puesto que hay una discordancía del 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 abordar este problema cambie el esquema tales que la conexión TLS termina en el loadbalancer, bastante que el servidor LDAP sí mismo del loadbalancer LDAP. Si esto no es posible la única opción es inhabilitar la validación FQDN y en lugar de otro validarla usando la

dirección IP.