Problemas de LDAP seguros após uma atualização para CUCM 10.5(2)SU2

Contents

Introduction

Este documento descreve problemas com o protocolo LDAP (Lightweight Diretory Access Protocol) seguro após a atualização para o Cisco Unified Communications Manager (CUCM) 10.5(2)SU2 ou 9.1(2)SU3 e as etapas que podem ser tomadas para resolver o problema.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas na versão 10.5(2)SU2 do 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.

Informações de Apoio

O CUCM pode ser configurado para usar o endereço IP ou o nome de domínio totalmente qualificado (FQDN) para autenticação LDAP segura. O FQDN é preferido. O comportamento

padrão do CUCM é usar o FQDN. Se o uso do endereço IP for desejado, o comando **utils ldap config ipaddr** pode ser executado a partir da CLI (Command Line Interface, interface de linha de comando) do Editor do CUCM.

Antes da correção para CSCun63825 apresentada em 10.5(2)SU2 e 9.1(2)SU3, o CUCM não aplicou rigorosamente a validação de FQDN para conexões TLS (Transport Layer Security) para LDAP. A validação de FQDN envolve uma comparação do nome de host configurado no CUCM (**CUCM Admin > Sistema > LDAP > Autenticação LDAP)**, e o campo Common Name (CN) ou Subject Alternative Name (SAN) do certificado LDAP apresentado pelo servidor LDAP durante a conexão TLS do CUCM ao servidor LDAP. Portanto, se a autenticação LDAP estiver habilitada (marque **usar SSL)** e o servidor/servidores LDAP forem definidos pelo endereço IP, a autenticação terá êxito mesmo se o comando **utils ldap config ipaddr** não for emitido.

Após uma atualização do CUCM para 10.5(2)SU2, 9.1(2)SU3 ou versões posteriores, a validação do FQDN é aplicada e qualquer alteração usando **utils ldap config** é revertida para o comportamento padrão, que é usar FQDN. O resultado dessa mudança foi a abertura do CSCux83666. Além disso, o comando CLI **utils ldap config status** é adicionado para mostrar se o endereço IP ou FQDN está sendo usado.

Cenário 1

Antes que a Autenticação LDAP de atualização seja habilitada, o servidor/servidores são definidos pelo endereço IP, o comando **utils ldap config ipaddr** é configurado na CLI do Editor do CUCM.

Após a atualização da autenticação LDAP falhar, e o comando **utils ldap config status** na CLI do Editor do CUCM mostra que o FQDN é usado para autenticação.

Cenário 2

Antes que a Autenticação LDAP de atualização seja ativada, o servidor/servidores são definidos pelo endereço IP, o comando **utils ldap config ipaddr** não está configurado na CLI do Editor do CUCM.

Após a atualização da autenticação LDAP falhar, e o comando **utils ldap config status** na CLI do Editor do CUCM mostra que o FQDN é usado para autenticação.

Problema

A autenticação LDAP segura falha se a autenticação LDAP estiver configurada para usar SSL (Secure Sockets Layer) no CUCM e o servidor/servidores LDAP tiver sido configurado usando o endereço IP antes da atualização.

Para confirmar as configurações de autenticação LDAP, navegue até a **página Admin do CUCM > Sistema > LDAP > Autenticação LDAP** e verifique se os servidores LDAP estão definidos pelo endereço IP, não FQDN. Se o servidor LDAP for definido pelo FQDN e o CUCM estiver configurado para usar o FQDN (consulte o comando abaixo para verificar), é improvável que esse seja o seu problema.

Para verificar se o CUCM (após uma atualização) está configurado para usar o endereço IP ou FQDN, use o comando **utils ldap config status** da CLI do editor do CUCM.

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

Para verificar se esse problema está ocorrendo, você pode verificar os registros do CUCM DirSync em busca desse erro. Esse erro indica que o servidor LDAP está configurado usando um endereço IP na página de configuração de autenticação LDAP no CUCM e não corresponde ao campo CN no certificado LDAP.

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

Solução

Navegue até a página **CUCM Admin > Sistema > LDAP > Autenticação LDAP** e altere a configuração do servidor LDAP do endereço IP do servidor LDAP para o FQDN do servidor LDAP. Se você precisar usar o endereço IP do servidor LDAP, use este comando da CLI do Editor do CUCM

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

Outros motivos que podem resultar em falha de validação de FQDN não relacionados a este problema específico :

1. O nome de host LDAP configurado no CUCM não corresponde ao campo CN no certificado LDAP (nome de host do servidor LDAP).

Para resolver esse problema, navegue até a página **Administrador do CUCM > Sistema > LDAP > Autenticação LDAP** e modifique as **Informações do Servidor LDAP** para usar o nome de host/FQDN do Campo CN no certificado LDAP. Além disso, verifique se o nome usado é roteável e pode ser acessado do CUCM usando **utils network ping** da CLI do editor do CUCM.

2. Um balanceador de carga DNS é implantado na rede e o servidor LDAP configurado no CUCM usa o balanceador de carga DNS. Por exemplo, a configuração aponta para adaccess.example.com, que então equilibra a carga entre vários servidores LDAP com base na geografia ou outros fatores. O servidor LDAP que responde à solicitação pode ter um FQDN diferente de adaccess.example.com. Isso resulta em uma falha de validação, pois há uma incompatibilidade de nome 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 esse problema, altere o esquema do balanceador de carga LDAP de modo que a conexão TLS termine no balanceador de carga, em vez do servidor LDAP em si. Se isso não for possível, a única opção é desabilitar a validação de FQDN e, em vez disso, validar usando o endereço IP.