Fixe problemas LDAP após uma elevação a CUCM 10.5(2)SU2

Índice

Introdução

Este documento descreve problemas com o Lightweight Directory Access Protocol (LDAP) seguro após ter promovido às comunicações unificadas de Cisco o gerente (CUCM) 10.5(2)SU2, ou 9.1(2)SU3 e as etapas que podem ser tomados para resolver a edição.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

A informação neste documento é baseada na versão 10.5(2)SU2 CUCM.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

CUCM pode ser configurado para usar o endereço IP de Um ou Mais Servidores Cisco ICM NT

ou o nome de domínio totalmente qualificado (FQDN) para a autenticação LDAP segura. O FQDN é preferido. O comportamento padrão de CUCM é usar o FQDN. Se o uso do endereço IP de Um ou Mais Servidores Cisco ICM NT é desejado o **comando ipaddr da configuração do ldap dos utils** pode ser executado do comando line interface(cli) do editor CUCM.

Antes do reparo para CSCun63825 que é introduzido em 10.5(2)SU2 e em 9.1(2)SU3, CUCM não reforçou restritamente a validação FQDN para conexões do Transport Layer Security (TLS) ao LDAP. A validação FQDN envolve uma comparação do hostname configurado em CUCM (**CUCM Admin > sistema > LDAP > autenticação LDAP)**, e o Common Name (CN) ou o campo alternativo sujeito do nome (SAN) do certificado LDAP apresentado pelo servidor ldap durante a conexão TLS de CUCM ao servidor ldap. Assim, se a autenticação LDAP é permitida (o **uso SSL da** verificação**)** e o servidor ldap/server é definido pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, a autenticação sucederá mesmo se o **comando ipaddr da configuração do ldap dos utils** não é emitido.

Depois que uma elevação CUCM a 10.5(2)SU2, a 9.1(2)SU3, ou a umas versões mais atrasadas, validação FQDN é reforçada e alguma muda usando **utils a configuração do ldap que** é revertida ao comportamento padrão, que é usar o FQDN. O resultado desta mudança era a abertura de CSCux83666. Também, o **estado da configuração do ldap dos utils do** comando CLI é adicionado para mostrar se o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o FQDN estão sendo usados.

Cenário 1

Antes que a autenticação LDAP da elevação esteja permitida, o server/server está definido pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, os **utils o comando ipaddr da configuração que do ldap** é configurado no CLI do editor CUCM.

Depois que a autenticação LDAP da elevação falha, e o **comando status da configuração do ldap dos utils no** CLI do editor CUCM mostra que o FQDN está usado para a autenticação.

Cenário 2

Antes que a autenticação LDAP da elevação esteja permitida, o server/server está definido pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, os **utils o comando ipaddr da configuração que do ldap** não é configurado no CLI do editor CUCM.

Depois que a autenticação LDAP da elevação falha, e o **comando status da configuração do ldap dos utils no** CLI do editor CUCM mostra que o FQDN está usado para a autenticação.

Problema

A autenticação LDAP segura falha se a autenticação LDAP está configurada para usar o secure sockets layer (SSL) em CUCM e o servidor ldap/server esteve configurado usando o endereço IP de Um ou Mais Servidores Cisco ICM NT antes da elevação.

A fim confirmar os ajustes da autenticação LDAP navegue à **página de admin > ao sistema > ao LDAP > à autenticação LDAP CUCM** e verifique que os servidores ldap estão definidos pelo endereço IP de Um ou Mais Servidores Cisco ICM NT, não FQDN. Se seu servidor ldap está definido pelo FQDN e o CUCM está configurado para usar o FQDN (veja o comando abaixo para a verificação) que é improvável que esta é sua edição.

A fim verificar se CUCM (após uma elevação) é configurado para usar o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o uso FQDN o **comando status da configuração do ldap dos utils do** CLI do editor CUCM.

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

A fim verificá-lo que você está experimentando este problema pode verificar os logs CUCM DirSync para ver se há este erro. Este erro indica que o servidor ldap está configurado usando um endereço IP de Um ou Mais Servidores Cisco ICM NT na página de configuração da autenticação LDAP em CUCM e não combina o campo do 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 Ao **CUCM Admin > sistema > LDAP >** página da **autenticação LDAP** e mude a configuração de servidor ldap do endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor ldap ao FQDN do servidor ldap. Se você deve usar o endereço IP de Um ou Mais Servidores Cisco ICM NT do uso do servidor ldap este comando do CLI do editor CUCM

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

Outras razões que podem enlatar o resultado na falha da validação FQDN não relativa a este isuse particular:

1. O hostname LDAP configurado em CUCM não combina o campo do CN no certificado LDAP (hostname do servidor ldap).

A fim endereçar esta edição navegue Ao **CUCM Admin > sistema > LDAP >** página da **autenticação LDAP** e altere a **informação do servidor ldap** para usar o hostname/FQDN do campo do CN no certificado LDAP. Também, verifique que o nome usado é roteável e pode ser alcançado de CUCM usando o **sibilo da rede dos utils do** CLI do editor CUCM.

2. Um equilibrador da carga DNS é distribuído na rede e o servidor ldap configurado em CUCM usa o equilibrador da carga DNS. Por exemplo, a configuração aponta a adaccess.example.com, que carregam então equilíbrios entre diversos servidores ldap baseados na geografia, ou a outros fatores. O servidor ldap que responde ao pedido pode ter um FQDN a não ser adaccess.example.com. Isto conduz a uma falha da validação desde que há uma má combinação do hostname.

```
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.
```

A fim endereçar esta edição mude o esquema do loadbalancer LDAP tais que a conexão TLS termina no loadbalancer, um pouco do que o servidor ldap próprio. Se isto não é possível a única opção é desabilitar a validação FQDN e validá-la pelo contrário usando o endereço IP de Um ou

Mais Servidores Cisco ICM NT.