Безопасные проблемы LDAP после обновления к CUCM 10.5 (2) SU2

Содержание

Введение

Этот документ описывает проблемы с безопасным Протоколом LDAP после обновления к Cisco Unified Communications Manager (CUCM) 10.5 (2) SU2, или 9.1 (2) SU3 и шаги, которые могут быть сделаны для решения вопроса.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на версии 10.5 (2) SU2 CUCM.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

CUCM может быть настроен для использования или IP-адреса или Полного доменного

имени (FQDN) для безопасной проверки подлинности LDAP. FQDN предпочтен. Поведение по умолчанию CUCM должно использовать FQDN. Если использование IP-адреса желаемо, чтобы команда **ipaddr config ldap utils** могла быть выполнена от Интерфейса командной строки (CLI) Издателя CUCM.

До исправления для CSCun63825 , который представлен в 10.5 (2) SU2 и 9.1 (2) SU3, CUCM строго не принуждал проверку FQDN для соединений Transport Layer Security (TLS) с LDAP. Проверка FQDN включает сравнение имени хоста, настроенного в CUCM (**Admin CUCM > Система> LDAP> Проверка подлинности LDAP)**, и Общее имя (CN) или поле альтернативного имени субъекта (SAN) сертификата LDAP, представленного Сервером LDAP во время TLS подключение от CUCM до Сервера LDAP. Так, если Проверка подлинности LDAP будет включена (проверьте **SSL использования)**, и Сервер LDAP / серверы определен IP-адресом, то аутентификация успешно выполнится, даже если не будет выполнена команда **ipaddr config ldap utils**.

После обновления CUCM к 10.5 (2) SU2, 9.1 (2) принужден SU3 или более поздние версии, проверка FQDN, и любые изменения с помощью **config ldap utils** вернулись к поведению по умолчанию, которое должно использовать FQDN. Результатом этого изменения было открытие CSCux83666. Кроме того, **статус config ldap utils** команды CLI добавлен, чтобы показать, используются ли IP-адрес или FQDN.

Сценарий 1

Прежде чем Проверка подлинности LDAP обновления включена, сервер/серверы определены IP-адресом, команда **ipaddr config ldap utils** настроена на CLI Издателя CUCM.

После сбоев Проверки подлинности LDAP обновления и команды **статуса config ldap utils** на CLI Издателя CUCM показывает, что FQDN используется для аутентификации.

Сценарий 2

Прежде чем Проверка подлинности LDAP обновления включена, сервер/серверы определены IP-адресом, команда **ipaddr config ldap utils** не настроена на CLI Издателя CUCM.

После сбоев Проверки подлинности LDAP обновления и команды **статуса config ldap utils** на CLI Издателя CUCM показывает, что FQDN используется для аутентификации.

Проблема

Безопасная проверка подлинности LDAP отказывает, если проверка подлинности LDAP настроена для использования Уровня защищенных сокетов (SSL) на CUCM, и Сервер LDAP / серверы были настроены с помощью IP-адреса до обновления.

Чтобы подтвердить, что параметры настройки проверки подлинности LDAP перешли к **Странице администратора CUCM> Система> LDAP> Проверка подлинности LDAP** и проверяют, что Серверы LDAP определены IP-адресом, не FQDN. Если ваш Сервер LDAP определен FQDN, и CUCM настроен для использования FQDN (см. команду ниже для проверки), маловероятно , что это - проблема.

Чтобы проверить, настроен ли CUCM (после обновления) для использования IP-адреса, или FQDN используют команду **статуса config ldap utils** от CLI издателя CUCM.

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

Чтобы проверить испытание этой проблемы, можно проверить журналы CUCM DirSync для этой ошибки. Эта ошибка указывает, что Сервер LDAP настроен с помощью IP-адреса на странице конфигурации Проверки подлинности LDAP в CUCM, и это не совпадает с полем CN в сертификате LDAP.

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

Решение

Перейдите к странице **CUCM Admin> System> LDAP> LDAP Authentication** и измените конфигурацию Сервера LDAP от IP-адреса Сервера LDAP к FQDN Сервера LDAP. Если необходимо использовать IP-адрес использования Сервера LDAP эта команда от CLI Издателя CUCM

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

Другие причины, что банка может привести к сбою проверки FQDN, не отнесенному к этому определенному isuse:

1. Имя хоста LDAP, настроенное в CUCM, не совпадает с полем CN в сертификате LDAP (имя хоста Сервера LDAP).

Для решения этой проблемы, перешли к странице **CUCM Admin> System> LDAP> LDAP Authentication** и модифицируют **информацию о Сервере LDAP** для использования hostname/FQDN от Поля CN в сертификате LDAP. Кроме того, проверьте, что используемое название маршрутизуемо и может быть достигнуто от CUCM использование **сети ping utils** от CLI издателя CUCM.

2. Балансировщик Загрузки DNS развернут в сети, и Сервер LDAP, настроенный в CUCM, использует Балансировщик Загрузки DNS. Например, конфигурация указывает к adaccess. пример. com, который тогда балансирует нагрузку между несколькими Серверами LDAP на основе географии или другими факторами. Сервер LDAP, который отвечает на запрос, может иметь FQDN кроме adaccess. пример. com. Это приводит к сбою проверки, так как существует несоответствие имени хоста.

```
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.
```

Для адресации к этому изменению проблемы, LDAP loadbalancer интригует таким образом, что TLS подключение завершается в loadbalancer, а не самом Сервере LDAP. Если это не возможно, единственная опция должна отключить проверку FQDN и вместо этого проверить

IP-адрес использования.