Содержание

Введение

Этот документ описывает, как предотвратить ситуацию с Версией 8.0 (1) Cisco Unified Communications Manager (CUCM), где тысячи телефонов должны иметь свои файлы Начального трастового списка (ITL), вручную удаленные.

Общие сведения

С Версией 8.0 (1) CUCM были представлены новая функция Безопасности по умолчанию (SBD) и использование файлов ITL. С этой новой характеристикой меры должны быть приняты при перемещении телефонов между другими кластерами CUCM. Если вы не выполняете надлежащие шаги, возможно встретиться с ситуацией, где тысячам телефонов нужно было вручную удалить их файлы ITL. Телефоны, которые поддерживают новые файлы ITL, загружают особый файл от своего сервера TFTP CUCM. Как только файл ITL установлен по телефону, все будущие файлы конфигурации и обновления файла ITL должны быть также:

- Подписанный Серверным сертификатом CCM+TFTP, который в настоящее время устанавливается в файле Списка надежных сертификатов (CTL) телефона (если кластерная безопасность с CTL включена).
- Подписанный Серверным сертификатом CCM+TFTP, который установлен в файле ITL телефона.
- Подписанный сертификатом, который существует в одном из хранилищ сертификата служб проверки доверия (TVS) Сервера CUCM, которые перечислены в файле ITL.

С новой функциональностью безопасности вот три проблемы, с которыми можно встретиться при перемещении телефона от одного кластера до другого кластера:

- Файл ITL нового кластера не подписан текущим ITL CCM+TFTP сертификат телефона, таким образом, телефон не принимает новый файл ITL или файлы конфигурации.
- Серверы TVS, которые перечислены в текущем файле ITL телефона, не могли бы быть

достижимыми, когда телефоны перемещены в новый кластер.

- Даже если серверы TVS достижимы для Проверки сертификата, старые кластерные серверы TVS не могли бы иметь сертификатов для нового сервера.

Если с этими тремя проблемами встречаются, один возможный вариант должен удалить файл ITL вручную из всех телефонов, которые перемещены между кластерами. Это не желаемое решение, поскольку оно требует широкомасштабного усилия как количества увеличений телефонов, на которые влияют.

> **Совет:** Для дополнительных сведений обратитесь к Безопасности разделом по умолчанию Руководства по обеспечению безопасности Cisco Unified Communications Manager, Выпуска 8.5 (1).

Проблема

Любые изменения, которые телефон получает через TFTP или HTTP от файлов конфигурации, не соблюдают. Параметры конфигурации, которые передают файлы конфигурации частично, включают:

- URL (такие как URL аутентификации, каталоги URL, и URL сервисов, для включения внутренней/внешней конфигурации каталогов)
- Функции локали
- Группы CallManager для основной и вторичной регистрации

Телефон, вероятно, регистрируется к настроенному серверу TFTP по умолчанию, но это, скорее всего, не регистрируется, если новый сервер TFTP не выполняет Сервис CallManager. Когда телефон имеет неправильный файл ITL для текущего сервера TFTP, телефонные console log показывают сообщение, подобное этому:

```
1715: ERR 16:59:35.170584 SECD: EROR:verifyFile: sgn verify file failed
</usr/ram/SEP00260BD749E9.cnf.xml>, errclass 8, errcode 19 (signer not in CTL)
1716: ERR 16:59:35.171327 SECD: EROR:verifyFile: verify FAILED,
</usr/ram/SEP00260BD749E9.cnf.xml>
```

Решение

В этом разделе описывается переместить телефоны эффективно от одного кластера до следующего, а также как вручную удалить файлы ITL из телефонов в худшем случае.

Объемный экспорт сертификата

> **Примечание:** Этот Объемный метод Экспорта Сертификата только работает, если оба кластера являются онлайновыми с сетевым подключением, в то время как перемещены телефоны.

Одно возможное решение, если и старые и новые кластеры являются онлайновыми в то же время, должно использовать Объемный метод миграции Сертификата.

Важно понять, что IP-телефоны проверяют каждый загружаемый файл или против файла ITL или против сервера TVS, который существует в файле ITL. Если телефон должен переместиться в новый кластер, файл ITL, что новым кластерным подаркам должно доверять хранилище сертификата TVS старого кластера.

Выполните эти шаги для реализации Объемного метода Экспорта Сертификата:

1. Перейдите к**> Security администрирования ОС> Объемный Сертификат**.

2. Экспортируйте сертификаты от нового кластера назначения (только TFTP) и исходный кластер к центральному Протоколу передачи файлов Secure Shell (SSH) (SFTP) сервер.

3. Выполните **Консолидировать** сервис **Сертификатов** от исходного кластера (только TFTP) на сервере SFTP, который использует Объемный интерфейс Сертификата.

4. Используйте функцию **Bulk Certificate** от старого кластера происхождения для импорта сертификатов TFTP из центрального сервера SFTP.

5. Перезапустите сервисы TVS на старом кластере происхождения.

6. Используйте Параметр DHCP 150, или некоторый другой метод, для обращения телефонов к новому кластеру назначения.

После того, как вы выполните эти шаги, телефоны загружают новый кластер назначения файл ITL и пытаются проверить его против текущего файла ITL. Так как сертификат не присутствует в текущем файле ITL, телефоны просят, чтобы старый сервер TVS проверил подпись нового файла ITL. Телефоны передают запрос TVS к старому кластеру происхождения на порте TCP 2445 для выполнения этого запроса.

Если процесс сертификата работал правильно, сервис TVS возвращается успешно, и телефоны заменяют в оперативной памяти файл ITL с недавно загруженным файлом ITL. Телефоны могут теперь загрузить и проверить файлы конфигурации со знаком от нового кластера.

Корпоративный параметр отката

> **Примечание:** Этот метод только допустим, если завершено, прежде чем телефонная миграция предпринята и не может использоваться, как только телефоны находятся в *сверять неисправном состоянии файла*. Телефоны, которые поддерживают сервис TVS, могут потенциально проиграть доступ к безопасным сервисам URL, таким как Корпоративный каталог, прежде чем они будут перемещены на новый кластер и после того, как *Подготовить Кластер для Отката к пред8.0* параметрам *установлен в True* на исходном кластере. После того, как перемещенный на новый кластер, телефоны загружают новые файлы ITL и Защищают операцию URL, должен возвратиться к обычному.

Это решение использует *Подготовить Кластер для Отката к пред8.0* Корпоративным параметрам CUCM. Как только этот параметр установлен на *Правда,* телефоны загружают специальный файл ITL, который содержит пустой TVS и разделы сертификата TFTP.

Когда телефон имеет пустой файл ITL, он принимает любой файл конфигурации без знака (для миграций к кластерам, которые выполняют версии CUCM ранее, чем Версия 8.x) и какой-либо новый файл ITL (для миграций к другим кластерам, которые выполняют Версию 8 CUCM. X . Для проверки пустого файла ITL перейдите к**> Security Параметров настройки> Трастовый Список> ITL**. Пустые записи появляются, где старый TVS и серверы TFTP использовали быть.

Телефоны должны иметь доступ к старым серверам CUCM только, пока он берет их для загрузки новых, пустых файлов ITL. Как только телефон имеет пустой файл ITL, старые серверы могут быть выведены из эксплуатации, выключены или восстановлены (зависящий от ваших потребностей бизнеса).

> **Совет:** Для дополнительных сведений обратитесь к Откату Кластера к пред8.0 разделам Выпуска Руководства по обеспечению безопасности Cisco Unified Communications Manager, Выпуска 8.5 (1).

Аппаратные маркеры безопасности (KEY-CCM-ADMIN-K9 =)

Если аппаратные маркеры безопасности (номер продукта **KEY-CCM-ADMIN-K9 =**) использовались для генерации CTL и на старых и на новых кластерах, телефоны в состоянии свободно мигрировать между кластерами, целый по крайней мере один тех же аппаратных ключей использовался и на старых и на новых кластерах.

Когда телефон, который имеет CTL от старого кластера, перемещен в новый кластер, это принимает CTL от нового кластера, поскольку новый CTL содержит сертификат маркера безопасности, который совпадает с сертификатом текущего CTL. Поскольку CTL также содержит сертификат для сервера CCM+TFTP, файлы ITL нового кластера также приняты телефоном, таким образом, нет никаких проблем, когда вы пытаетесь переместить телефон между кластерами.

Для телефонов, которые не используют функцию SBD (ITLs), такой как 7960 и 7940 моделей, необходимо выполнить клиента CTL снова на исходном кластере сначала для добавления новых записей TFTP для серверов TFTP нового кластера перед перемещением телефонов в новый кластер. Это вызвано тем, что эти модели телефонов не протягиваются для файлов TFTP для сервера, который не находится в CTL.

Этот метод требует маркерных аппаратных средств дополнительных мер безопасности и должен быть настроен на старом кластере. Обычно, маркеры безопасности используются для получения возможности Безопасного протокола транспорта в реальном времени (SRTP) в кластере и шифровали/аутентифицировали файлы конфигурации. Как только кластеру включили безопасность с маркерами безопасности, необходимо вручную удалить CTL из каждого телефона на том кластере (с самого телефона) для отключения безопасности на том кластере.

Ручное удаление файла ITL

Если некоторый необратимый выход из строя происходит, и ключ/сертификат TFTP больше не доступен от старого кластера (это поддержано в резервной копии Платформы восстановления после отказа (DRF)), то единственный доступный параметр переместить телефон на новый кластер состоит в том, чтобы вручную удалить файл ITL из телефонов.

> **Примечание:** Этот процесс отличается для каждой модели телефона. Шаги, которые требуются, чтобы удалять файлы ITL на наиболее распространенных моделях телефонов, описаны в этом разделе, но шаги для других моделей могут быть найдены в Телефонных Руководствах по администрированию.

Выполните эти шаги для ручного удаления файлов ITL по телефонам серии 7900:

1. Перейдите к**> Security Параметров настройки> Трастовый Список> Файл ITL**.

2. Введите ****#** для разблокирования параметров настройки.

3. Нажмите **Erase**.

Для ручного удаления файлов ITL на 8900 или телефоны серии 9900, перейдите к **Параметрам настройки> Параметры настройки Администратора>> Security Параметров настройки Сброса Параметры настройки**.