Проблемы проверки подлинности RADIUS в ONS 15454 версии 6.0

Содержание

Введение

Этот документ описывает несколько известных неполадок с проверкой подлинности сервера Сервиса RADIUS в версии 6.0 ONS 15454 в среде Cisco ONS 15454.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco ONS 15454
- RADIUS server (Сервер RADIUS)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 6.0 Cisco ONS 15454

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

RADIUS является системой распределенной безопасности, которая защищает удаленный доступ к сетям и сетевым сервисам против неавторизованный доступа. RADIUS включает эти три компонента:

- Протокол с форматом кадра, использующим протокол дейтаграмм пользователя (UDP)/IP
- Сервер
- Клиент

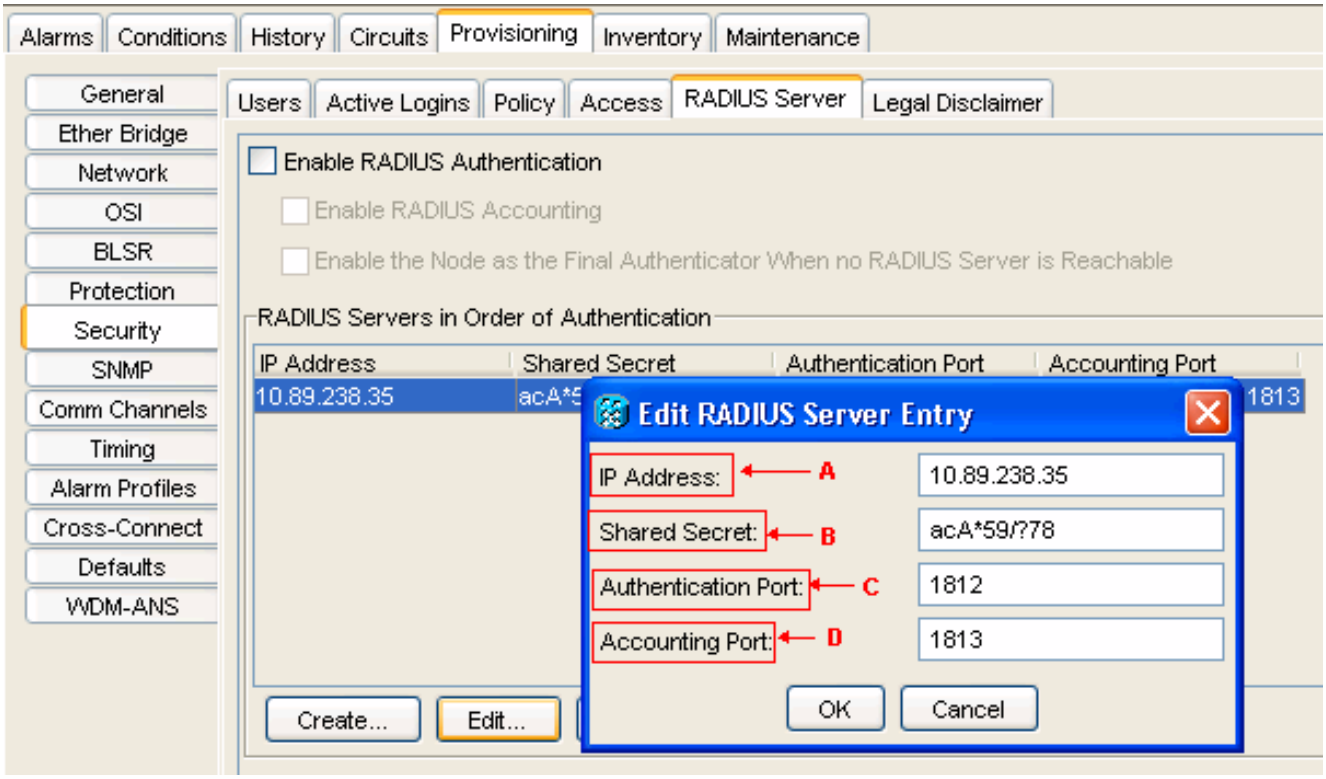
Узел ONS 15454 действует в качестве клиента RADIUS. Клиентские сведения о пользователе проходов к назначенным серверам RADIUS, и затем действуют на ответ. Серверы RADIUS получают запросы подключения пользователя, аутентифицируют пользователя и возвращают все сведения о конфигурации, необходимые для клиента для предоставления услуги пользователю.

Общий секретный ключ аутентифицирует транзакции между Клиентом RADIUS и сервером. Общий секретный ключ никогда не передается по сети. Кроме того, любые пароли пользователя зашифрованы, когда обменено между клиентом и сервером RADIUS. Процесс шифрования устраняет возможность кого-то, кто контролирует незащищенную сеть для определения пароля пользователя.

Общий secret

Общий секретный ключ является текстовой строкой, которая служит паролем между Клиентом RADIUS ONS15454 и сервером RADIUS. Выполните эти шаги для создания общего секретного ключа:

1. Войдите в Cisco Transport Controller (CTC).
2. Перейдите к Network view.
3. Выберите определенный ONS 15454, чтобы перейти к представлению Полки.
4. Нажмите**> Security Provisioning> сервер RADIUS**.
5. Введите IP-адрес сервера RADIUS в поле IP Address (см. стрелку на рисунке 1).
6. Введите общий секретный ключ в поле Shared Secret. Общий секретный ключ является текстовой строкой, которая служит паролем между Клиентом RADIUS и сервером RADIUS (см. стрелку B на рисунке 1).
7. Введите номер порта Проверки подлинности RADIUS в поле Authentication Port (см. стрелку C на рисунке 1).Номер порта проверки подлинности по умолчанию является 1812. Если узел является ENE, установите порт аутентификации в номер в диапазоне 1860 и 1869.
8. Введите номер порта тарификации RADIUS в поле Accounting Port (см. стрелку D на рисунке 1).Номер порта тарификации по умолчанию является 1813. Если узел является ENE, установите порт учета в номер в диапазоне 1870 и 1879.**Рисунок 1 – безопасность: RADIUS server (Сервер RADIUS)**



Используйте общие секретные ключи, чтобы гарантировать, что Устройство с поддержкой RADIUS, которое вы настроили с тем же общим секретным ключом, передает все Сообщения RADIUS кроме сообщения Access-Request.

Общие секретные ключи удостоверяются, что Сообщение RADIUS не становится модифицированным в пути. Другими словами, общие секретные ключи поддерживают целостность сообщения. Общие секретные ключи также шифруют некоторые атрибуты RADIUS, например, User-Password и Туннельный Пароль.

Версия 6.0 ONS 15454 ограничивает длину общего секретного ключа к 16 символам. Однако от версии 6.2 ONS 15454 и далее, Cisco планирует увеличить максимальную длину до 128 символов. См. идентификатор ошибки Cisco CSCsc16614 (только зарегистрированные клиенты) для получения дополнительной информации.

Поддержки группы символов общего секретного ключа:

- Буквы (верхний регистр и нижний регистр), например, A, B, a и b.
- Цифры, например, 1, 2 и 3.
- Символы, которые представляют все символы, которые не определены как буквы или цифры, например,>, (и *.

Сопоставление User Security Group

Пара значения атрибута (AV) представляет переменную и одно из возможных значений, которые может держать переменная. В ONS 15454 пользователи сопоставлены с другими группами безопасности на основе пары значение-атрибут Cisco. Например:

"shell:priv-lvl=X", где X может быть значение от 0 до 3:

- 0 представляет RTRV.
- 1 представляет ПРОВА.

- 2 представляет MAINT.
- 3 представляет СУПЕР.

Password

Сервер RADIUS и клиент не ограничивают символы, которые вы используете для пароля. Однако CTC имеет ограничение. Для версии 6.0 ONS 15454 вот символы, которые поддерживает CTC:

- Буквы (верхний регистр и нижний регистр), например, A, B, a и b.
- Цифры, например, 1, 2 и 3.
- Только #, %, и + специальные символы.

Cisco планирует удалить ограничение специальных символов в более поздних версиях ONS 15454. См. идентификатор ошибки Cisco CSCsc16604 (только зарегистрированные клиенты) для получения дополнительной информации.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация