Содержание

Введение

Этот документ предоставляет ответы на большинство часто задаваемых вопросов, касающихся защищенной системы управления доступом Cisco Secure ACS 5.x и выше.

Опознавательные связанные проблемы

Вопрос. Могут несколько пользователей/групп ACS 5.x внутренняя база данных быть исключенными из политики пароля пользователя (> Users Администрирования системы> параметры аутентификации)?

O. По умолчанию каждый пользователь внутренней базы данных должен соответствовать политике пароля пользователя. В настоящее время никакие пользователи/группы ACS 5.x внутренняя база данных не могут быть исключены.

Вопрос. Могут несколько администраторов GUI ACS 5.x быть исключенными из политики паролирования административного пользователя (Администрирование системы> Администраторы> Параметры настройки> Аутентификация)?

O. По умолчанию каждый административный пользователь GUI должен соответствовать политике паролирования административного пользователя. В настоящее время никакой административный пользователь ACS 5.x не может быть исключен.

Вопрос. ACS 5.x оказывают поддержку для программных средств VMware?

O. Нет. В настоящее время программные средства VMware не поддерживаются с версией ACS 5. x . См. идентификатор ошибки Cisco CSCtg50048 (только зарегистрированные клиенты) для получения дополнительной информации.

Вопрос. Когда LDAP настроен как идентификационное хранилище, каковы поддерживаемые протоколы Аутентификации eap для ACS 5.x?

O. Когда LDAP используется в качестве идентификационного хранилища, ACS 5.2 поддерживает PEAP-GTC, GTC EAP-FAST, и протоколы EAP-TLS только. Это не поддерживает MSCHAPv2 EAP-FAST, EAP-MSCHAPv2 PEAP и EAP-MD5. Для получения дополнительной информации обратитесь к Совместимости Протокола аутентификации и Базы данных пользователей.

Вопрос. Почему сделал аутентификацию для WLC с радиусом использования на сбое ACS, и почему ACS не показал неудачных попыток?

О. Проблема существует с **ACS 5.0 и совместимостью WLC** перед исправлением 4. Исправление 8 загрузки, и применяет исправление на CLI. Не используйте TFTP для устранения этой проблемы.

Вопрос. Почему я неспособен восстановить tar.gz файлы, которые были выполнены резервное копирование с командой backup-log в ACS 5.2?

О. Вы не можете восстановить файлы журнала, которые выполнены резервное копирование с **командой backup-log**. Можно восстановить только те файлы, выполнившие резервное копирование для конфигурации AcS и ОС ADE. См. **резервную копию** и **команды backup-logs** в справочном руководстве по интерфейсу CLI для Cisco Secure Access Control System 5.1 для получения дополнительной информации.

Вопрос. Я могу ограничить количество неуспешных попыток пароля на ACS 5.2?

О. Нет. Эта функция не доступна на ACS 5.2, но это, как ожидают, будет интегрировано в ACS 5.3. См. Функции Не Поддерживаемый раздел Комментариев к выпуску для системы управления доступом Cisco Secure Access Control System 5.2 для получения дополнительной информации.

Вопрос. Я неспособен использовать опцию для изменения пароля при следующем входе в систему для внутренних пользователей в ACS 5.0. Как решить этот вопрос?

О. Опция для изменения пароля при следующем входе в систему не поддерживается в ACS 5.0. Поддержка этой функции доступна в ACS 5.1 и более поздних версиях.

Вопрос. Что это встревожило на среднем значении ACS?

О. Эта ошибка означает, что, когда Представление ACS достигает предела 250,000 сеансов, это бросает сигнал тревоги для удаления 20,000 сеансов. База данных представления ACS хранит все предыдущие сеансы аутентификации и когда она достигает 250,000, она дает сигнал тревоги, чтобы очистить кэш и удалить 20,000 сеансов.

Вопрос. Как делают я решаю это сообщение об ошибках: **: 24407 Active Directory, ,** ?

О. Когда существует проблема с управлением паролями во время аутентификации SDI, это сообщение об ошибках появляется. ACS 5.x используется в качестве RADIUS прокси, и пользователи должны аутентифицироваться сервером RSA. RADIUS прокси к RSA будет работать только без управления паролями. Причина состоит в том, что значение OTP должно быть восстанавливаемым сервером RADIUS для проксирования значения пароля к серверу RSA. Когда управлению паролями включают в туннельной группе, Запрос RADIUS передается с атрибутами MSCHAPv2. RSA не поддерживает MS-0CHAPv2; это поддерживает только PAP.

Для решения этого вопроса отключите управление паролями. Для получения дополнительной информации обратитесь к идентификатору ошибки Cisco CSCsx47423 (только зарегистрированные клиенты).

Вопрос. Действительно ли возможно ограничить admin ACS для управления только определенными устройствами в ACS 5.1?

О. Нет, не возможно ограничить admin ACS для управления только определенными устройствами в ACS 5.1.

Вопрос. ACS поддерживает QoS на аутентификации так, чтобы RADIUS мог быть расположен по приоритетам по TACACS?

О. Нет, ACS не поддерживает QoS на аутентификации. ACS не расположит по приоритетам запросы Проверки подлинности RADIUS по TACACS или запросы TACACS по RADIUS.

Вопрос. Может ACS 5.x TACACS прокси и Проверки подлинности RADIUS к другому TACACS или серверам RADIUS?

О. Да, весь ACS 5.x версии может проксировать Проверки подлинности RADIUS к другим серверам RADIUS. ACS 5.3 и позже может проксировать Аутентификации TACACS к другим Серверам tacacs.

Вопрос. Может ACS 5.x проверять атрибуты наборного (телефонный) доступа Пользователя Active Directory для предоставления доступа?

О. Да, в ACS 5.3 и позже можно позволить, запретить и управлять доступом полномочий для удаленного доступа по телефонной линии пользователя. Разрешения проверены во время аутентификаций или запросов из Active Directory. Это установлено на выделенном словаре Active Directory.

Вопрос. ACS 5.x поддерживают CHAP или типы аутентификации MSCHAP для TACACS +?

О. Да, TACACS + CHAP и типы аутентификации MSCHAP поддерживаются в версиях ACS 5.3 и позже.

Вопрос. Я могу установить тип пароля внутреннего пользователя ACS к какой-либо внешней базе данных?

О. Да, в ACS 5.3 и позже можно установить тип пароля внутреннего пользователя ACS. Эта функция была доступна в ACS 4. x .

Вопрос. Я могу передать/отказать аутентификацию на основе времени, в которое пользователь был создан в ACS Внутреннее Идентификационное Хранилище?

О. Да, в ACS 5.3 и позже можно использовать **Количество Часов Начиная с**

Пользовательского атрибута **Создания** для создания политики. Этот атрибут содержит количество часов, так как пользователь был создан во Внутреннем Идентификационном Хранилище ко времени текущего запроса аутентификации.

Вопрос. Я могу использовать подстановочные знаки для добавления новой записи хоста во Внутренней базе данных ACS?

О. Да, ACS 5.3 и позже позволяет вам использовать подстановочные знаки, когда вы добавляете новые хосты во Внутреннее Идентификационное Хранилище. Это также позволяет вам вводить подстановочные знаки (после ввода первых трех октетов) для определения всех устройств от определенного изготовителя.

Вопрос. Я могу настроить пулы IP-адреса на ACS 5.x и назначить их от ACS?

О. Нет, не в настоящее время возможно создать пулы IP-адреса на ACS 5. x .

Вопрос. Я могу видеть IP-адрес клиента AAA, куда запрос прибыл в отчёт об ОШИБКЕ ПРОВЕРКИ ПОДЛИННОСТИ?

О. Нет, не возможно видеть IP-адрес клиента AAA от того, где вошел запрос.

Вопрос. Что такое Восстановление сообщения Просмотра журнала в ACS 5.3?

О. ACS 5.3 предоставляет новую характеристику для восстановления любых журналов, которые пропущены, когда представление не работает. ACS собирает эти пропущенные журналы и хранит их в его базе данных. Используя эту функцию, можно получить пропущенные журналы от базы данных ACS до обзорной базы данных после того, как представление будет резервным копированием. Для использования этой функции необходимо установить Конфигурацию Восстановления Сообщения журнала в **на**. Для получения дополнительной информации при настройке Восстановления сообщения Просмотра журнала, обратитесь к Работам системы Средства просмотра Мониторинга и Отчёта.

Вопрос. Я могу сжать ACS 5.x база данных путем запуска команды database-compress от CLI Прикладного устройства управления услугами Solution Engine? Эта функция была доступна в ACS 4. x .

О. Да, в ACS 5.3 и позже, **команда database-compress** уменьшает размер базы данных ACS с опцией для удаления Таблицы транзакций ACS. Администраторы ACS могут выполнить эту команду для сокращения размера базы данных. Это помогает уменьшать размер базы данных и время, потраченное для резервных копий и полной синхронизации, которая необходима для обслуживания.

Вопрос. Я могу искать запись клиента AAA на основе ее IP-адреса?

О. Да, ACS 5.3 и позже позволяет вам искать сетевое устройство с помощью своего IP-адреса. Можно также использовать подстановочные знаки и диапазон для поиска определенного набора сетевых устройств.

Вопрос. Я могу создать условие на основе времени, в которое пользователь был создан в ACS Внутреннее Идентификационное Хранилище?

О. Да, в ACS 5.3 и позже можно использовать **Количество Часов Начиная с Пользовательского** атрибута **Создания**, который позволяет вам настроить условия правила политики, на основе времени, в которое пользователь был создан в ACS Внутреннее Идентификационное Хранилище. Пример: Если **group=HelpDesk&NumberofHoursSinceUserCreation> 48** тогда отклонение. Этот атрибут содержит количество часов, так как пользователь был создан во Внутреннем Идентификационном Хранилище ко времени текущего запроса аутентификации.

Вопрос. Я могу зарегистрироваться, какое Идентификационное Хранилище Пользователь аутентифицировался в разделе Авторизации Политики обслуживания?

О. Да, в ACS 5.3 и позже можно использовать **Опознавательный Идентификационный** атрибут **Хранилища**, который позволяет вам настроить условия правила политики на основе Опознавательного Идентификационного Хранилища. Пример: Если **AuthenticationIdentityStore=LDAP_NY** тогда отклоняют. Этот атрибут содержит название Идентификационного используемого Хранилища, и это обновлено с соответствующим Идентификационным Названием магазина после успешной аутентификации.

Вопрос. Когда ACS переходит к следующему Идентификационному Хранилищу, определенному в Последовательности хранилища идентификаторов?

О. ACS переходит к следующему Идентификационному Хранилищу, определенному в Последовательности хранилища идентификаторов в этих сценариях:

- Пользователь не найден в первом Идентификационном Хранилище
- Идентификационное Хранилище не доступно в последовательности

Вопрос. Какова политика Выведения из строя Учетной записи в ACS 5.3?

О. Политика Выведения из строя Учетной записи позволяет вам отключать пользователей Внутреннего Идентификационного Хранилища, когда настроенная дата вне разрешенной даты, настроенный номер дней вне разрешенных дней, или количество последовательных неуспешных попыток входа превышает порог. Значение по умолчанию для даты превышает, 30 дней от текущей даты. Значение по умолчанию в течение многих дней не должно составлять больше чем 60 дней с текущего дня. Значение по умолчанию для неудачных попыток равняется 5.

Вопрос. Я могу изменить пароль пользователя внутренней базы данных ACS по telnet?

О. Да, вам разрешают изменить пароль пользователя внутренней базы данных, использующего TACACS + по telnet. Необходимо выбрать **Enable TELNET Change Password** под **Контролем за Изменением пароля** на ACS 5. x .

Вопрос. Основной ACS 5.x экземпляр автоматически периодически обновляют резервные экземпляры, или это должно только произойти, когда изменилась конфигурация?

О. ACS 5.x сразу реплицирует во Вторичный ACS каждый раз, когда вы вносите изменения на Основном ACS. Кроме того, если вы не внесете изменений в Основной ACS тогда, то он будет делать репликацию силы каждые 15 минут. На этом этапе нет опции для управления таймером так, чтобы ACS мог реплицировать информацию после специфического времени.

Вопрос. Я могу просмотреть/экспортировать отчёт относительно ACS 5.x всех пользователей, в которых в настоящее время входят и аутентифицируют от ACS на других клиентах NAS?

О. Да, это возможно. Существует два отдельных отчета для RADIUS и TACACS +. Можно найти их при **Мониторинге и Отчётах> Отчёты> Каталог> Каталог Сеанса> Активные сеансы RADIUS** и **Активные сеансы TACACS**. Оба отчёта основываются на учетной информации от клиентов NAS, так как она позволяет вам отслеживать, когда пользователь соединяется и выходит из системы. История сеанса даже позволяет вам получать информацию от запуска и останавливать сообщения в течение определенного дня.

Дополнительные сведения

- Страница технической поддержки системы управления доступом Cisco Secure Access Control System
- Cisco Systems – техническая поддержка и документация