TAC

ID документа: 118703

Обновлено: 05 января 2015

Внесенный Аароном Леонардом, Шанкаром Раманатаном, и Джесси Дюбуа, специалистами службы технической поддержки Cisco.

PDF загрузки
Печать
[+] Feedback

Родственные продукты

- Wireless, LAN (WLAN)
- 802.1x

Содержание

Введение

Этот документ предоставляет краткий обзор базовой конфигурации рекомендации для крупномасштабных беспроводных развертываний, таких как Контроллер беспроводной локальной сети (WLC) AireOS с RADIUS с платформой Cisco Identity Services Engine (ISE) или сервер Cisco Secure Access Control Server (ACS). Этот документ ссылается на другие документы с большими техническими подробностями.

Наблюдаемые признаки

Как правило, университетские среды встречаются с этим состоянием краха Аутентификации, авторизации и учета (AAA). В этом разделе описываются обычные Признаки/Журналы, засвидетельствованные в этой среде.

1. Производительность RADIUS монитора

Клиент Dotx испытывает большую задержку со многими повторными попытками для аутентификации.

Используйте **команду show radius auth statistics** (GUI: **Монитор> Статистика> серверы RADIUS**) для поиска проблем. В частности ищите большие числа Повторных попыток, Отклонений и Таймаутов. Например:

Ищите:

- Высокая Повторная попытка: Первое соотношение Запроса (должны быть не больше, чем 10%),
- Высокое Отклонение: Примите соотношение
- Высокий Таймаут: Первое соотношение Запроса (должны быть не больше, чем 5%),

Если существуют проблемы, проверьте для:

- Неверно - настроенные клиенты
- Проблемы возможности доступа к сети между WLC и сервером RADIUS
- Проблемы между сервером RADIUS и базой данных бэкэнда, если в использовании, такой как с Active Directory (AD)

2. WLC видит очередь RADIUS, полную на Msglogs

WLC получает это сообщение об очереди RADIUS:

3. Debug AAA

Отладка AAA показывает это сообщение:

Отладка AAA возвращает Ошибочный **Таймаут** AAA **(-5)** для мобильных устройств. AAA-сервер недостижим и придерживается клиентским deauthorization.

4. Сервер RADIUS Слишком Занят и Не Отвечает

Вот Регистрационное Trap-сообщение Системного времени:

Настройка оптимального метода

Настройка стороны WLC

- Протокол EAP - Заставляет исключение клиента 802.1X работать.

  Включите клиентское исключение глобально для 802.1X.
  Исключение клиента набора на Беспроводных локальных сетях 802.1X (WLAN) по

крайней мере к 120 секундам.
Таймеры EAP набора, как описано в Исключении Клиента 802.1X на статье AireOS WLC.

- Тайм-ауты повторной передачи RADIUS набора по крайней мере к пяти секундам.
- Session-Timeout набора по крайней мере к восьми часам.
- Отключите Агрессивное Аварийное переключение, которое не позволяет одиночному соискателю с некорректным поведением заставлять WLC отказывать между серверами RADIUS.
- Настройте Быстро Безопасный Роуминг для своих клиентов.

  Удостоверьтесь, что клиенты EAP Microsoft Windows используют Защищенный доступ по протоколу Wi-Fi 2 (WPA2) / Расширенный стандарт шифрования (AES), таким образом, они могут использовать Оппортунистическое ключевое кэширование (OKC).

  Если можно выделять клиентов iOS Apple к их собственному WLAN, то можно включить 802.11r на том WLAN.

  Включите централизованное управление ключами Cisco (CCKM) для любого WLAN, который поддерживает 792x телефоны (но **не** включайте CCKM ни на каких идентификаторах наборов сервисов (SSID), которые поддерживают Microsoft Windows или клиентов Android, потому что они имеют тенденцию иметь проблематичные реализации CCKM).

  Включите Кэширование ключа Sticky (SKC) для любого WLAN EAP, который поддерживает Операционную систему Macintosh (MAC OS) X и/или клиенты Android.

  См. Роуминг WLAN 802.11 и Быстро-безопасный Роуминг на CUWN для получения дополнительной информации.

  Примечание: Контролируйте свое использование кэша парного главного ключа (PMK) WLC в пиковое время с **show pmk-cache вся** команда. Если вы достигаете своего максимального размера кэша PMK или рядом с ним, то необходимо будет, вероятно, отключить SKC.
  При использовании ISE с профилированием то используйте профилирование DHCP/HTTP стороны WLC. Это обертывает копировальные данные в пакет RADIUS Accounting, который легко распределен нагрузку, который гарантирует, что все данные для оконечной точки достигают той же Сети услуг общего пользования (PSN).

  Удостоверьтесь, что промежуточный учет выключен, пока вам не нужен он для основанных на байте сервисов составления счетов. В противном случае промежуточный учет только добавляет загрузку без дополнительного преимущества.

  Выполните лучший код WLC.

Настройка серверной части RADIUSУменьшите скорость регистрации.

Большинство серверов RADIUS конфигурируемо, о какой регистрации они сохранят. Если ACS или ISE используются, администратор может выбрать, какие категории зарегистрированы к контролирующей базе данных. Один пример мог бы быть то, если учетные данные отосланы сервера RADIUS и просмотрены с другим приложением, таким как СИСТЕМНЫЙ ЖУРНАЛ, то не пишите данные в базу данных локально. На ISE гарантируйте, что регистрационное подавление остается включенным в любом случае. Если это должно быть отключенный для целей устранения проблем, то переходят **к администрированию> Система> Регистрация> Фильтры Набора** и используют опцию Bypass Suppression для отключения подавления на отдельной оконечной точке или пользователе. В Версии 1.3 ISE и позже, оконечная точка может щелкнуться правой кнопкой мыши в оперативном опознавательном журнале для отключения подавления также.

Гарантируйте, что задержка аутентификации бэкэнда низка (AD, Протокол LDAP, Rivest, Shamir, Адлемен (RSA)). При использовании ACS или ISE опознавательные сводные отчеты могут быть выполнены для мониторинга задержки на основе на сервер и для средней и для пиковой задержки. Чем дольше это берет запрос, который будет обработан, тем ниже опознавательная скорость ACS или ISE может обработать. 95% времени, большая задержка происходит из-за медленного ответа от базы данных бэкэнда.

Отключите Повторные попытки Пароля Защищенного расширяемого протокола аутентификации (PEAP). Большинство устройств не поддерживает повторные попытки пароля в туннеле PEAP, таким образом, повторная попытка от сервера EAP заставляет устройство прекращать отвечать и перезапуск новым сеансом EAP. Это вызывает таймауты EAP вместо отклонений, что означает, что не будут поражены клиентские исключения.

Отключите Неиспользованные Протоколы EAP. Это не важно, но действительно добавляет, что некоторая эффективность к EAP обменивается, и гарантирует, что клиент не может использовать слабый или непреднамеренный метод EAP.

Включите резюме сеанса PEAP и быстро воссоединитесь.

Не передавайте Проверки подлинности MAC к AD если не необходимый. Это - распространенная ошибка конфигурации, которая увеличивает загрузку на контроллерах домена, против которых аутентифицируется ISE. Они часто приводят к отрицательным поискам, которые являются трудоемкими и увеличивают среднюю задержку.

Используйте Датчик Устройства где применимый (определенный ISE).

Адресовать вопрос техподдержке (требует контракта сервиса Cisco.)

Связанные обсуждения Сообщества Cisco Support

Сообщество Cisco Support является форумом для вас, чтобы спросить и ответить на вопросы, общие предложения, и сотрудничать с вашими узлами.

См. Cisco Technical Tips Conventions для получения информации об условных обозначениях, используемых в этом документе.

Обновлено: 05 января 2015
ID документа: 118703