

Настройте функцию нейтрализации сервера RADIUS на контроллерах беспроводной локальной сети



ID документа: 106258

Обновлено : 30 апреля 2008

Внесенный Николасом Дарчисом, специалистом службы технической поддержки Cisco.



[Загрузка PDF](#)

[Печать](#)

[Обратная связь](#)

Родственные продукты

- [Контроллеры беспроводных LAN серии Cisco 4400](#)
- [Cisco 2100 Series Wireless LAN Controllers](#)
- [Cisco Catalyst 3750 Series Integrated Wireless LAN Controllers](#)
- [Модуль беспроводных сервисов \(WiSM\) Cisco Catalyst серии 6500/7600](#)
- [Контроллеры беспроводных LAN серии Cisco 2000](#)
- [Cisco Wireless LAN Controller Module](#)
- [Cisco 4100 Series Wireless LAN Controllers](#)
- [+ Покажите больше](#)

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Функция нейтрализации сервера RADIUS](#)

[Режимы нейтрализации](#)

[Активный режим](#)

[Пассивный режим](#)

[Режим выключено](#)

[Настройка](#)

[Настройте функцию нейтрализации сервера RADIUS с CLI](#)

[Настройте функцию нейтрализации сервера RADIUS с GUI](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

[Соответствующие дискуссии сообщества технической поддержки Cisco](#)

Введение

Этот документ описывает, как настроить функцию нейтрализации сервера RADIUS с Контроллерами беспроводной локальной сети (WLC).

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о конфигурации Облегченных точек доступа (LAP) и WLC Cisco.
- Базовые знания о Контроле И Инициализация протокола Точки беспроводного доступа (CAPWAP).
- Базовые знания о Решениях для Безопасности беспроводной связи.

Используемые компоненты

Сведения в этом документе основываются на WLC Cisco 4400, который выполняет релиз микропрограммы 5.0.

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

Функция нейтрализации сервера RADIUS

Версии программного обеспечения WLC ранее, чем 5.0 не поддерживают механизм восстановления сервера RADIUS. Когда основной сервер RADIUS станет недоступным, WLC будет аварийное переключение к следующему активному резервному серверу RADIUS. Даже если основной сервер будет доступен, WLC продолжит использовать дополнительный сервер RADIUS навсегда. Обычно в качестве первичного выбирается мощный и наиболее предпочтительный сервер.

В WLC 5.0 и более поздних версиях, WLC поддерживает функцию нейтрализации сервера

RADIUS. С этой функцией WLC может быть настроен, чтобы проверить, доступен ли основной сервер и переключается назад на основной сервер RADIUS, как только это доступно. Чтобы сделать это, WLC поддерживает два новых режима, пассивные и активные, для проверки статуса сервера RADIUS. WLC возвращается к самому предпочтительному серверу после указанного значения таймаута.

Режимы нейтрализации

Активный режим

В активном режиме, когда сервер не отвечает на запрос аутентификации WLC, WLC отмечает сервер как мертвый и затем перемещается, сервер к неактивному серверу объединяют, и начинает передавать тестовые сообщения периодически, пока не отвечает тот сервер. Если сервер отвечает, то WLC перемещает неработающий сервер в активный пул и прекращает передавать тестовые сообщения. В этом режиме, когда запрос аутентификации прибывает, WLC всегда выбирает самый низкий индекс (наивысший приоритет) сервер от активного пула серверов RADIUS.

WLC передает тестовый пакет после таймаута (по умолчанию составляет 300 секунд) для определения состояния сервера в случае, если сервер был безразличен ранее.

Пассивный режим

В пассивном режиме, если сервер не отвечает на запрос аутентификации WLC, WLC перемещает сервер к неактивной очереди и устанавливает таймер. Когда таймер истекает, WLC перемещает сервер к активной очереди независимо от реального состояния сервера. Когда запрос аутентификации прибывает, WLC выбирает самый низкий индекс (наивысший приоритет) сервер от активной очереди (который мог бы включать неактивный сервер). Если сервер не отвечает тогда, WLC отмечает его как неактивный, устанавливает таймер и перемещается в следующий сервер наивысшего приоритета. Этот процесс продолжается, пока WLC не находит активный сервер RADIUS, или пул активного сервера исчерпан.

WLC предполагает, что сервер активен после таймаута (по умолчанию составляет 300 секунд) в случае, если сервер был безразличен ранее. Если это все еще безразлично, WLC ждет другого таймаута и попробовал еще раз, когда входит запрос аутентификации.

Режим выключено

В режим выключено, WLC поддерживает аварийное переключение только. Другими словами, нейтрализация отключена. Когда основной сервер RADIUS выключится, WLC будет аварийное переключение к следующему активному резервному серверу RADIUS. Даже если основной сервер доступен, WLC продолжает использовать дополнительный сервер RADIUS навсегда.

Настройка

Настройте функцию нейтрализации сервера RADIUS с CLI

Примечание: [Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд \(только для зарегистрированных клиентов\).](#)

Используйте эти команды от CLI WLC для активации опции нейтрализации сервера RADIUS на WLC.

Первый шаг должен выбрать режим нейтрализации сервера RADIUS. Как отмечалось ранее, WLC поддерживает активный и пассивные режимы нейтрализации.

Для выбора режима нейтрализации введите эту команду:

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- активный - Передает зонды к неработающим серверам для тестирования статуса.
- пассивный- Состояние сервера Наборов на основе последней транзакции.
- прочь - Отключает тест нейтрализации сервера (по умолчанию).

Следующий шаг должен выбрать интервал, который задает тестовый интервал для активного режима или неактивное время для пассивных режимов операции.

Для установки интервала введите эту команду:

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180 - 3600> - Вводят тестовый интервал, или неактивное время в секундах (по умолчанию составляет 300 секунд).

Интервал задает тестовый интервал в случае нейтрализации активного режима или неактивное время в случае нейтрализации пассивного режима.

Для активного режима операции необходимо настроить имя пользователя, которое будет использоваться в тестовом запросе, отправленном к серверу RADIUS.

Для настройки имени пользователя введите эту команду:

```
WLC1 > config radius fallback-test username {username}
```

<username> - Вводит имя до 16 алфавитно-цифровых знаков (по умолчанию является зондом Cisco).

Примечание: Можно ввести собственное имя пользователя или оставить его с по умолчанию. Имя пользователя по умолчанию является "зондом Cisco". Поскольку это имя пользователя используется для передачи тестовых сообщений, вы не должны настраивать пароль.

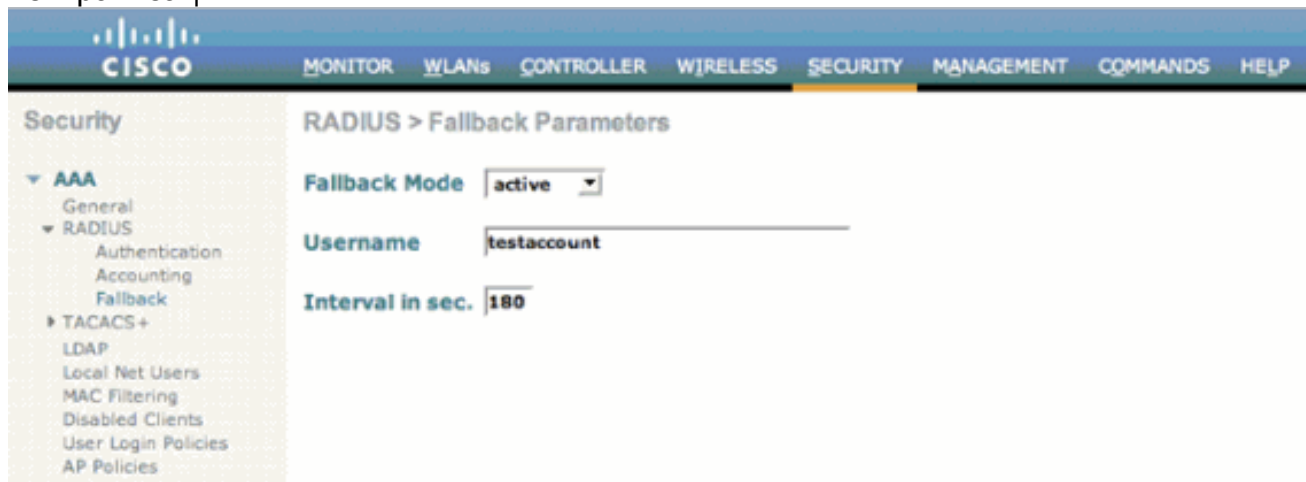
Настройте функцию нейтрализации сервера RADIUS с GUI

Выполните эти шаги для настройки WLC с GUI:

1. Настройте режим нейтрализации сервера RADIUS. Чтобы сделать это, выберите **Security> RADIUS> Fallback** от GUI WLC. Страница RADIUS> Fallback Parameters

появляется.

- От выпадающего списка Режимы нейтрализации выберите режим нейтрализации. Доступные параметры включают активный, пассивный, и прочь. Вот снимок экрана в качестве примера для конфигурации активного режима нейтрализации:



- Для активного режима операции введите имя пользователя в поле имени пользователя.
- Введите тестовое значение интервала в Интервал в сек. поле.
- Щелкните "Применить".

Если агрессивная опция аварийного переключения активирована в WLC, WLC слишком агрессивен для маркировки AAA-сервера как "не ответ". Однако, это не должно быть сделано, потому что AAA-сервер возможно не быстро реагирующий только тому конкретному клиенту, если вы делаете тихий сброс. Он может отвечать другим действительным клиентам (с действительными сертификатами). WLC может все еще отметить AAA-сервер как "не ответ" и "не функциональный".

Чтобы избежать этого, отключите функцию aggressive failover. Введите команду `config radius aggressive-failover disable` от графического интерфейса контроллера для выполнения этого. Если эта функция отключена, то контроллер будет переключаться на следующий сервер AAA, если три клиента подряд не смогут получить ответ от сервера RADIUS.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

[Средство Output Interpreter \(OIT\) \(только для зарегистрированных клиентов\) поддерживает определенные команды show.](#) Посредством OIT можно анализировать выходные данные команд show.

Введите команду `show radius summary` для проверки конфигурации нейтрализации. Например:

```
WLC1 >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Type..... IP Address
Aggressive Failover..... Enabled
Keywrap..... Disabled
```

```
Fallback Test:
Test Mode..... Active
Probe User Name..... testaccount
Interval (in seconds)..... 180
```

Authentication Servers

```
Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
-----
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none
```

Accounting Servers

```
Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
-----
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Примечание: [Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".](#)

- `debug dot1x events enable` - Настраивает отладки событий 802.1X.
- `debug aaa events enable` - Настраивает отладки всех событий AAA.

Дополнительные сведения

- [Пример конфигурации аутентификации EAP в контроллерах WLAN \(WLC\)](#)
- [Регистрация облегченных точек доступа у контроллеру беспроводных LAN \(WLC\)](#)
- [Решения по обеспечению безопасности Настройки](#)
- [Пример конфигурации "Dynamic VLAN Assignment with RADIUS Server and Wireless LAN Controller"](#)
- [Cisco Systems – техническая поддержка и документация](#)

Был ли этот документ полезен? [Да](#) [нет](#)

Спасибо за ваш отзыв.

[Адресовать вопрос техподдержке \(требуется контракт сервиса Cisco.\)](#)

Соответствующие дискуссии сообщества технической поддержки Cisco

[Сообщество технической поддержки Cisco является форумом, в котором можно задавать вопросы и получать ответы, обмениваться предложениями и сотрудничать со своими равноправными коллегами.](#)

[См. Условные обозначения технических советов Cisco для получения информации по условным обозначениям, которые используются в данном документе.](#)

Обновлено : 30 апреля 2008

ID документа: 106258