Интеграция ACS Version 5.x с примером конфигурации WAAS

Содержание

Введение

Этот документ описывает, как настроить интеграцию Сервисов WAAS (WAAS) Cisco с Версией 5 Access Control Server (ACS) Cisco. x. Когда настроено на шаги в этот документ, пользователи в состоянии аутентифицироваться на WAAS с TACACS + учетные данные через ACS.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

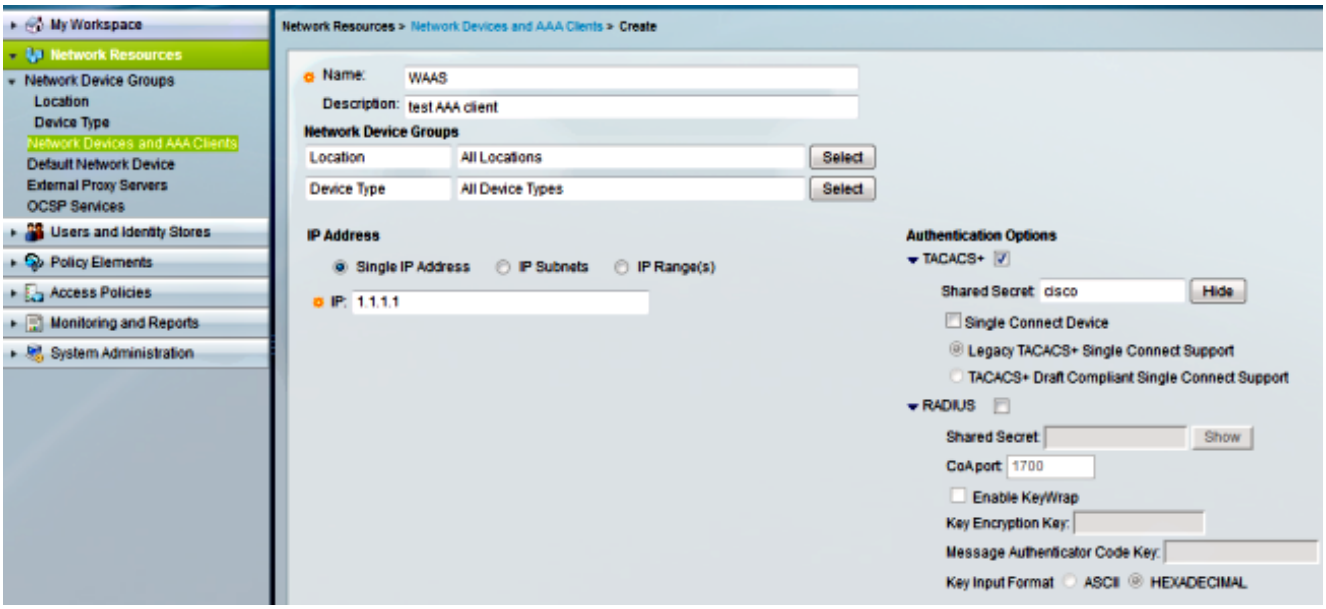
- Версия 5 Cisco Secure ACS. x
- Cisco WAAS

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.

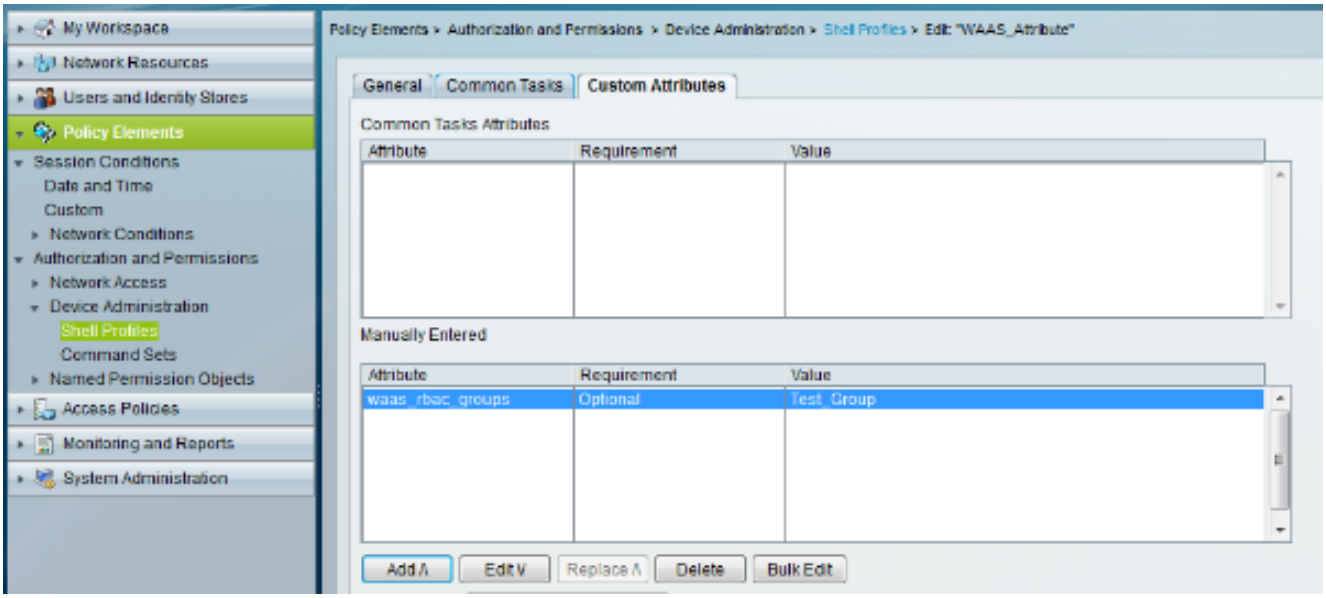
Настройка

Настройте ACS

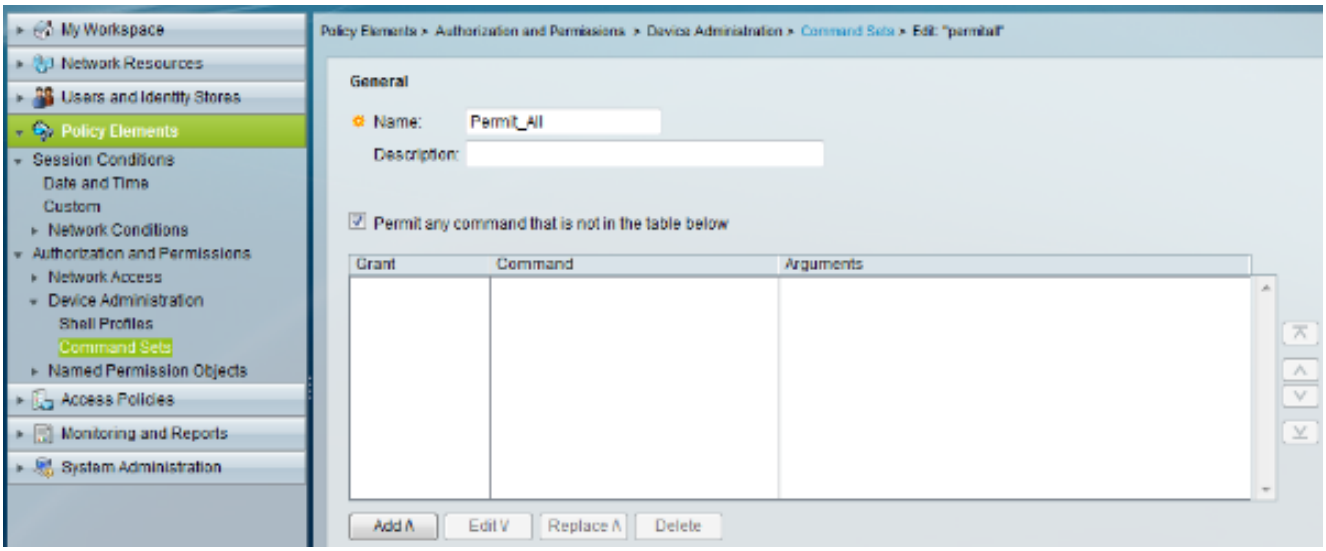
1. Для определения клиента AAA на ACS Version 5.x перейдите к **Сетевым ресурсам> Сетевые устройства и Клиенты AAA.** Настройте клиента AAA с описательным именем, одним IP-адресом и общим секретным ключом для TACACS +.



2. Для определения Профиля Shell перейдите к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Профили Shell**. В данном примере настроен новый профиль оболочки под названием **WAAS_Attribute**. Этот настраиваемый атрибут передается WAAS, который позволяет ему выводить, какая группа пользователей является группой администраторов. Настройте эти настраиваемые атрибуты:
Атрибут является **waas_rbac_groups**.**Требование** является **Дополнительным** так, чтобы оно не нарушало никакое другое устройство.**Значение** является названием группы, которая должна быть назначенным административным доступом (Test Group).

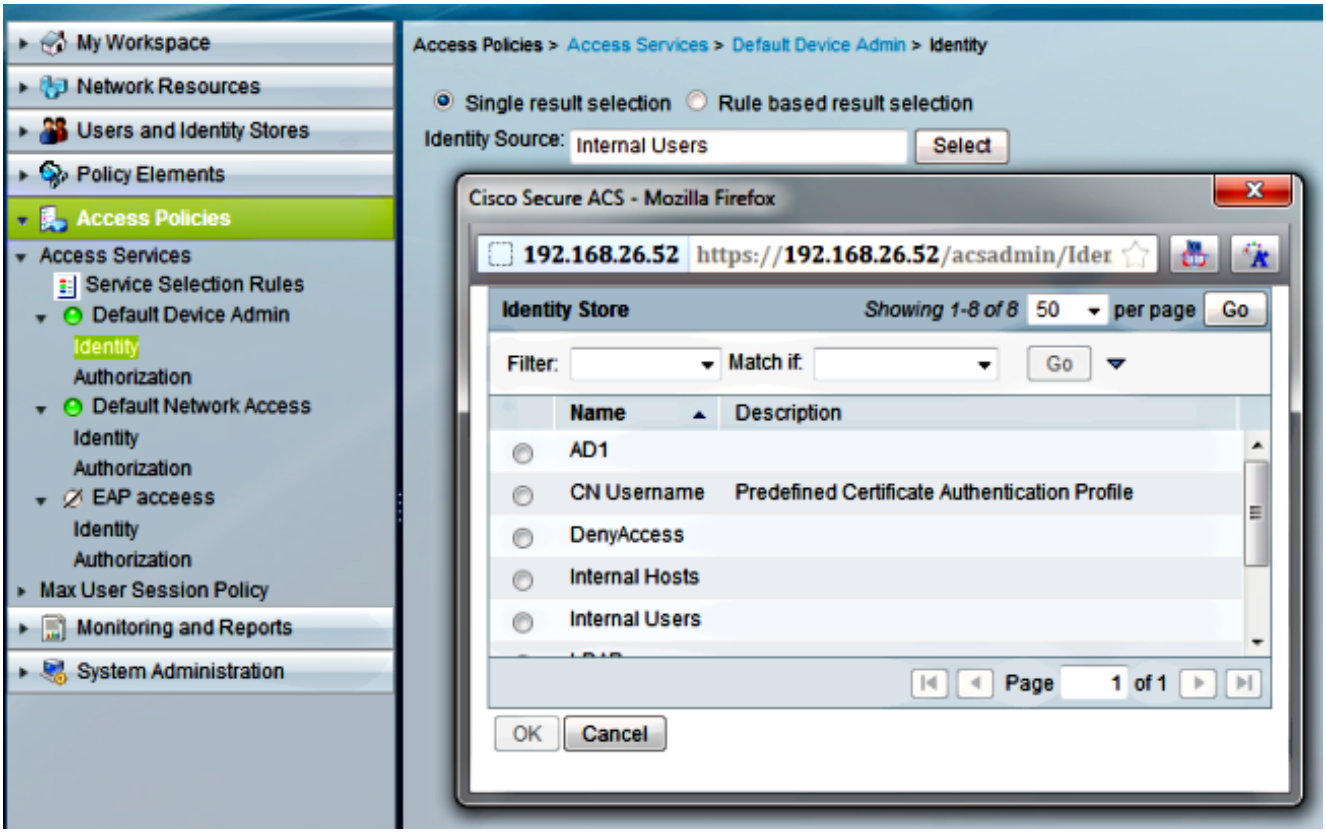


3. Для определения набора команд, чтобы позволить все команды, перейти к **Элементам Политики> Авторизация и Разрешения> Администрирование устройств> Наборы команд**.
   Отредактируйте набор команд **Permit_All**.Если вы проверяете **Разрешение какая-либо команда, которая не находится в таблице ниже** флажка, пользователю предоставляют полные
   полномочия.

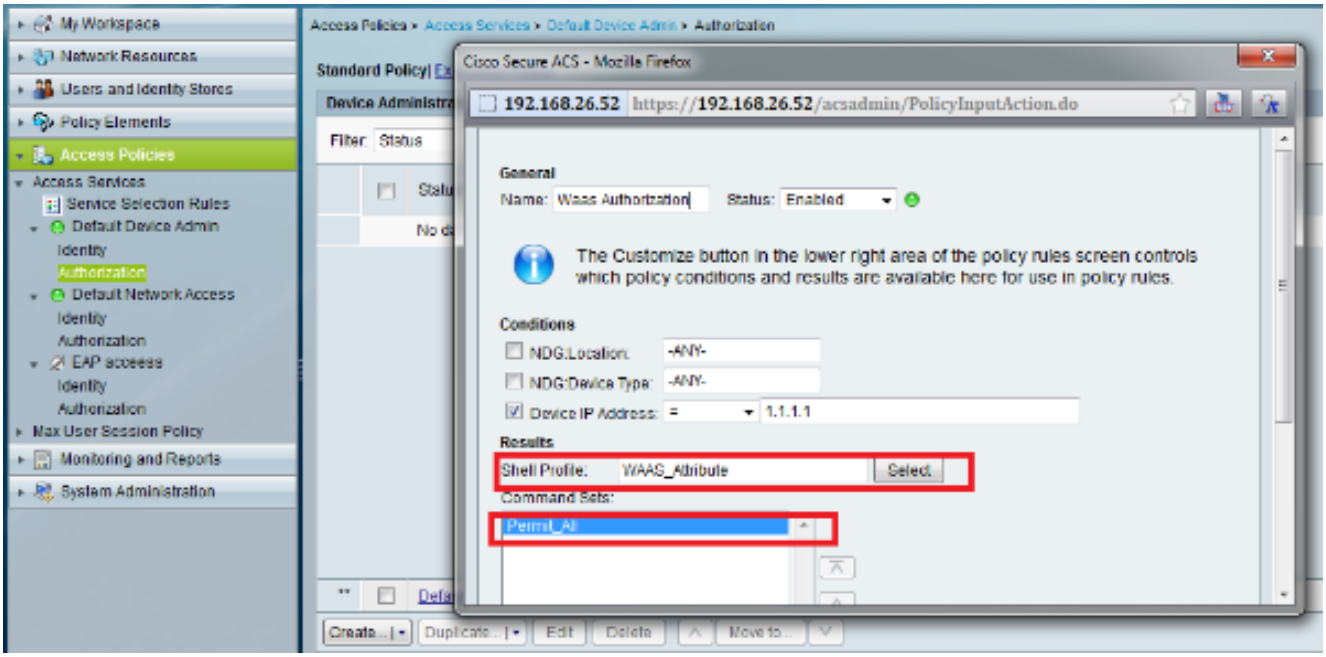


   Примечание: Так как данный пример использует TACACS, выбранный сервис по умолчанию является **администратором устройства по умолчанию**.

4. Для обращения идентичности к корректному идентификационному источнику перейдите к **Политике доступа> Службы доступа> Администратор устройства по умолчанию> Идентичность.** Если пользователь существует в локальной базе данных ACS, выберите **Internal Users**. Если пользователь существует в Active Directory, выберите настроенное идентификационное хранилище (**AD1** в данном примере).

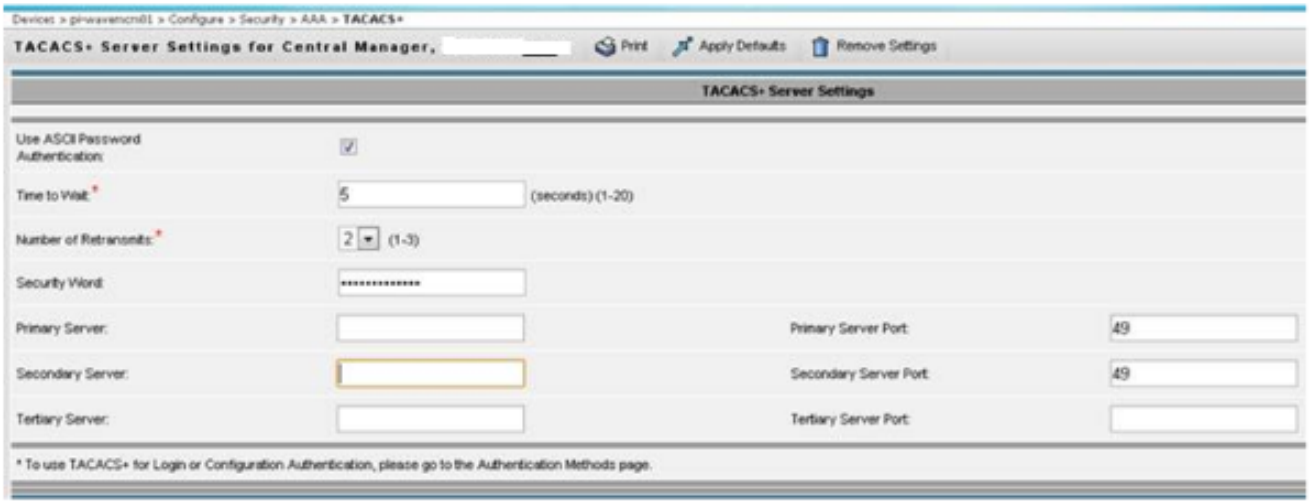


5. Для создания правила авторизации перейдите к **Политике доступа> Службы доступа> Администратор устройства по умолчанию> Авторизация.** Создайте новую политику авторизации под названием **Авторизация WAAS**. Это проверяет для запросов от WAAS. В данном примере IP устройства используется в качестве условия. Однако это может быть изменено на основе требований развертываний. Примените профиль оболочки и наборы команд, настроенные в Шагах 2 и 3 в этот раздел.

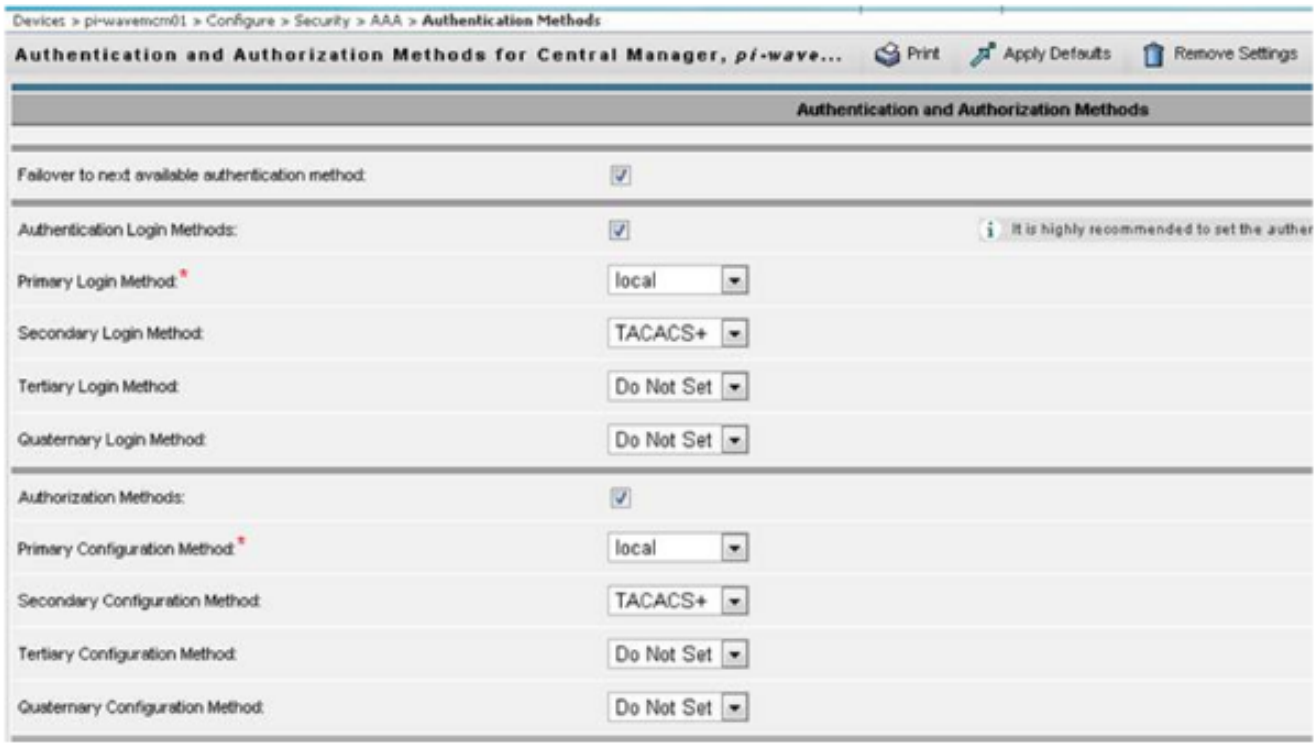


Конфигурация на WAAS

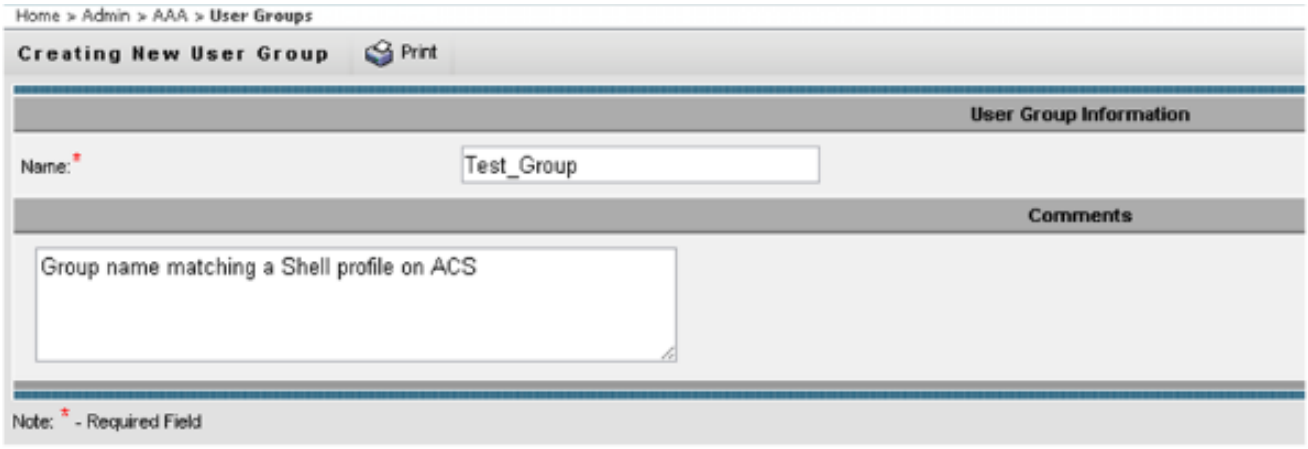
1. Для определения TACACS + сервер, перейдите к **Устройствам> *<Центральное Имя системы Менеджера>>* Настраивает> Security> AAA> TACACS +**. Настройте IP-адрес сервера ACS и предварительный общий ключ.



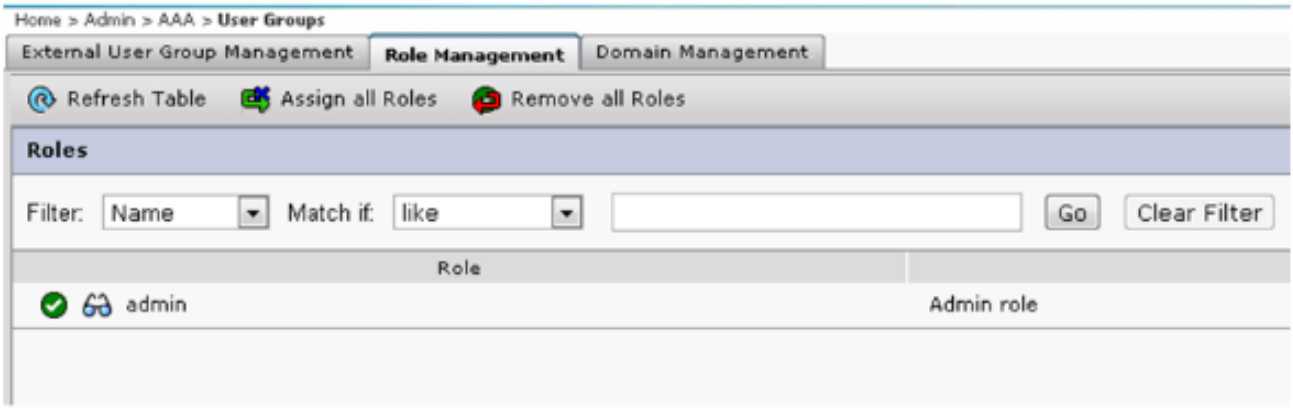
2. Для изменения методов проверки подлинности и авторизация перейдите к **Устройствам> *<Центральное Имя системы Менеджера>>* Настраивает> Security> AAA> Методы аутентификации**. В этом снимке экрана основной способ входа в систему настроен для **локальной переменной** со вторичным устройством, настроенным для **TACACS +**.



3. Перейдите к **Дом> Admin> AAA> Группы пользователей** для добавления имени группы, которое совпадает **со Значением** настраиваемого атрибута (см. Шаг 2 в **Настраивать** раздел **ACS**) в WAAS.



4. Назначьте эту группу (Test_Group) права **уровня admin** на вкладке **Home> Admin> AAA> User Groups Role Management**. Роль **admin** на Центральном Менеджере предварительно сконфигурирована.



Проверка

Попытка войти в систему WAAS с TACACS + учетные данные. Если все настроено правильно, вы - предоставленный доступ.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.