Беспроводное администрирование системы управления и системы управления сетью с ACS 5.x пример конфигурации

Содержание

Введение

Этот документ описывает использование защищенного сервера управления доступом Cisco ACS 5.x для настройки системы управления беспроводной сетью Cisco (WCS) и администрирования системы управления сетью (NCS) Cisco Prime.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Wireless Control System
- Cisco главная система управления сетью
- Cisco Secure Access Control Server

Используемые компоненты

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

- Cisco Wireless Control System 7.0.172.0
- Cisco Secure ACS 5. x

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

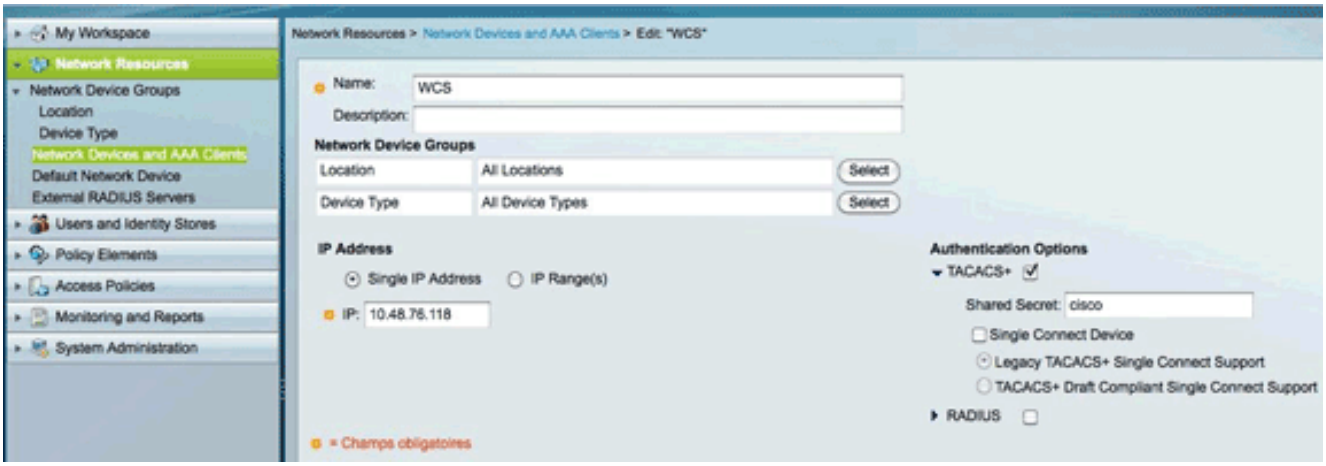
Настройка

Этот пример конфигурации описывает, как аутентифицировать пользователя с TACACS +.

Примечание: Несмотря на то, что различные варианты и возможности существуют при аутентификации пользователей WCS/NCS с Cisco Secure ACS 5.x, не, все комбинации описаны в этом документе. Однако данный пример предоставляет вам информацию, необходимую, чтобы понять, как модифицировать пример к точной конфигурации, которой вы хотите достигнуть.

Шаг 1. Добавьте WCS к клиентам AAA ACS.

1. На Cisco Secure ACS выберите **Network Resources> Network Devices и AAA Clients**.

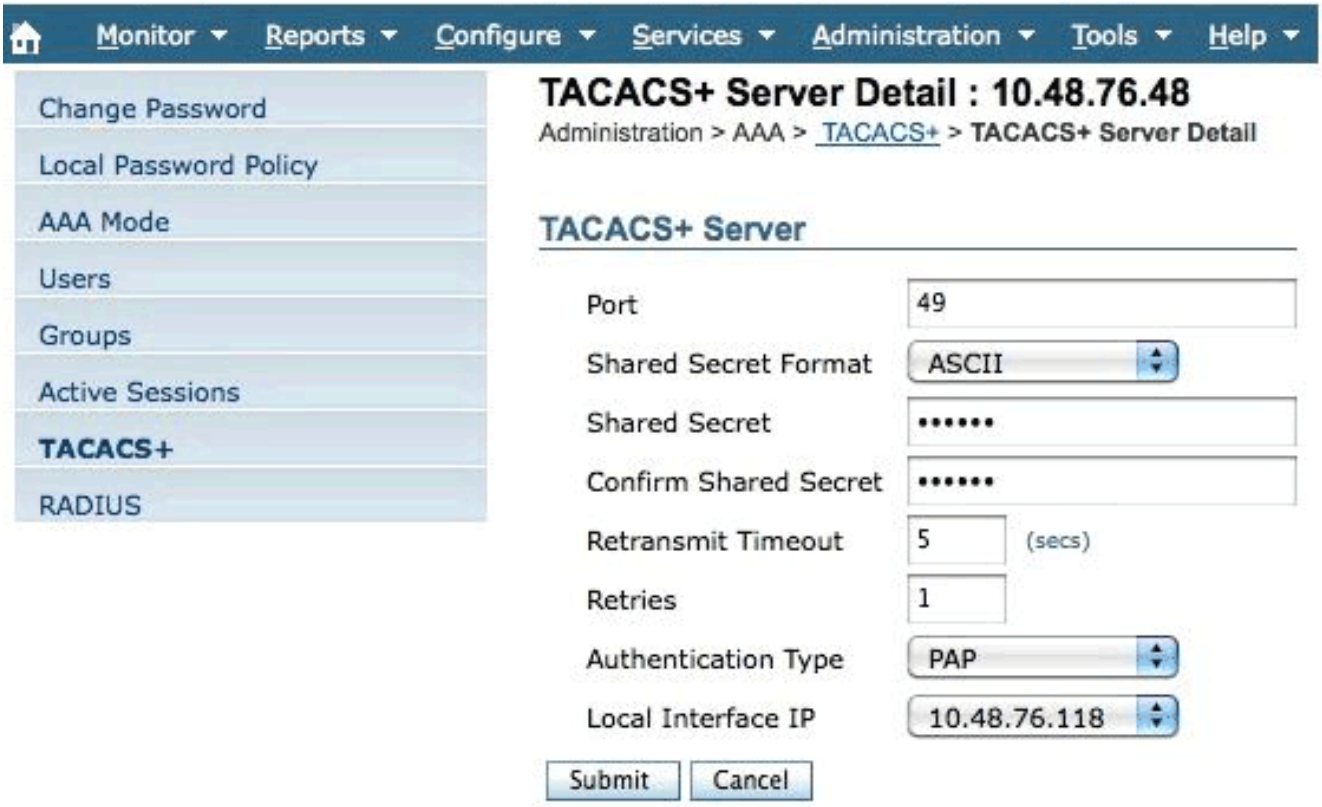


2. Введите имя в поле Name (Имя).
3. Введите IP-адрес WCS в поле IP address.
4. Под областью Authentication Options нажмите флажок **TACACS +**, чтобы включить TACACS +, и затем ввести условие, которое будет использоваться в качестве общего секретного ключа.**Примечание:** Данный пример использует *Cisco* в качестве общего секретного ключа; однако, из соображений безопасности, необходимо использовать менее очевидный термин.

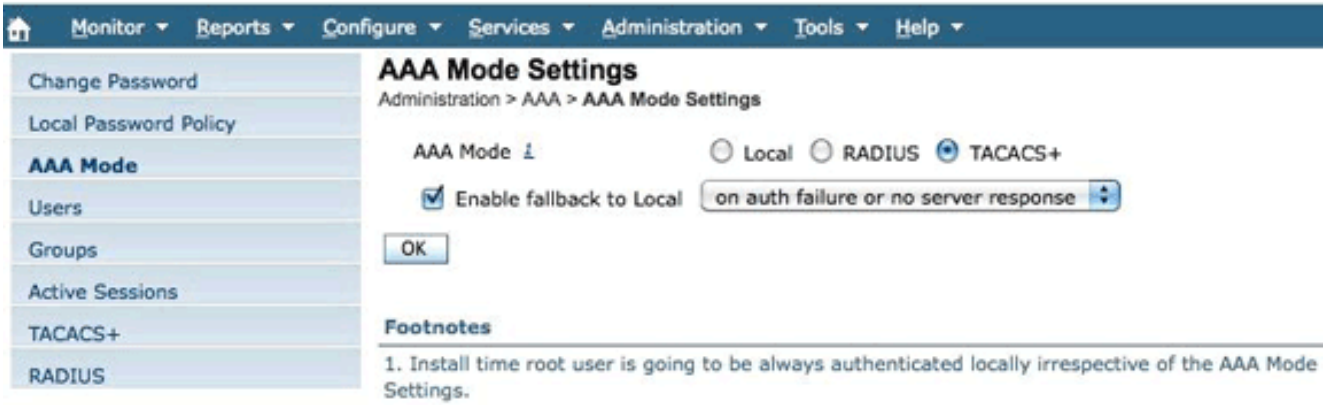
Шаг 2. Добавьте Cisco Secure ACS как TACACS + сервер в WCS.

1. Войдите к WCS и выберите **Administration> AAA**.

2. Нажмите **TACACS +**.



3. Введите свое условие общего секретного ключа в поля Shared Secret и Confirm Shared Secret.
4. Выберите Cisco ACS IP address из поля Local Interface IP.
5. На левой области навигации нажмите **AAA Mode**.



6. Нажмите кнопку с зависимой фиксацией **TACACS +**.**Примечание:** Из соображений безопасности Cisco рекомендует выбрать **на подлинном сбое или никаком ответе сервера** от Разрешать нейтрализации до локального выпадающего списка. Выбор этой опции препятствует тому, чтобы вы были заблокированы в случае проблем. Можно изменить опцию, как только все работает правильно.

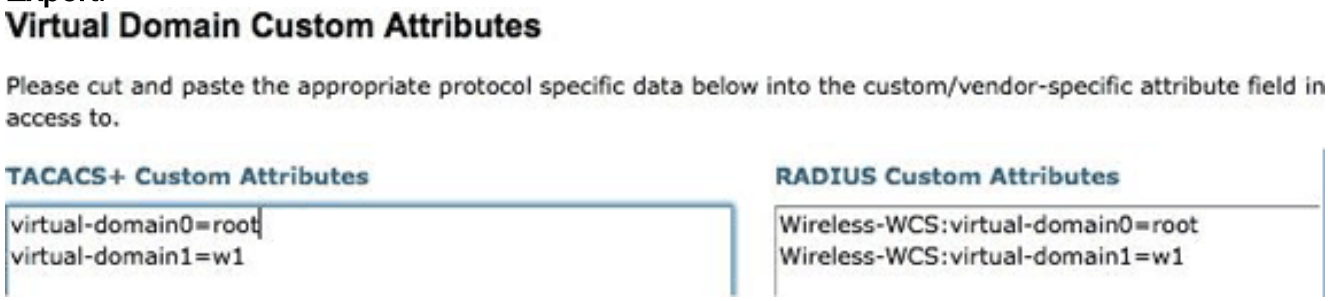
Шаг 3. Настройте корректный профиль оболочки на ACS.

Этот шаг описывает, как настроить Cisco Secure ACS для возврата корректных атрибутов для определения полномочий пользователя на WCS.

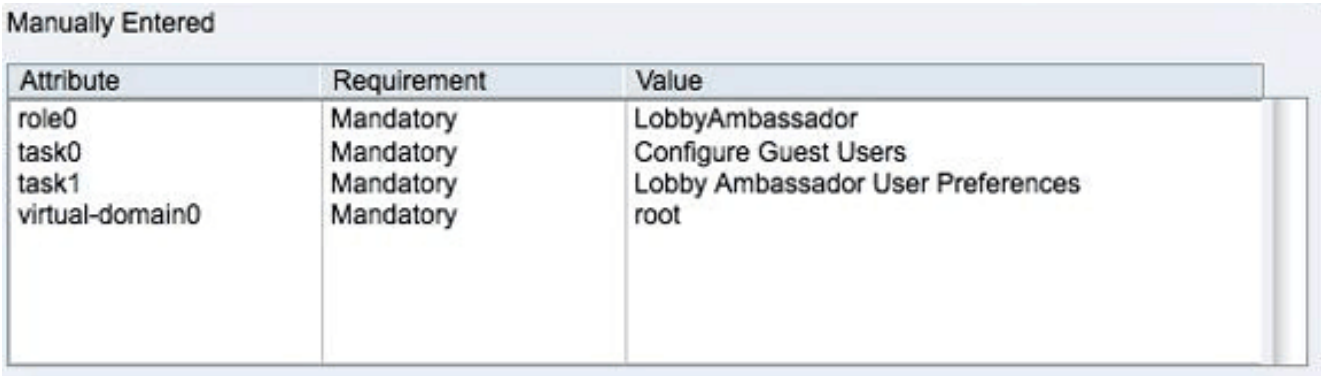
1. В левой области навигации нажмите **Groups**.Список пользовательских типов появляется. Данный пример аутентифицирует пользователя от Посла Лобби пользовательский тип.
2. Щелкните по ссылке **Листа задач** рядом с группой **LobbyAmbassador**.

Примечание: Необходимо настроить роль пользователя (Лоббируйте Посла за данный пример), и список задач, которые они могут выполнить и элементы меню, к которым они могут обратиться. При использовании последнего релиза WCS необходимо также настроить действительный домен, которому будет принадлежать пользователь.

3. Выберите **Administration> виртуальные домены**.
4. Нажмите **Export**.



5. Выберите **Policy Elements> Authorization и Permissions> Device Administration> Shell Profiles** для создания нового профиля оболочки.
6. Введите понятное имя (такое как *WCS*), и затем нажмите вкладку **Custom Attributes**.
7. Настройте атрибуты, поскольку они существуют на WCS.



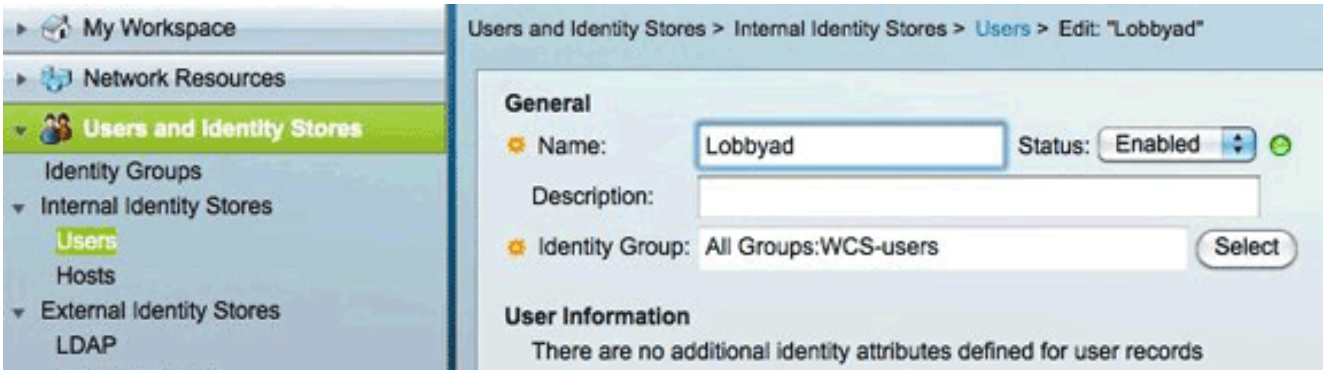
Примечание: В версиях ACS ранее, чем исправление 7 версии 5.2, вы могли бы столкнуться с проблемами при вводе задачи, которая содержит слово "предупреждение". Это исправлено в более поздних версиях ACS. Та же проблема существует в версиях платформы Identity Services Engine (ISE) ранее, чем 1.2.Вот пример того, как вручную ввести атрибуты:`-type “role0” in the “Attribute” field`
`-type “LobbyAmbassador” in the Value field`
`-click the “add” button.`

`Etc… for the other attributes.`**Примечание:** В ACS 4 это было возможно к скопировать/вставить списку атрибутов от GUI WCS до ACS 4 GUI. В ACS 5 они

должны быть введены один за другим.В NCS и Главной Инфраструктуре, атрибут должен быть введен в очень определенный заказ. Заказ является действительным доменом, ролью и списком задач. Если введено в неправильный заказ, NCS/Prime отказывается от аутентификации.`NCS:virtual-domain0=ROOT-DOMAIN`
`NCS:role0=Super Users`
`NCS:task0=View Alerts and Events`

Шаг 4. . Настройте Cisco Secure ACS для возврата атрибутов.

1. Настройте пользователя (данный пример использует *Lobbyad*) как пользователь на ACS.



Примечание: Для простоты конфигурации данный пример добавляет пользователя Lobbyad к *users group WCS*. Этот шаг не является обязательным.)

2. В Политике доступа, под **Администратором устройства по умолчанию> Авторизация**, настраивают правило совпасть с аутентификацией WCS.

3. Если имя пользователя принадлежит *users group WCS*, возвратите профиль оболочки *wcs* (который содержит атрибуты группы).
4. Если вы хотите настроить другие типы пользователей (такие как администраторы), необходимо настроить другой профиль оболочки для возврата других атрибутов. С тех пор вы должны администраторы группы в другой группе, чтобы дифференцироваться и знать что профиль оболочки возвратиться.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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

Дополнительные сведения

- Руководство по конфигурированию Cisco Wireless Control System, выпуск 7.0.172.0
- Руководство пользователя для системы управления доступом Cisco Secure Access Control System 5.2
- Cisco Systems – техническая поддержка и документация