NAC (CCA): Настройте аутентификацию на чистом Access Manager с ACS 5.x и позже

Содержание

Введение

Этот документ предоставляет сведения, как настроить аутентификацию на Clean Access Manager (CAM) с системой управления доступом Cisco Secure Access Control System (ACS) 5.x и позже. Для подобной конфигурации с помощью версий ранее, чем ACS 5.x, обратитесь к NAC (CCA): Настройка проверки подлинности Clean Access Manager (CAM) с помощью ACS.

Предварительные условия

Требования

Эта конфигурация применима к версии 3.5 CAM и позже.

Используемые компоненты

Сведения в этом документе основываются на версии 4.1 CAM.

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

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Схема сети

В настоящем документе используется следующая схема сети:

Настройте аутентификацию на CCA с ACS 5. x

Выполните следующие действия:

1. **Добавьте новые роли Создайте роль Admin**От CAM выберите **User Management> User Roles> New Role**.Введите уникальное имя, **admin**, для роли в поле Role Name.Введите **Роль пользователя Admin** как дополнительное Описание Роли.Выберите **Normal Login Role** в качестве типа роли.Настройте **Внеполосную (OOB)** VLAN роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 10.По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**.Роль теперь появляется во вкладке List of Roles как показано в VLAN Метки для Основанного на роли раздела сопоставлений OOB.**Создайте роль пользователя**От CAM выберите **User Management> User Roles> New Role**.Введите уникальное имя, **пользователей**, для роли в поле Role Name.Введите **Роль Обычного пользователя** как дополнительное Описание Роли.Настройте **Внеполосную (OOB)** VLAN роли пользователя с соответствующей VLAN. Например, выберите VLAN ID и задайте ID как 20.По окончании нажмите **Create Role**. Для восстановления свойств по умолчанию на форме нажмите **Reset**.Роль теперь появляется во вкладке List of Roles как показано в VLAN Метки для Основанного на роли раздела сопоставлений OOB.
2. **VLAN метки для Основанных на роли сопоставлений OOB**От CAM выберите **User Management> User Roles> List of Roles** для наблюдения списка ролей до сих пор.
3. **Добавьте сервер проверки подлинности RADIUS (ACS)**Выберите **User Management> Auth Servers> New**.От раскрывающегося меню Типа проверки подлинности выберите **Radius**.Введите имя поставщика как **ACS**.Введите Имя сервера как **аутентификацию. cisco . com**.**Порт сервера** — номер порта **1812**, на котором слушает сервер RADIUS.**RADIUS Type. Метод аутентификации RADIUS.** Поддерживаемые методы включают EAPMD5, PAP, CHAP, MSCHAP и MSCHAP2.**Роль по умолчанию** используется, если сопоставление с ACS не определено или установлено правильно, или если атрибут RADIUS не определен или установлен правильно на ACS.**Общий секретный ключ** — общий секретный ключ RADIUS, связанный с IP-адресом указанного клиента.**Nas-ip-address** — Это значение, которое будет передаваться со всеми пакетами Проверки подлинности RADIUS.**Нажмите Add сервер**.
4. **Сопоставьте пользователей ACS с ролями пользователя CCA**Выберите **User**

Management> Auth Servers> Mapping Rules> Add Mapping Link для сопоставления пользователя с правами администратора в ACS к роли пользователя с правами администратора CCA.Выберите **User Management> Auth Servers> Mapping Rules> Add Mapping Link** для сопоставления обычного пользователя в ACS к роли пользователя CCA.Вот сводка сопоставления роли пользователя:

5. **Включите альтернативным поставщикам на странице пользователя**Выберите **Administration> User Pages> Login Page> Add> Content**, чтобы включить альтернативным поставщикам на странице регистрационной информации пользователя для входа.

Конфигурация ACS5.x

1. Выберите **Network Resources> Network Devices и AAA Clients**, затем нажмите **Create** для добавления **CAM** как **Клиент AAA**.
2. Предоставьте **Название, IP-адрес** и выберите **RADIUS** под Параметрами проверки подлинности. Затем предоставьте **Общий секретный ключ** для **CAM** и нажмите **Submit**.
3. Выберите **Network Resources> Network Devices и AAA Clients**, затем нажмите **Create** для добавления **CAS** как **Клиент AAA**.
4. Предоставьте **Название, IP-адрес** и выберите **RADIUS** под Параметрами проверки подлинности. Затем предоставьте **Общий секретный ключ** для **CAS** и нажмите **Submit**.
5. Выберите **Network Resources> Network Devices и AAA Clients** и нажмите **Create** для добавления **ASA** как **Клиент AAA**.
6. Предоставьте **Название, IP-адрес** и выберите **RADIUS** под Параметрами проверки подлинности. Затем предоставьте **Общий секретный ключ** для **ASA** и нажмите **Submit**.
7. Выберите **Users и Identity Stores> Identity Groups** и нажмите **Create** для создания новой Identity Group.
8. Предоставьте **Имя группы** и нажмите **Submit**.
9. Выберите **Users и Identity Stores> Identity Groups** и нажмите **Create** для создания новой Identity Group.
10. Предоставьте **Имя группы** и нажмите **Submit**.
11. Выберите **Users и Identity Stores>> Users Internal Identity Stores** и нажмите **Create** для создания нового пользователя.
12. Предоставьте **Имя** пользователя и измените состав группы на **Административную группу**. Затем предоставьте **пароль** и подтвердите пароль. **Нажмите кнопку Submit (Отправить).**
13. Выберите **Users и Identity Stores>> Users Internal Identity Stores** и нажмите **Create** для создания нового пользователя.
14. Предоставьте **Имя** пользователя и измените состав группы на **Users group**. Затем предоставьте **пароль** и подтвердите пароль. **Нажмите кнопку Submit (Отправить).**
15. Выберите **Policy Elements> Authorization и Permissions> Network Access> Authorization Profiles** и нажмите **Create** для создания **нового профиля авторизации**.
16. Предоставьте **Имя профиля** и нажмите **RADIUS Attributes**.
17. От вкладки **атрибутов RADIUS** выберите **RADIUS-IETF** в качестве **Типа словаря**. Затем нажмите **Select**, следующий за **атрибутом RADIUS**.
18. Выберите **Атрибут Class** и нажмите **OK**.
19. Гарантируйте, что **Значение атрибута Статично**, и введите **Admin** как значение. **Нажмите Add**, затем нажмите **Submit**.

20. Выберите **Policy Elements> Authorization и Permissions> Network Access> Authorization Profiles** и нажмите **Create** для создания **нового профиля авторизации**.
21. Предоставьте **Имя профиля** и нажмите **RADIUS Attributes**.
22. От вкладки **атрибутов RADIUS** выберите **RADIUS-IETF** в качестве **Типа словаря**. Затем нажмите **Select**, следующий за **атрибутом RADIUS**.
23. Выберите **Атрибут Class** и нажмите **OK**.
24. Гарантируйте, что **Значение атрибута Статично**, и введите **Пользователей** как значение. **Нажмите Add**, затем нажмите **Submit**.
25. Выберите **Access Policies> Access Services> Service Selection Rules** и определите, какой сервис обрабатывает **Запрос RADIUS**. В данном примере сервисом является **Доступ к сети по умолчанию**.
26. Выберите **Acces Policies> Access Services> Default Network Access** (сервис, определенный в предыдущем шаге, который обработал Запрос RADIUS)**,> Авторизация**. Нажмите **Customize**.
27. **Move Identity Group** от **Доступного** до **Выбранного столбца**. **Нажмите кнопку OK.**
28. Нажмите **Create** для создания нового правила.
29. Гарантируйте, что **Идентификационный** флажок **Флажка Группа** установлен, затем нажмите **Select**, следующий за **Identity Group**.
30. Выберите **Административную группу** и нажмите **OK**.
31. Нажмите **Select** в разделе **Профилей Авторизации**.
32. Выберите **Admin Authorization Profile** и нажмите **OK**.
33. Нажмите **Create** для создания нового правила.
34. Гарантируйте, что **Идентификационный** флажок **Флажка Группа** установлен, и нажмите **Select**, следующий за Identity Group..
35. Выберите **Users group** и нажмите **OK**.
36. Нажмите **Select** в разделе **Профилей Авторизации**.
37. Выберите **Users Authorization Profile** и нажмите **OK**.
38. **Нажмите кнопку OK.**
39. **Нажмите кнопку Save Changes (Сохранить изменения).**

Устранение неполадок

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

Дополнительные сведения

- Поддержка устройства Cisco NAC
- Система управления доступом Cisco Secure Access Control System
- Cisco Systems – техническая поддержка и документация