NAC (CCA) 4.x: Пример конфигурации сопоставления пользователей с определенными ролям при помощи LDAP

Содержание

Введение

Этот документ описывает функцию сопоставления Протокола LDAP для сопоставления пользователей с определенными ролями в Устройстве Network Admission Control (NAC) или Cisco Clean Access (CCA).

Устройство Cisco NAC (раньше Cisco Clean Access) является легко развернутым продуктом NAC, который использует инфраструктуру сети для обеспечивания соблюдения политики безопасности на всех устройствах, которые ищут на вычислительные ресурсы доступа к сети. С NAC-устройством, администраторы сети могут аутентифицировать, авторизовать, оценить, и перепромежуточный соединенный проводом, радио, и удаленные пользователи и их машины перед доступом к сети. Это определяет, совместимы ли сетевые устройства, такие как портативные ПК, IP-телефоны или игровые приставки с политикой безопасности вашей сети, и восстанавливает любые уязвимости прежде, чем разрешить доступ к сети.

Предварительные условия

Требования

Этот документ предполагает, что Менеджер CCA, Сервер CCA и Сервер LDAP установлены и работают должным образом.

Используемые компоненты

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

- Устройство Cisco NAC, серии 3300 - чистит Access Manager 4.0
- Устройство Cisco NAC, серии 3300 - чистый сервер доступа 4.0

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.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Аутентификация против Active Directory бэкэнда

Несколько типов опознавательных поставщиков в Чистом Access Manager могут использоваться для аутентификации пользователей против сервера Active Directory (AD), составляющего собственность сервиса каталогов Microsoft. Они включают Windows NT (NTLM), Kerberos и (предпочтенный) LDAP.

При использовании LDAP для соединения с AD, Поиск (Admin), Полное составное имя (DN), как правило, должно устанавливаться в DN учетной записи или с администраторскими привилегиями или с привилегиями рядового пользователя. Первая запись общего имени (CN) должна быть администратором AD или пользователем с привилегиями чтения. Обратите внимание на то, что поисковый фильтр, SAMAccountName, является названием регистрационной информации пользователя для входа в AD схеме по умолчанию.

Пример AD/конфигурации LDAP

Это иллюстрирует пример конфигурации с помощью LDAP для передачи с Active Directory бэкэнда:

1. Создайте пользователя Администратора домена в Пользователях и компьютерах Active Directory. Разместите этого пользователя в Папку Пользователи.
2. В Пользователях и компьютерах Active Directory выберите **Find** из Меню действий.Удостоверьтесь, что ваши результаты показывают столбец Group Membership для созданного пользователя. Ваши результаты поиска должны показать **пользователю** и связанному **Составу группы** в рамках Active Directory. Это - информация, которую необходимо будет передать в Чистый Access Manager.
3. От Чистого веба - консоли Access Manager перейдите **к Управлению пользователями> Серверы проверки подлинности> Новая** форма **Сервера**.
4. Выберите **LDAP** в качестве типа сервера.
5. Для **Поиска (Admin) Полный DN** и **Поисковые Основные поля Context**, введите результаты Находки в Пользователях и компьютерах Active Directory.
6. Эти поля - все, что необходимо для надлежащего устанавливания этого сервера

проверки подлинности в CAM:**ServerURL**: ldap://192.168.137.10:389 - Это - IP-адрес контроллера домена и порт прослушивания LDAP.**Поиск (Admin) Полный DN**: CN=sheldon muir, Cn=Users, DC=domainname, DC=com**Поисковый основной контекст**: DC=domainname, DC=com**Роль по умолчанию**: Выберите роль по умолчанию, в которую будет помещен пользователь когда-то аутентифицируемый.**Описание:** Используемый только для ссылки.**Название поставщика**: Это - название Сервера LDAP, используемого для настройки Страницы пользователя на CAM.**Поисковый Пароль**: пароль домена muir's sheldon**Поисковый фильтр**: $user$ SAMAccountName=

7. **Нажмите Add сервер**.На этом этапе ваш Подлинный Тест должен работать.
8. Чтобы к тестовой аутентификации:От **вкладки User Management> Auth Servers> Auth Test** выберите поставщика, против которого вы хотите протестировать учетные данные в списке **Поставщика**. Если поставщик не появляется, удостоверьтесь, что это правильно настроено во вкладке **List of Servers**.Введите имя пользователя и пароль для пользователя и в случае необходимости значения ИДЕНТИФИКАТОРА VLAN.Нажмите **Authenticate**.Результаты тестирования появляются у основания окна.**Аутентификация выполнена успешно:**Для любого типа поставщика, Результата: когда подлинный тест успешно выполняется, успешная Аутентификация и Роль пользователя отображена.Для LDAP/СЕРВЕРОВ RADIUS, когда аутентификация успешна и настроены сопоставляющие правила, атрибуты/значения, заданные в правиле сопоставления, также отображены, если сервер проверки подлинности (LDAP/RADIUS) возвращает те значения. Пример:`Result: Authentication successful`
`Role: <role name>`
`Attributes for Mapping:`
`<Attribute Name>=<Attribute value>` **Отказавшая аутентификация:**Когда аутентификация отказывает, индикаторы сообщения наряду с Аутентификацией подведенный результат как показано.

Сопоставьте пользователей с ролями Использование атрибутов или ИДЕНТИФИКАТОРОВ VLAN

Формы Правил **Сопоставления** могут использоваться для сопоставления пользователей в роль (роли) пользователя на основе этих параметров:

- ИДЕНТИФИКАТОР VLAN трафика пользователя, который происходит из недоверяемой стороны CAS (все типы сервера проверки подлинности)
- Опознавательные атрибуты прошли от LDAP и серверов проверки подлинности RADIUS (и атрибуты RADIUS прошли от Концентраторов Cisco VPN),

Например, если у вас есть две компании пользователей на той же IP-подсети, но с другими привилегиями доступа к сети, такими как беспроводные сотрудники и студенты, можно использовать атрибут от Сервера LDAP для сопоставления одной компании пользователей в роль индивидуального пользователя. Можно тогда создать политику трафика, чтобы позволить доступ к сети одной роли и запретить доступ к сети к другим ролям.

Устройство Cisco NAC выполняет последовательность сопоставления как показано:

Устройство Cisco NAC позволяет администратору задавать сложные булевы выражения при определении сопоставляющих правил для Kerberos, LDAP и Серверов проверки подлинности RADIUS. Сопоставляющие правила разломаны на условия, и можно

использовать булевы выражения для объединения многопользовательских атрибутов и ID несколько интерфейсов VLAN для сопоставления пользователей в роли пользователя. Сопоставление правил может быть создано для диапазона ИДЕНТИФИКАТОРОВ VLAN, и соответствия атрибута могут быть сделаны нечувствительными к регистру. Это позволяет множественным условиям быть гибко настроенными для правила сопоставления.

Правило сопоставления включает подлинный тип поставщика, выражение правила и роль пользователя, в которую можно сопоставить пользователя. Выражение правила включает один или комбинация условий, с которыми параметры пользователя должны совпасть, чтобы быть сопоставленными в роль указанного пользователя. Условие состоит из типа условия, исходного названия атрибута, оператора и значения атрибута, против которого совпадают с определенным атрибутом.

Для создания правила сопоставления вы сначала добавляете (сохраняют) условия настроить выражение правила. Затем как только выражение правила создано, можно добавить правило сопоставления к серверу проверки подлинности для роли указанного пользователя.

Сопоставление правил может располагаться каскадом. Если источник имеет несколько правил сопоставления, правила оценены в заказе, в котором они появляются в списке правил сопоставления. Роль для первого положительного правила сопоставления используется. Как только правило встречено, другие правила не протестированы. Если никакое правило не истинно, роль по умолчанию для того источника аутентификационной информации используется.

Настройте правило сопоставления

Выполните следующие действия:

1. Перейдите **к Управлению пользователями> Серверы проверки подлинности> Сопоставляющие Правила** и нажмите **Добавлять** ссылку **Правила Сопоставления** для сервера проверки подлинности.**Добавить** форма **Правила Сопоставления** появляется.
2. Настройте условия для сопоставления правила (A):**Название поставщика** — Название Поставщика устанавливает поля формы Правил Сопоставления для того типа сервера проверки подлинности. Например, форма только позволяет ИДЕНТИФИКАТОР VLAN, сопоставляющий конфигурацию правила для Kerberos, Windows NT, Windows NetBIOS SSO и типов сервера проверки подлинности S/Ident. Форма позволяет ИДЕНТИФИКАТОР VLAN или Атрибут, сопоставляющий конфигурацию правила для RADIUS, LDAP и типов аутентификации SSO VPN Cisco.**Тип условия** — Настраивает и добавляет условия сначала (шаг A в рисунок) прежде, чем добавить правило сопоставления. Выберите один из них из выпадающего меню для установки полей формы Условия:**Атрибут** — Для LDAP, RADIUS, поставщики аутентификации SSO VPN Cisco только.**ИДЕНТИФИКАТОР VLAN** — Все типы сервера проверки подлинности.Для типа условия ИДЕНТИФИКАТОРА VLAN (см. рисунок), это поле называют **Именем свойства**. По умолчанию это заполнено с "ИДЕНТИФИКАТОРОМ VLAN" (и отключено для редактирования).**Название атрибута** — Для Серверов LDAP (см. рисунок), **Название атрибута** является текстовым полем, в которое вы вводите исходный атрибут, который вы хотите протестировать. Название должно быть идентично (регистрозависимый) к названию атрибута, который передает источник аутентификационной информации, пока вы не выбираете**, равняние игнорируют**

оператора **случая** для создания условия.**Значение атрибута** — Вводит значение, которое будет протестировано против исходного **Названия атрибута**.**Оператор (Атрибут)** — Выбирает оператора, который определяет тест исходной строки атрибута:если значение **Названия атрибута** совпадает **со Значением атрибута, равняется** — Истинный.если значение **Названия атрибута** не совпадает **со Значением атрибута, не равняется** — Истинный.если значение **Названия атрибута** содержит **Значение атрибута, содержит** — Истинный.если значение **Названия атрибута** начинается **со Значения атрибута, запускается с** — Истинный.**концы с** — Истинный, если значение **Названия атрибута** заканчивается **Значением атрибута**.**равняется игнорируют регистр** — Истинный, если значение **Названия атрибута** совпадает со строкой **Значения атрибута**. Не имеет значения, является ли строка прописной или строчной.**Оператор (ИДЕНТИФИКАТОР VLAN)** — Если вы выбираете VLAN ID в качестве **Типа Условия**, выбираете одного из этих операторов для определения условия, которое тестирует против целых чисел ИДЕНТИФИКАТОРА VLAN:если ИДЕНТИФИКАТОР VLAN совпадает с ИДЕНТИФИКАТОРОМ VLAN в поле **Property Value, равняется** — Истинный.если ИДЕНТИФИКАТОР VLAN не совпадает с ИДЕНТИФИКАТОРОМ VLAN в поле **Property Value, не равняется** — Истинный.если ИДЕНТИФИКАТОР VLAN находится в пределах диапазона значений, настроенных для поля **Property Value, принадлежит** — Истинный. Значением должны быть разделенные ИДЕНТИФИКАТОРЫ VLAN одной или более запятых. Диапазоны ИДЕНТИФИКАТОРОВ VLAN могут быть заданы дефисом (-), например, [2,5,7,100-128,556-520]. Только целые числа могут быть введены, не строки. Обратите внимание на то, что скобки являются дополнительными.**Пример:Добавьте Условие (Сохраните Условие)** —, Удостоверяются, что настроили условие, затем **нажмите Add Условие** для добавления условия к выражению правила (иначе конфигурация не сохранена).

3. Добавьте Правило Сопоставления к Роли (B): Добавьте правило сопоставления (**шаг B** в рисунок) после того, как вы настроите и добавите условие (условия).**Имя роли** — после добавления по крайней мере одного условия выберите роль пользователя, к которой вы примените сопоставление из выпадающего меню.**Приоритет** — Выбирает приоритет от выпадающего для определения заказа, в котором протестированы сопоставляющие правила. Первое правило, которое оценивает к истине, используется для присвоения пользователя роль.**Выражение правила** — для способствования настройке условных операторов для правила сопоставления, это поле отображает содержание последнего Условия, которое будет добавлено. После добавления условия (условий) необходимо **нажмите Add Правило Сопоставления** для сохранения всех условий к правилу.**Описание** Дополнительное описание правила сопоставления.**Добавьте Сопоставление (Сохраните Сопоставление)** —, Нажимают эту кнопку, когда сделано добавляя условия создать правило сопоставления для роли. Необходимо Добавить или Сохранить сопоставление на указанную роль, или конфигурация и условия не будут сохранены.

Отредактируйте правила сопоставления

- **Приоритет** — для изменения приоритета сопоставления управляет позже, нажимает/стрелка вниз рядом с записью в **Управлении пользователями> Серверы проверки подлинности> Список Серверов**. Приоритет определяет заказ, в котором протестированы правила. Первое правило, которое оценивает к истине, используется

для присвоения пользователя на роль.
- **Edit** — Нажмите кнопку Edit рядом с правилом модифицировать правило сопоставления или удалить условия из правила. Обратите внимание на то, что при редактировании составного условия, условия внизу (создал позже) не отображены. Это должно избежать петель.
- **Delete** — Нажмите кнопку delete рядом с записью Правила Сопоставления для сервера проверки подлинности для удаления того отдельного правила сопоставления. Нажмите кнопку delete рядом с условием на Редактировании, сопоставляющем форму правила для удаления того условия из Правила Сопоставления. Обратите внимание на то, что вы не можете удалить условие, которое зависит от другого правила в составном операторе. Для удаления отдельного условия необходимо удалить составное условие сначала.

Устранение неполадок

Если сопоставление AD пользователя к роли пользователя CCA не работает, затем удостоверьтесь, что вы сопоставляете пользователей с ролью на основе атрибутов с Названиями атрибута = memberof, Operator=contains и Значение атрибута = (имя группы).

Дополнительные сведения

- Страница технической поддержки устройства Cisco NAC
- Cisco Systems – техническая поддержка и документация