ACS ограниченный пользовательский доступ с RADIUS на примере конфигурации Nexus

Содержание

Введение

Этот документ описывает, как предоставить ограниченный доступ пользователям Nexus так, чтобы они могли только ввести ограниченные команды с сервером Cisco Secure Access Control Server (ACS) как сервер RADIUS. Например, вы могли бы хотеть, чтобы пользователь был в состоянии войти к привилегированному или режиму конфигурации и только быть позволенными ввести интерфейсные команды. Для достижения этого необходимо создать настраиваемую роль для пользователя на сервере RADIUS, который используется.

Предварительные условия

Требования

Сервер RADIUS (ACS в данном примере) и Nexus должен быть в состоянии связаться друг с другом и выполнить аутентификации.

Используемые компоненты

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

- Версия ACS 5. x
- Коммутаторы Nexus 7000

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

Конфигурация настраиваемых ролей на Nexus

Для создания роли, которая только предоставляет доступ для чтения-записи для интерфейсной команды, войдите:

```
switch(config)# role name Limited-Access
switch(config-role)# rule 1 permit read-write feature interface
```

Дополнительные правила доступа разрешения определены с этим синтаксисом:

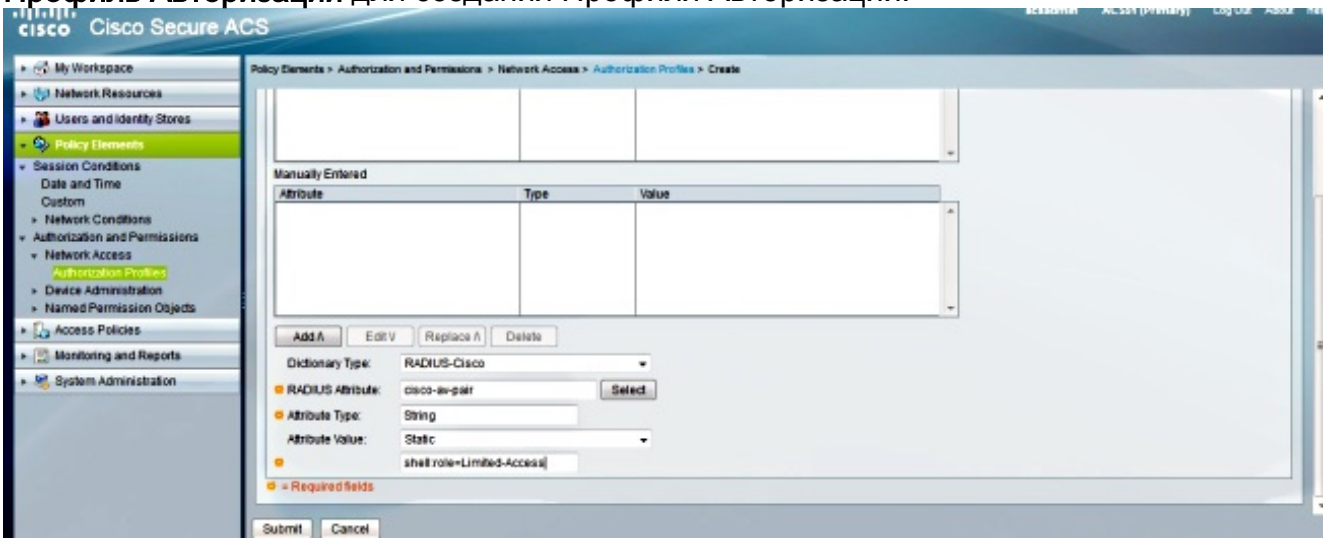
```
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmp
TargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmp
TargetAddrEntry
```

Настройте Nexus для проверки подлинности и авторизация

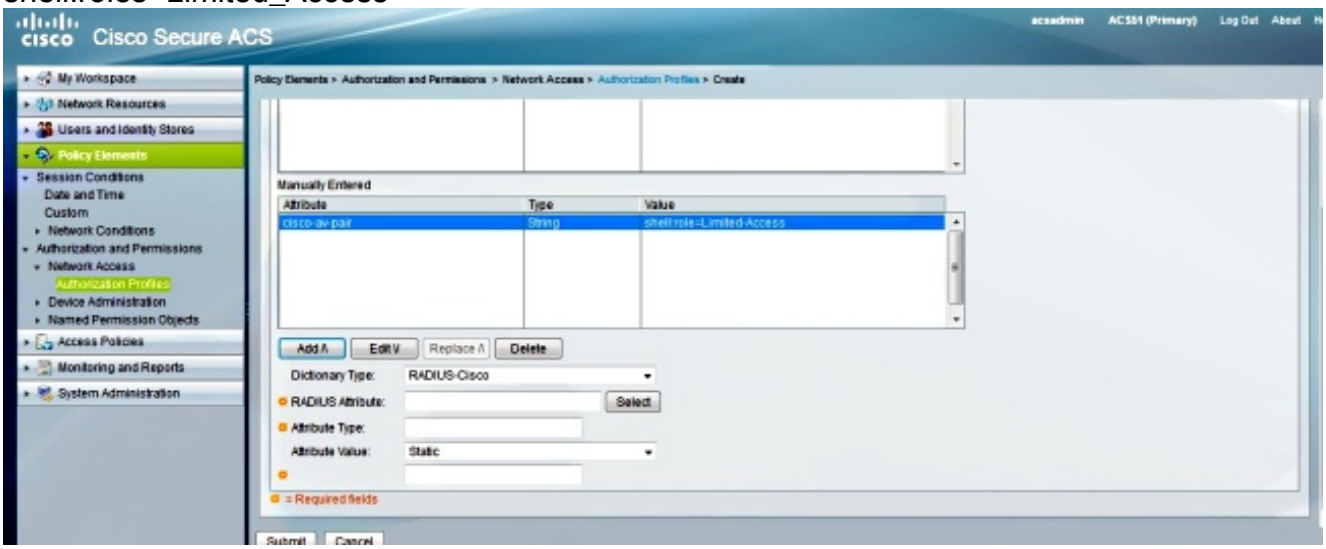
1. Для создания локального пользователя на коммутаторе с полными полномочиями для нейтрализации введите команду **имени пользователя**:
   `Switch(config)#username admin privilege 15 password 0 cisco123!`
2. Для обеспечения IP-адреса сервера RADIUS (ACS) войдите:
   ```
   switch# conf terminal
   switch(config)# Radius-server host 10.10.1.1 key cisco123
   authenticationaccounting
   switch(config)# aaa group server radius RadServer
   switch(config-radius)#server 10.10.1.1
   switch(config-radius)# use-vrf Management
   ```
   Примечание: Ключ должен совпасть с Общим секретным ключом, настроенным на сервере RADIUS для этого устройства Nexus.
3. Для тестирования доступности сервера RADIUS введите **команду test aaa**:
   `switch# test aaa server Radius 10.10.1.1 user1 Ur2Gd2BH`Тестовая аутентификация должна отказать с Отклонением от сервера, так как это еще не настроено. Однако это подтверждает, что сервер достижим.
4. Для настройки login authentication войдите: `Switch(config)#aaa authentication login default group Radserver`
   `Switch(config)#aaa accounting default group Radserver`
   `Switch(config)#aaa authentication login error-enable`Вы не должны волноваться о локальном методе нейтрализации здесь, потому что нейтрализации Nexus к локальной переменной самостоятельно, если сервер RADIUS недоступен.

Конфигурация ACS

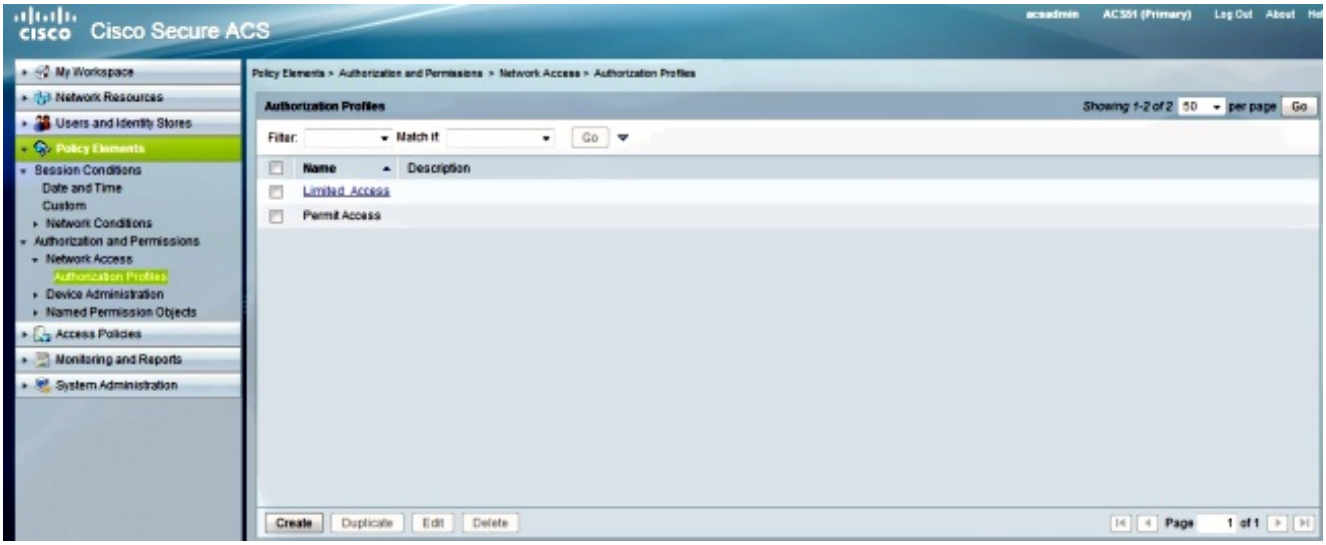
1. Перейдите к **Элементам Политики> Аутентификация и Разрешения> Доступ к сети> Профиль Авторизации** для создания Профиля Авторизации.



2. Введите имя для профиля.
3. Под вкладкой **Custom Attributes** введите эти значения:
   Тип словаря: Cisco радиусаАтрибут: Cisco-av-pairТребование: обязательныйЗначение: shell:roles=Limited_Access



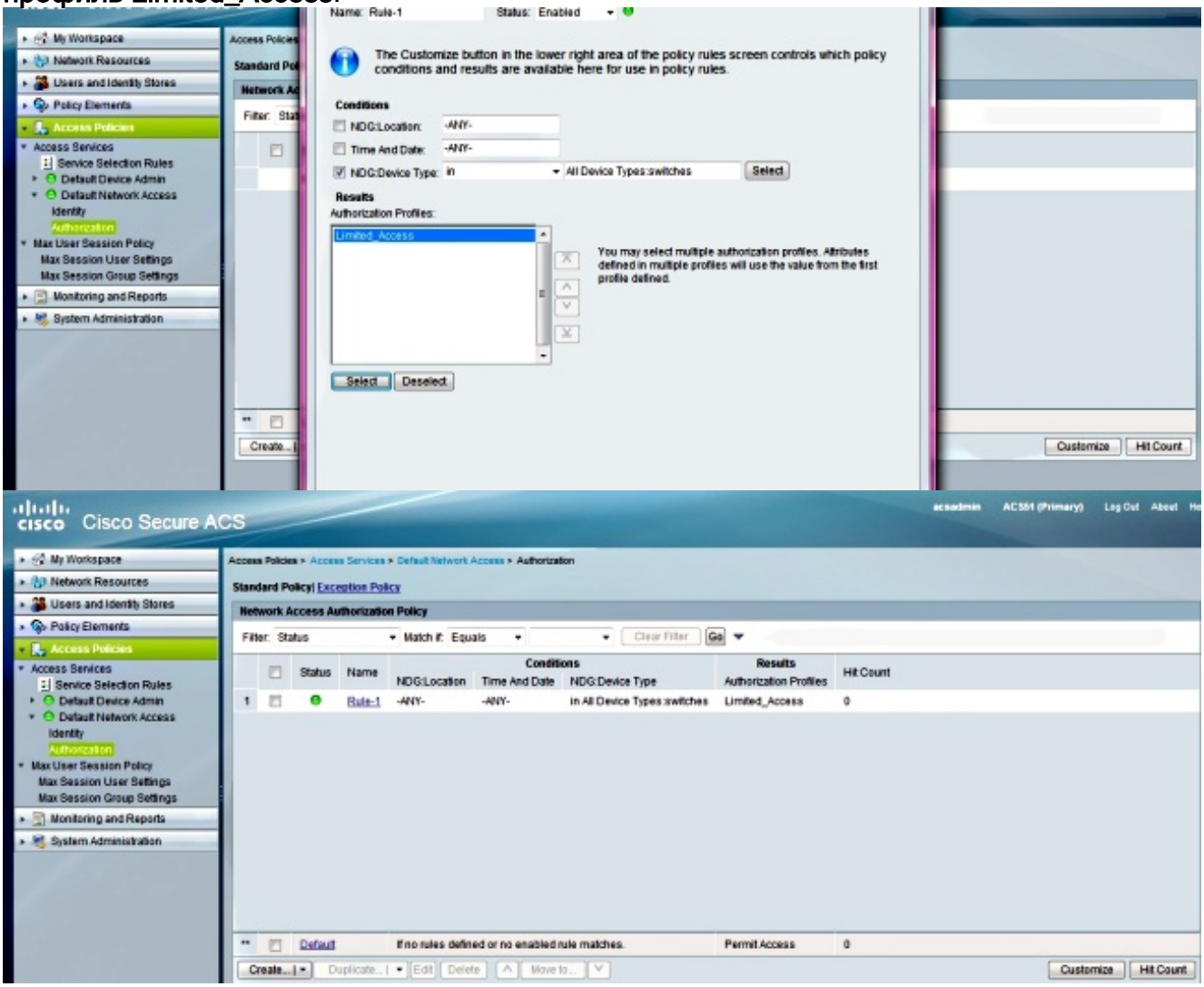
4. Отправьте изменения для создания основанной на атрибуте роли для коммутатора Nexus.



5. Создайте новое правило авторизации или отредактируйте текущее правило в корректной политике доступа. Запросы RADIUS обработаны Политикой Доступа к сети

по умолчанию.

6. В области **Conditions** выберите соответствующие условия. В области **Results** выберите **профиль Limited_Access**.



7. **Нажмите кнопку ОК.**

Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

Проверка роли Nexus

Введите **команду show role** в Nexus для отображения определенных ролей и правил настроенного адреса.

```
switch# show role  (Displays all the roles and includes
custom roles that you have created and their permissions.)

Role: network-admin

Description: Predefined network admin role has access to all
commands on the switch.
------------------------------------------------------------------
Rule Perm Type Scope Entity
```

```
-------------------------------------------------------------------
1 permit read-write

Role:Limited_Access
Description: Predefined Limited_Access role has access to these commands.
-------------------------------------------------------------------
Rule Perm Type Scope Entity
-------------------------------------------------------------------
1 permit read-write feature Interface
```

Проверка присвоения роли пользователя Nexus

Войдите к Nexus с именем пользователя и паролем, настроенным на ACS. После входа в систему введите **команду show user-account**, чтобы проверить, что у тестового пользователя есть роль Limited_Access:

```
switch# show user-account
user:admin
this user account has no expiry date
roles:network-admin

user:Test
this user account has no expiry date
roles:Limited_Access
```

Как только пользовательская роль доступа подтверждена, коммутатор в режим конфигурации и попытку ввести команду кроме интерфейсной команды. Пользователю нужно запретить доступ.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

- **show role** - Отображает определение роли и правила настроенного адреса.
- **show user-account** - Отображает подробные данные учетной записи пользователя и включает присвоение роли.

Устранение неполадок

Этот раздел предоставляет сведения, можно использовать для устранения проблем конфигурации коммутатора.

Выполните эти шаги на коммутаторе для присвоения роли:

1. Проверьте, какая группа AAA используется для аутентификации с **командами show running-config aaa и show aaa authentication**.
2. Для RADIUS проверьте Виртуальную маршрутизацию и Передачу (VRF) ассоциация с группой AAA с **командами show aaa authentication и show running-config radius**.
3. Если эти команды проверяют, что ассоциация корректна, введите **debug radius вся** команда для включения регистрации трассировки.
4. Проверьте, что корректные атрибуты выдвигаются от ACS.

Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных**

данных, чтобы просмотреть анализ выходных данных команды show.

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

- show running-config aaa -
- show aaa authentication -
- show running-config radius
- debug radius все