# Интеграция Nexus с примером конфигурации ACS 5.2

## Содержание



## Введение

Этот документ предоставляет пример TACACS + конфигурация аутентификации на коммутаторе Nexus. По умолчанию при настройке коммутатора Nexus для аутентификации через Access Control Server (ACS), вы автоматически размещены в network-operator/vdc-operator роль, которая предоставляет доступ только на чтение. Чтобы быть размещенными в network-admin/vdc-admin роль, необходимо создать оболочку на ACS 5.2. Этот документ описывает тот процесс.

## Предварительные условия

### Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Определите свой коммутатор Nexus как клиента в ACS.
- Определите IP-адрес и идентичный общий секретный ключ на ACS и Nexus.

**Примечание:** Создайте контрольную точку или резервную копию на Nexus перед внесением любых изменений.

### Используемые компоненты

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

- ACS 5.2
- Nexus 5000, 5.2 (1) N1 (1)

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.

### Устройство Nexus для проверки подлинности и авторизация с конфигурацией ACS 5.2

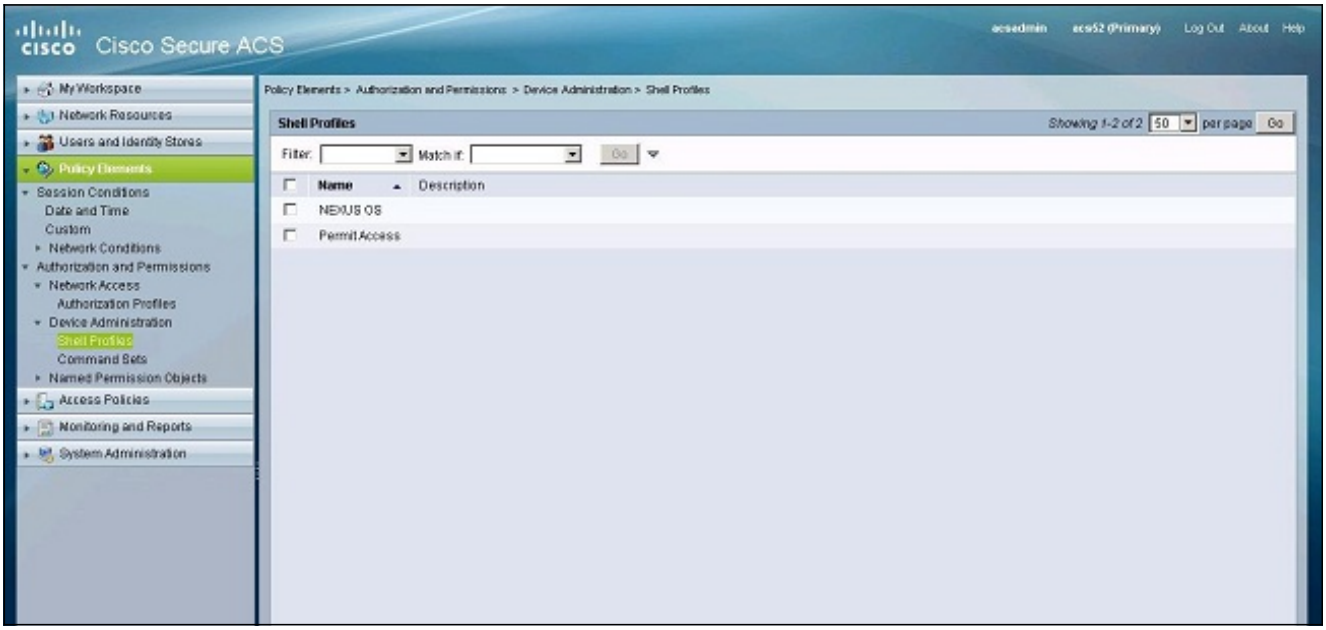
Выполните следующие действия:

1. Создайте локального пользователя на коммутаторе Nexus с полными полномочиями для нейтрализации:
   ```
   username admin privilege 15 password 0 cisco123!
   ```
2. Включите TACACS +, затем предоставьте IP-адрес TACACS + Сервер (ACS):
   ```
   feature tacacs+
   tacacs-server host IP-ADDRESS key KEY
   tacacs-server key KEY
   tacacs-server directed-request
   aaa group server tacacs+ ACS
   server IP-ADDRESS
   use-vrf management
   source-interface mgmt0
   ```
   **Примечание:** Ключ должен совпасть с общим секретным ключом, настроенным на ACS для этого устройства Nexus.
3. Протестируйте доступность Сервера tacacs:
   `test aaa group group-name username password` Тестовая аутентификация должна отказать с сообщением отклонения от сервера, так как не был настроен сервер. Это сообщение отклонения подтверждает, что TACACS + сервер достижим.
4. Настройте login authentication:
   ```
   aaa authentication login default group ACS
   aaa authentication login console group ACS
   aaa accounting default group ACS
   aaa authentication login error-enable
   aaa authorization commands default local
   aaa authorization config-commands default local
   ```
   **Примечание:** Если сервер проверки подлинности недостижим, Nexus использует локальную проверку подлинности.

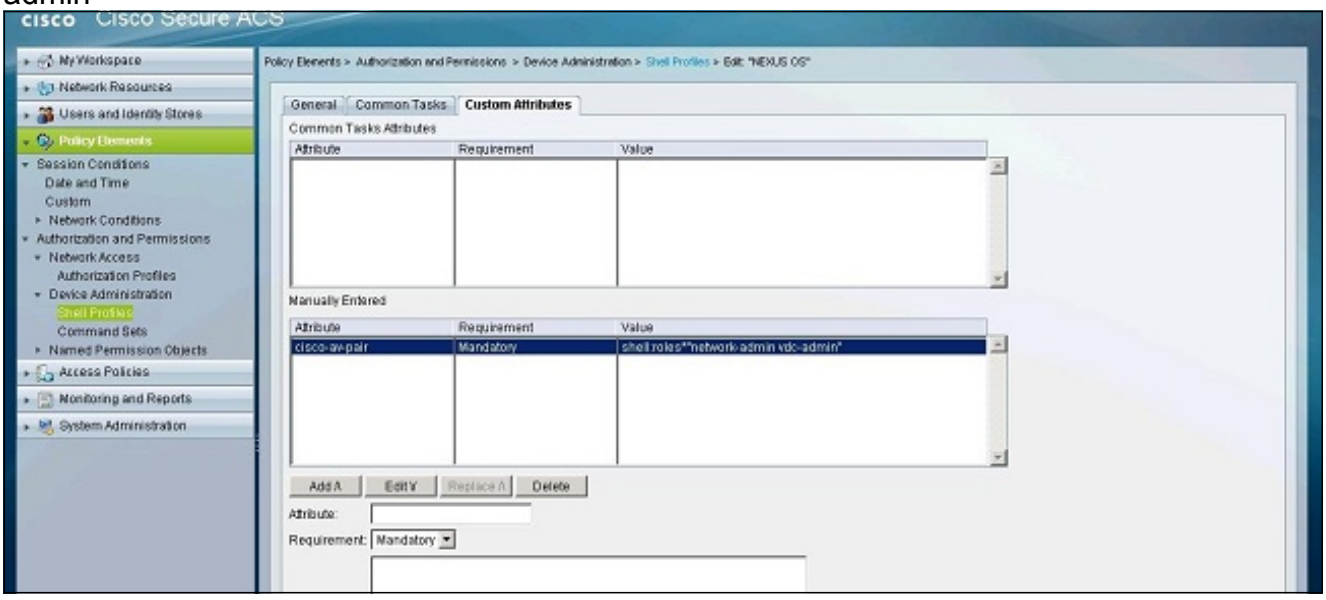
## ACS 5.x конфигурация

Выполните следующие действия:

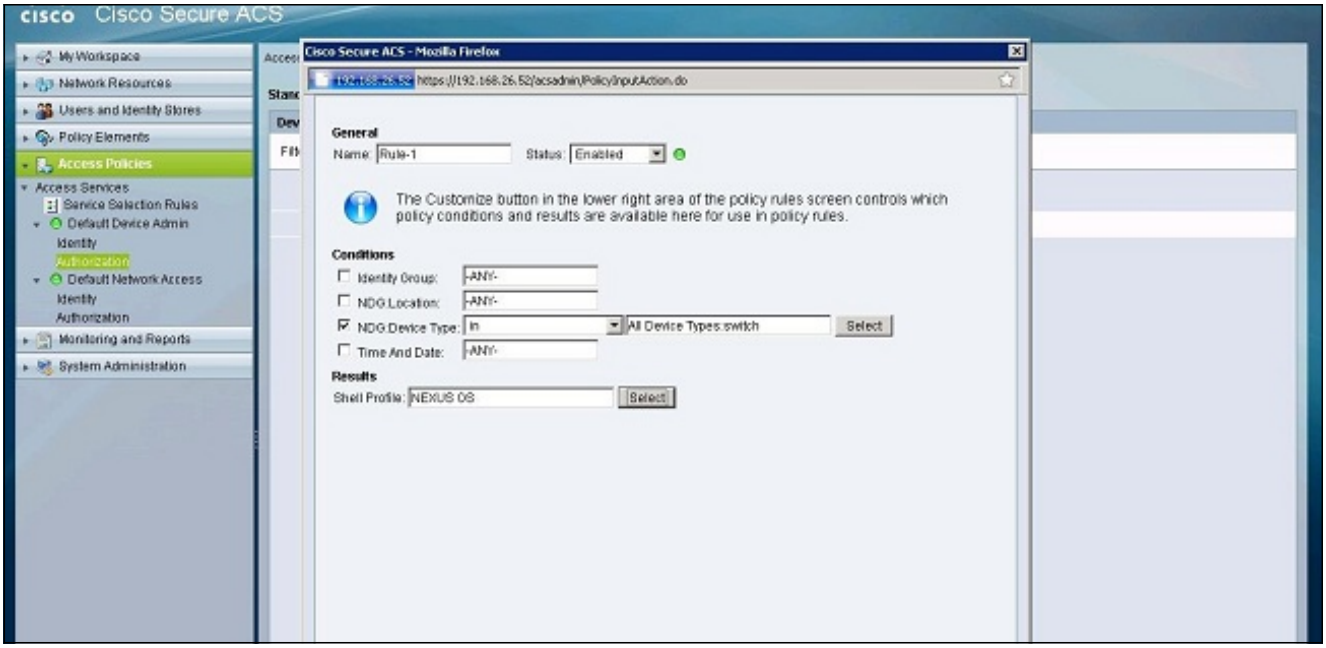
1. Перейдите к **Элементам Политики> Аутентификация и Разрешения> Администрирование устройств> Профили Shell** для создания Профиля Shell.




2. Введите имя для профиля.
3. Под вкладкой Custom Attributes введите эти значения:Атрибут: Cisco-av-pairТребование: обязательныйЗначение: shell:roles* "admin vdc сетевого admin"




4. Отправьте изменения для создания основанной на атрибуте роли для коммутатора Nexus.
5. Создайте новое правило авторизации или отредактируйте существующее правило в корректной политике доступа. По умолчанию TACACS + запросы обработаны политикой доступа Администратора устройства по умолчанию.
6. В области Conditions выберите соответствующие условия. В области Results выберите Nexus профиль оболочки
   ОС.




7. **Нажмите кнопку ОК.**

# Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

- show tacacs + — Отображает TACACS + статистика.
- show running-config tacacs + — Отображает TACACS + конфигурация в рабочей конфигурации.
- show startup-config tacacs + — Отображает TACACS + конфигурация в загрузочной конфигурации.
- show tacacs-server — Отображает весь настроенный TACACS + параметры сервера.

# Дополнительные сведения

- Cisco Systems – техническая поддержка и документация