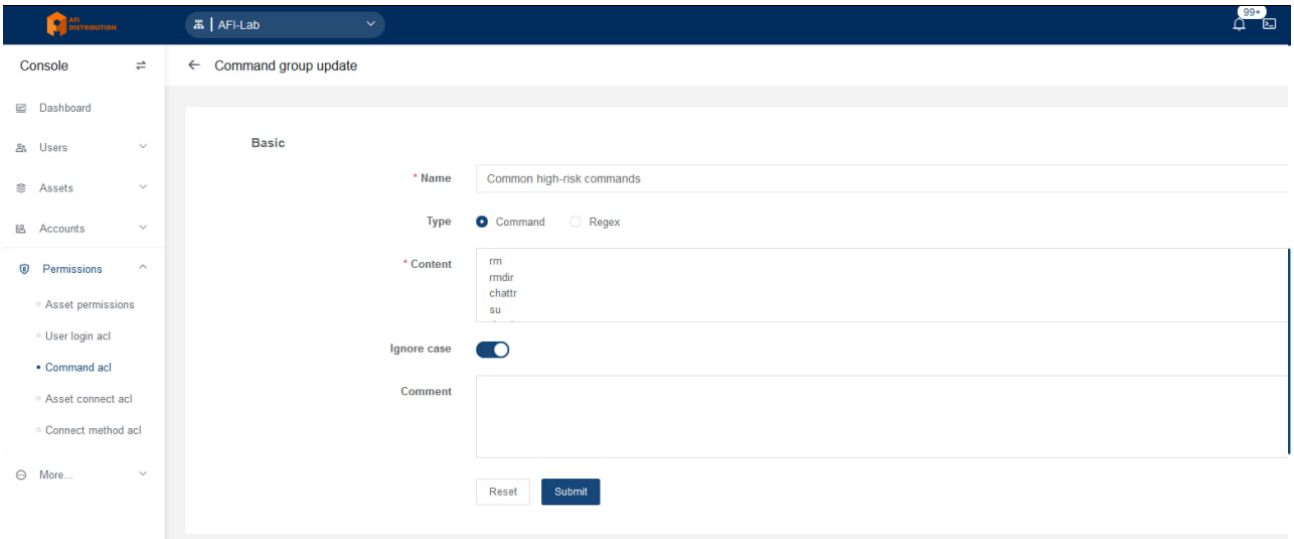
Администрирование системы

- Настройка блокировки команд SSH и запросов СУБД
- Настройка подключения к целевым системам по HTTP(веб-интерфейсы приложений)
- Как подключаться к доменным активам с единой доменной УЗ?
- Автоматическое повышение привилегий при подключении по SSH
- Создание УЗ и SSH ключей на целевой системе (Push Accounts)
- Обнаружение неконтролируемых учетных записей (Discover Accounts)
- Изменение пути по умолчанию для SFTP подключений

Настройка блокировки команд SSH и запросов СУБД

1. Перейдите в раздел **"Console - Permissions - Command Acl"**, откройте вкладку **"Command Group"**.

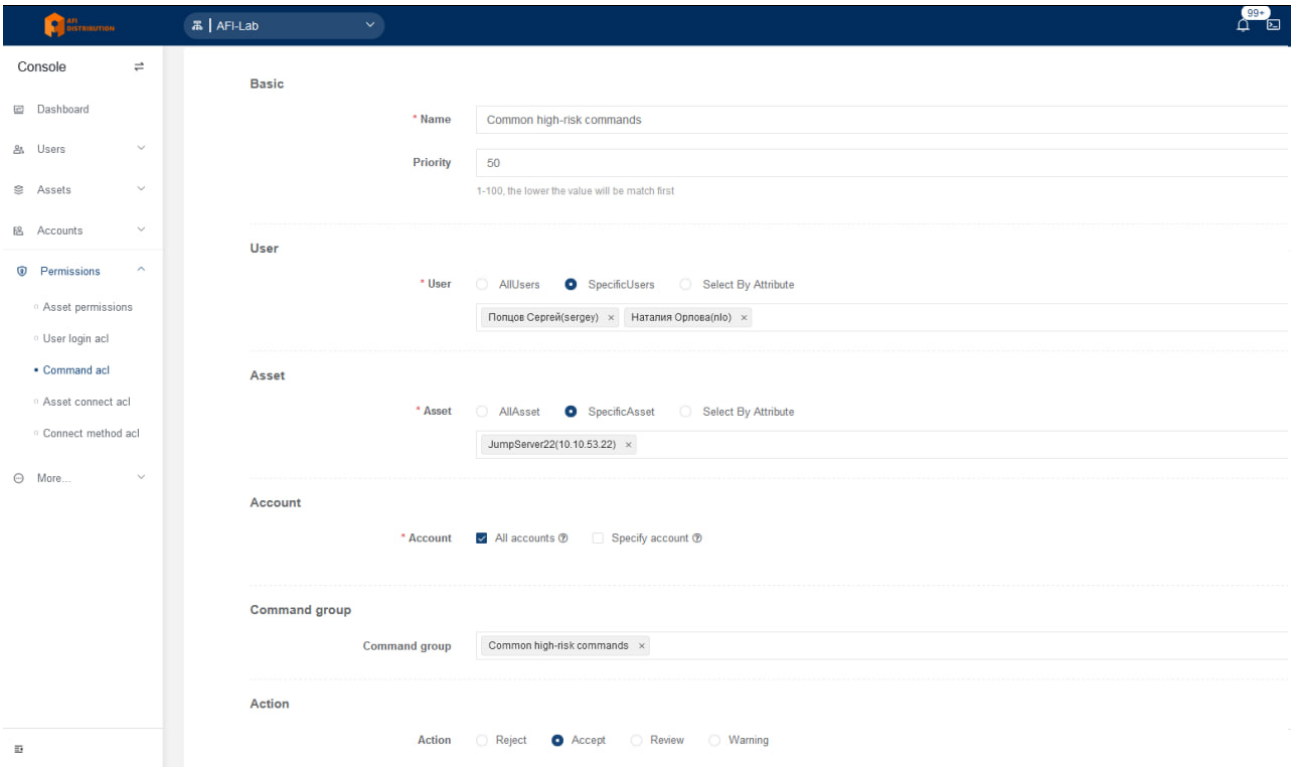
2. Нажмите кнопку **"Create"**, введите название списка, например **"Common high-risk commands"** и заполните список нужных команд или регулярных выражений (см. скриншот) и сохраните, нажав кнопку **"Submit"**.



3. Перейдите во вкладку **"Command filter"**, нажмите **"Create"** для создания фильтра.

4. Настройка фильтра включает следующие параметры:

- Priority: приоритет фильтра, всегда выполняется действие того фильтра, чей приоритет будет выше.
- User: пользователи JumpServer, для которых будет работать фильтр
- Asset: целевые системы, подключение к которым будет контролироваться фильтром
- Account: учетные записи на целевых системах, которые будут контролироваться фильтром
- Command Group: группы команд, которые будут блокироваться
- Action: действие фильтра: **Reject** - заблокировать команду, **Accept** - выполнить команду, **Review** - отправить команду на согласование указанному сотруднику, **Warning** - предупредить о выполнении команды указанного сотрудника.



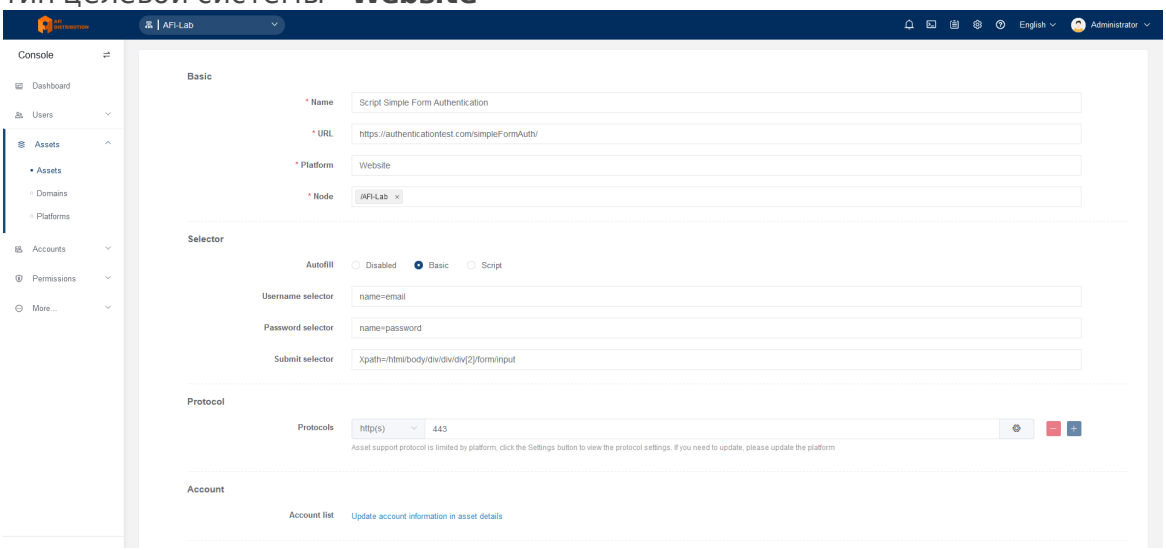
5. Нажмите **"Submit"** для сохранения настроек.

Настройка подключения к целевым системам по HTTP(веб-интерфейсы приложений)

Для подключения к целевым системам по HTTP вам необходимо:
Настроить публикацию браузера через Panda (сервер публикации приложений на базе Linux)
или
Настроить публикацию браузера через RDS(RemoteApp).

Создание устройства типа "Вебсайт"

1. Зайдите в раздел **"Console - Assets"** , нажмите кнопку **"Create"** и выберите тип целевой системы - **Website**



2. В разделе **"Selector"** нужно указать параметры полей формы, которые **JumpServer** заполнит автоматически при открытии сессии.
На пример:

При таких настройках, имя пользователя будет введено в HTML элемент с **name="email"**, пароль будет введет в HTML элемент с **name="password"** и затем будет нажата кнопка с **Xpath=/html/body/div/div/div[2]/form/input**

Вы можете посмотреть элементы веб-формы входа в браузере, нажав правую кнопку мышки на поле ввода и выбрав пункт "Исследовать" (для Firefox) или "Просмотреть код" (для Chrome).
Также можно использовать дополнительные настройки и параметры элементов формы входа, для этого переключитесь в режим **Script**:

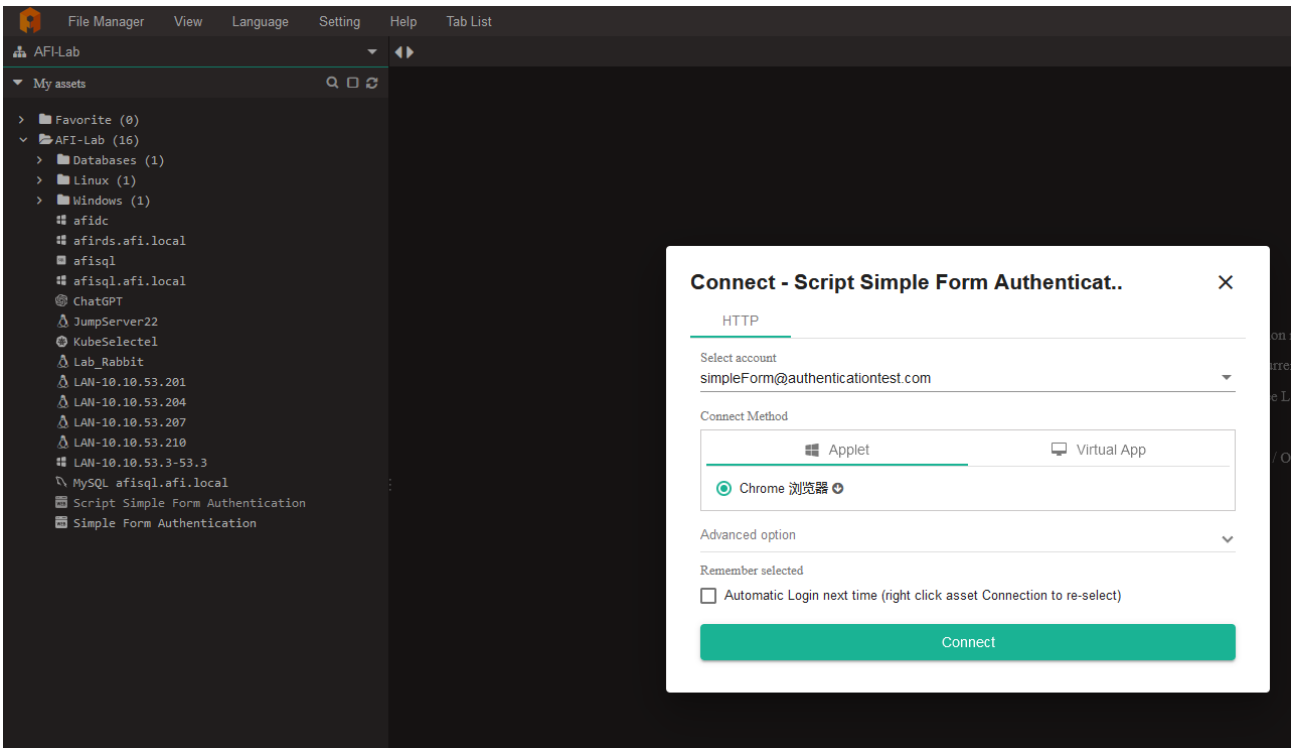
3. в разделе **Account list** нужно добавить учетную запись и пароль, которая будет использоваться при авторизации, аналогично как это делается при других типах подключения.
4. Сохранить настройки, нажав кнопку **"Submit".**

Пример скрипта авторизации в Google:

```
[
  {
   "step": 1,
   "value": "{USERNAME}",
   "target": "name=identifier",
   "command": "type"
  },
  {
   "step": 2,
   "value": "",
   "target": "Xpath=/html/body/div[1]/div[1]/div[2]/c-wiz/div/div[3]/div/div[1]/div/div/button/span",
   "command": "click"
  },
  {
   "step": 3,
   "value": "{SECRET}",
   "target": "name=Passwd",
   "command": "type"
  },
  {
   "step": 4,
   "value": "",
   "target": "Xpath=/html/body/div[1]/div[1]/div[2]/c-wiz/div/div[3]/div/div[1]/div/div/button/span",
   "command": "click"
  }
]
```

Подключение к веб-интерфейсам через веб-терминал

Если все настроено верно, при выборе нужного устройства в веб-терминале, вы увидите вариант запуска сессии:

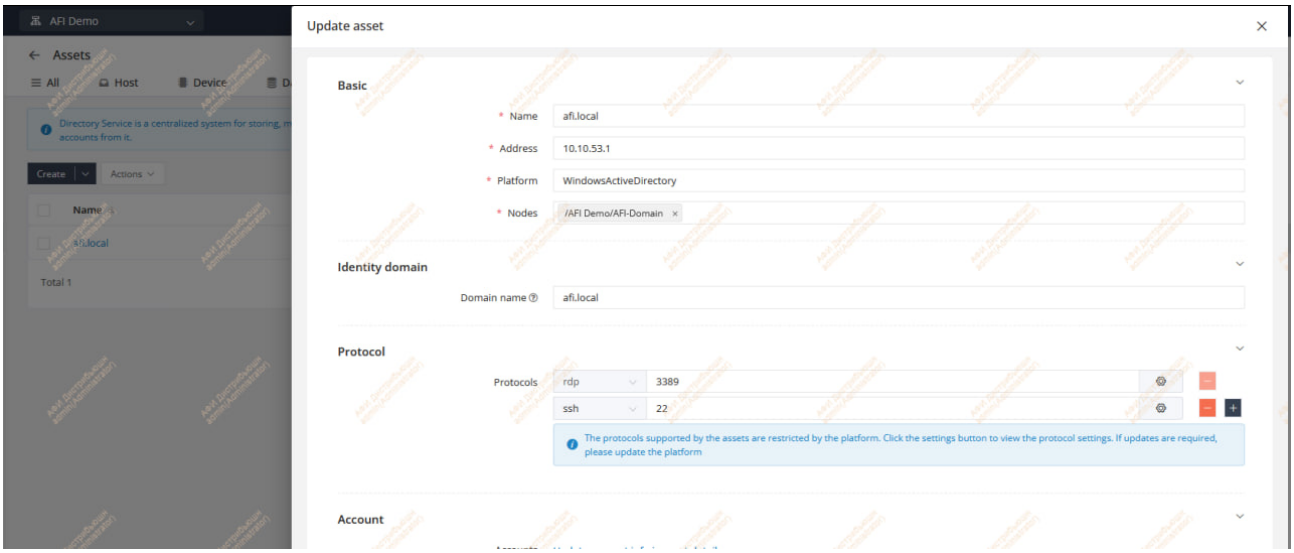


Как подключаться к доменным активам с единой доменной УЗ?

В предыдущих версиях JumpServer была строгая привязка УЗ к конкретному активу, то есть не было возможности подключаться с одной и той же доменной УЗ к разным активам без дублирования этой УЗ.

В последних версиях JumpServer добавили такую возможность:

1. Перейдите в **Console - Assets - Directory service** и создайте актив, указав параметры домена.
(см. скриншот №1)



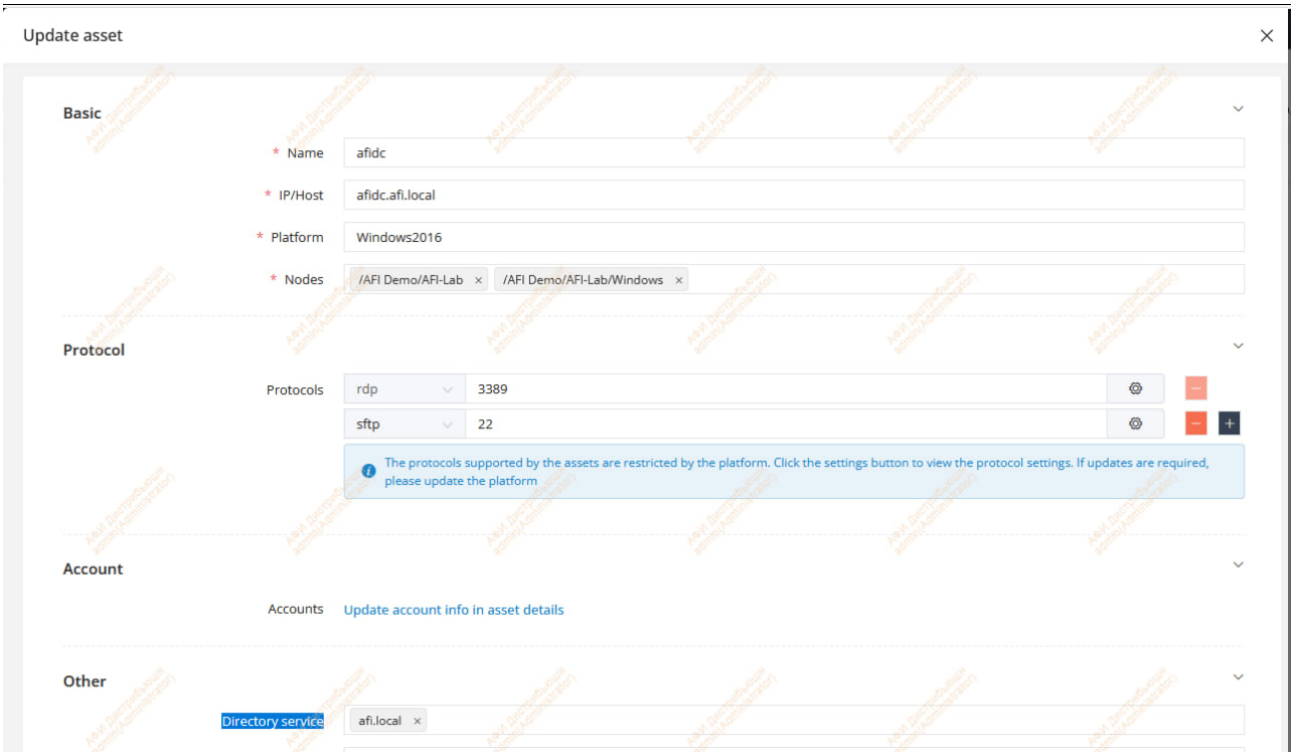
Примечание: если у вас нет вкладки **Directory Service**, обновите JumpServer до последней версии

2. Добавьте необходимые доменные УЗ к этому активу

3. В разделе **System Settings - Platforms** выберите платформу, которая будет использоваться для доменных активов, например Windows2016, и включите в ней опцию **DS Enabled**

Примечание: если платформа является основной, ее редактирование заблокировано, просто создайте ее дубликат.

4. В **Console - Assets** выберите нужный актив и откройте для редактирования. Внизу должен появиться параметр Directory service, укажите имя вашего DS актива, созданного на первом шаге (см. скриншот)



5. Теперь доменные УЗ будут отображаться у каждого доменного актива, и их можно будет использовать для подключения.

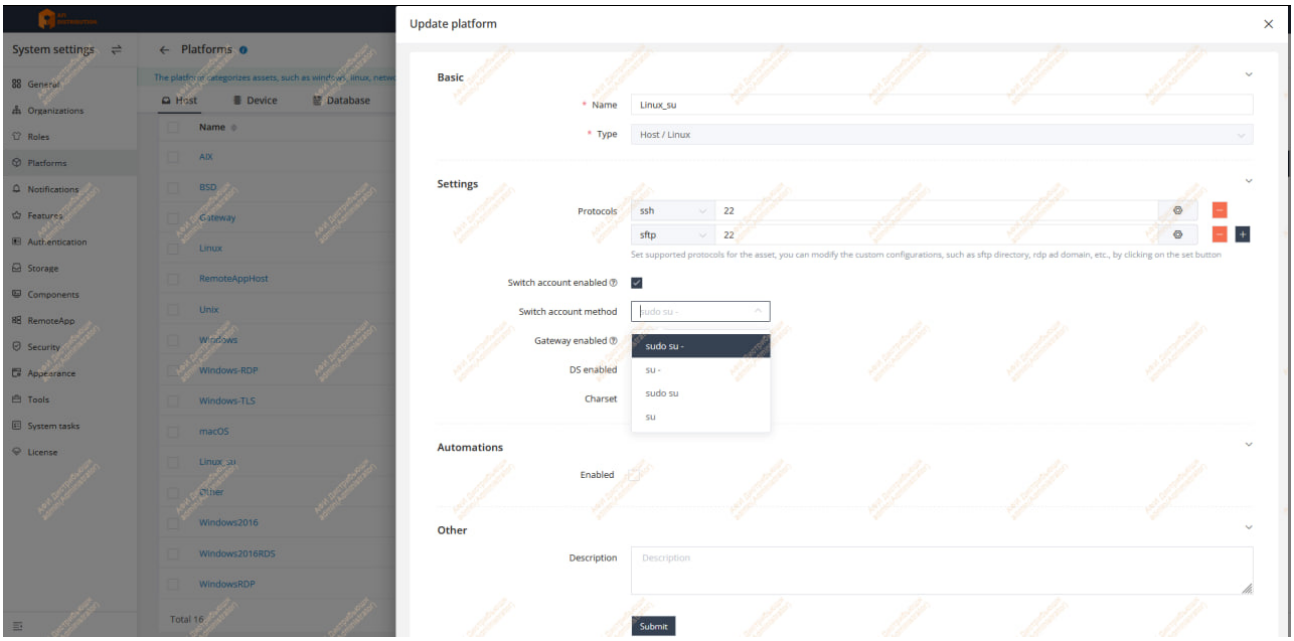
Автоматическое повышение привилегий при подключении по SSH

Обычно под УЗ root нельзя подключаться по SSH напрямую, поэтому после подключения для повышения привилегий обычно выполняется команда su и вводится пароль от УЗ root.

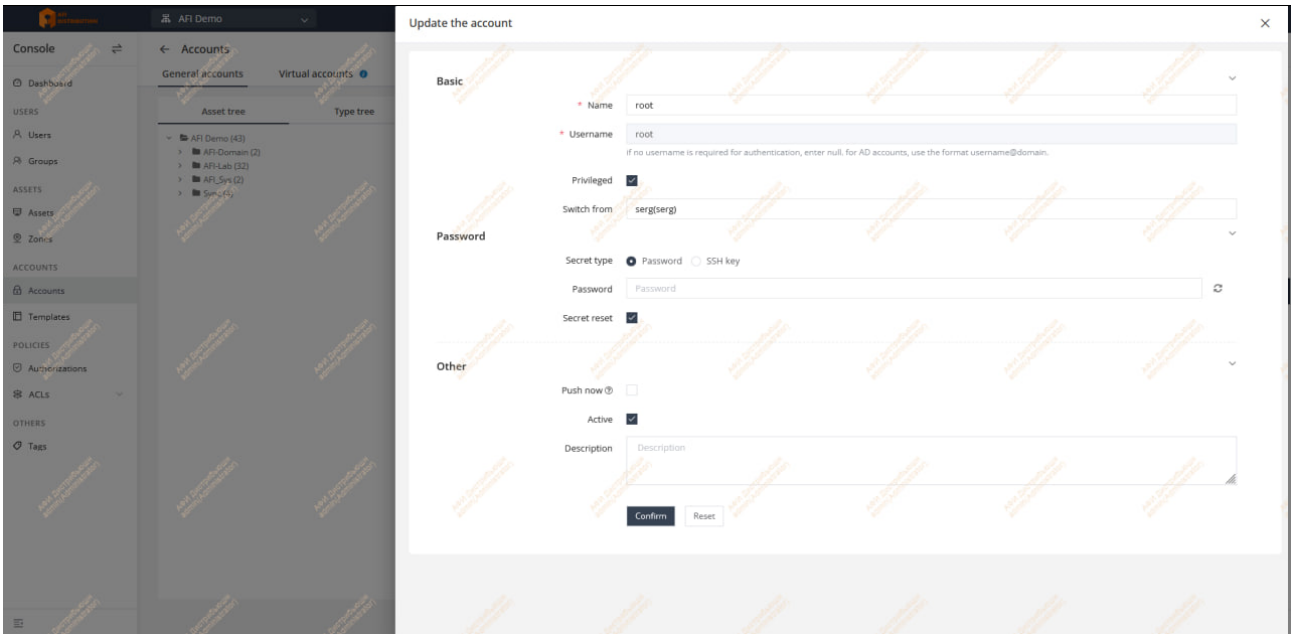
JumpServer позволяет автоматизировать этот процесс и запустить SSH сессию с автоматическим повышением прав до root без знания/раскрытия пароля.

Для этого нужно:

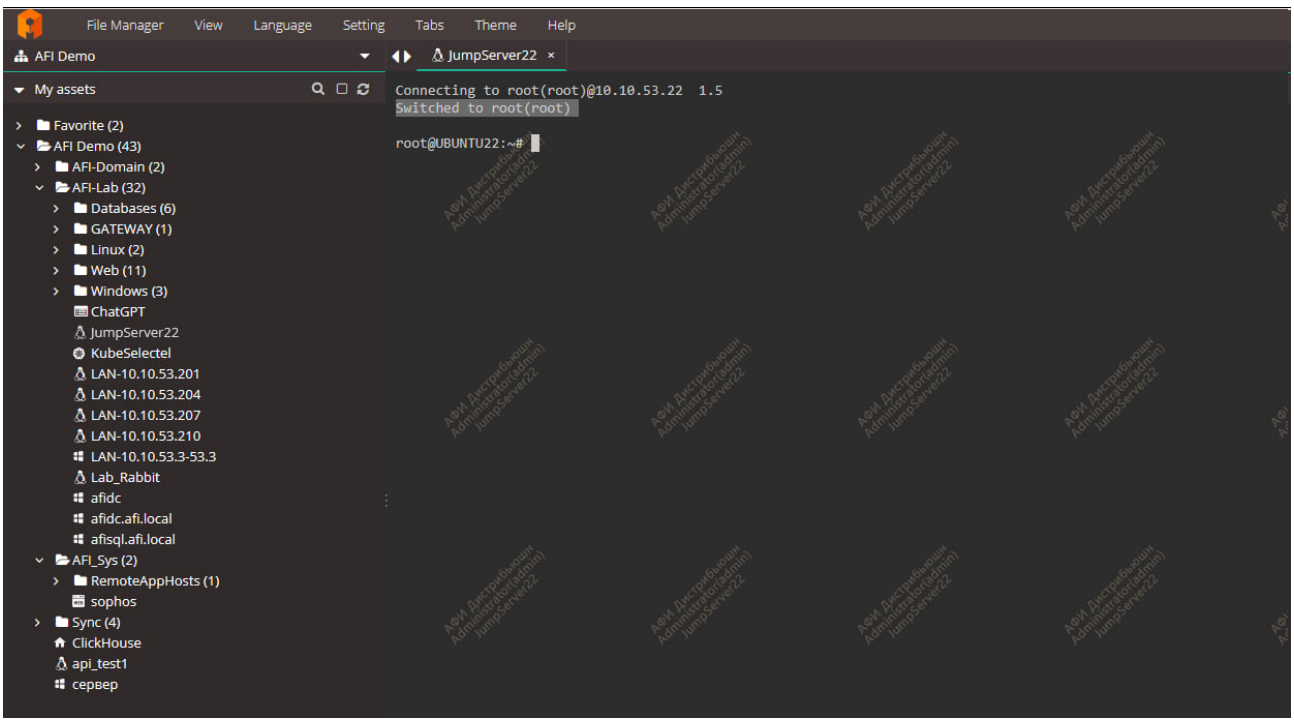
1. Зайти в **System Settings - Platforms**, в списке выбрать нужную платформу на базе Linux (или скопировать стандартную), открыть параметры и в поле **Switch Account Method** указать нужную команду, которая будет использоваться для переключения УЗ, например "**su -**"



2. Перейти в **Console - Accounts**, найти там привилегированную УЗ, например root, открыть для редактирования и в поле Switch from указать УЗ (в моем примере это УЗ serg), с которой будет осуществляться подключение изначально, сохранить изменения.



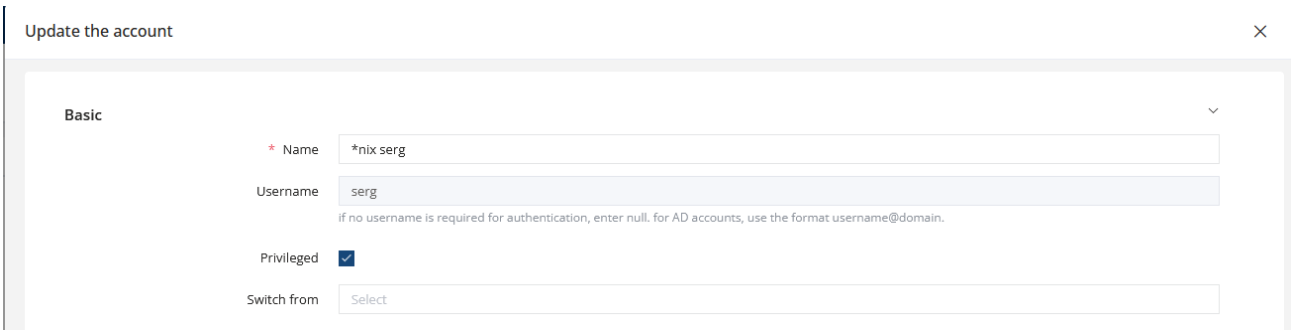
3. Теперь при подключении по SSH можно выбрать root, но сессия запуститься с УЗ serg и автоматически переключится на root после авторизации, при старте сессии вы увидите надпись "**switched to root(root)**"



Создание УЗ и SSH ключей на целевой системе (Push Accounts)

JumpServer может автоматически **создавать на целевых системах учетные записи и SSH ключи** с указанными параметрами.

Любые действия (создание УЗ или SSH ключей, обнаружение УЗ, смена пароля и ротация SSH ключа) на целевых системах JumpServer выполняет от имени привилегированной УЗ, которая добавлена к вашему активу, причем эта УЗ должна быть отмечена как **"Privileged"** в свойствах аккаунта:



Если у вашего актива нет ни одной УЗ, отмеченной как "Privileged", JumpServer даже не будет пытаться выполнить задачи по работе с вашими учетными записями.

Как работает Push Account

1. Если учетная запись не существует на целевой системе и не существует в списке УЗ JumpServer - она будет создана на целевой системе и добавлена.

2. Если учетная запись существует на целевой системе и существует в списке УЗ JumpServer - ничего не произойдет,даже если пароли не совпадают

3. Если учетная запись существует на целевой системе, но отсутствует в списке УЗ JumpServer - будет изменен пароль УЗ на целевой системе(согласно настройкам параметров пароля в задаче) и добавлена в список УЗ в JumpServer

4. Если учетная запись отсутствует на целевой системе, но присутствует в списке УЗ JumpServer - УЗ будет создана на целевой системе с тем же паролем, который задан в УЗ в JumpServer

Создание УЗ или SSH ключа

Перейдите в раздел **PAM - Push Accounts**, на вкладке **Account push task** нажмите кнопку **Create** и заполните необходимые параметры:

Assets: здесь можно выбрать несколько активов, на которых будет созданы учетные записи или SSH ключи

Nodes: выбор папки с активами, то есть JumpServer попробует создать УЗ на ВСЕХ активах в выбранной папке или папках

Accounts: имена УЗ, которые будут созданы на всех выбранных активах

Secret strategy:
Specified Secret: задать новый пароль вручную
Random generate: сгенерировать пароль автоматически

Password rules: здесь можно указать параметры генерации пароля

Push parameters: доступно только для активов типа хост, дополнительные параметры создания УЗ на линукс ОС.

Periodic: включить периодическое выполнение задачи создания УЗ.

Обнаружение неконтролируемых учетных записей (Discover Accounts)

JumpServer может автоматически **обнаруживать неконтролируемые учетные записи** на целевых системах - такие УЗ, которые не были внесены в список известных в интерфейсе JumpServer.

Обнаруженную учетную запись можно автоматически добавить в список контролируемых УЗ, автоматически сменив ей пароль, либо удалить с целевой системы.

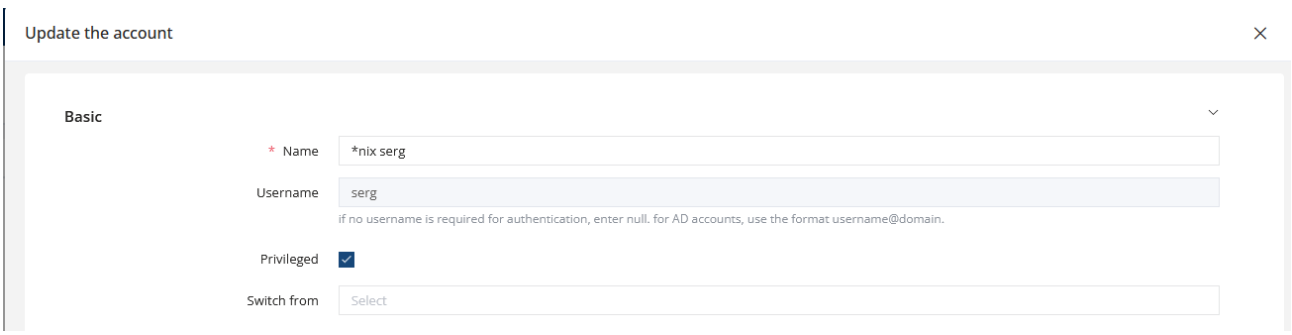
Зачем нужно обнаружение УЗ?

Неконтролируемые учетные записи являются большой проблемой и могут быть использованы злоумышленниками.

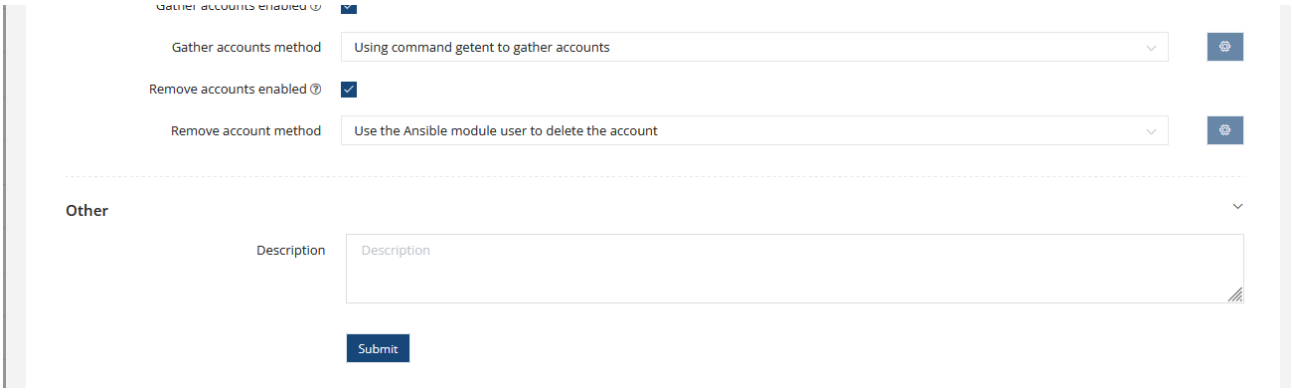
Неконтролируемая УЗ:
- может быть создана временно "для теста", имеет слабый или стандартный пароль;
- может быть создана бывшим сотрудником\подрядчиком, в т.ч без согласования;
- непонятно кем используется, если вообще используется.

Настройка обнаружения УЗ

Любые действия (создание УЗ или SSH ключей, обнаружение УЗ, смена пароля и ротация SSH ключа) на целевых системах JumpServer выполняет от имени привилегированной УЗ, которая добавлена к вашему активу, причем эта УЗ должна быть отмечена как **"Privileged"** в свойствах аккаунта:



Также в настройках платформы, нужно отметить опцию **Gather accounts enabled** (в ключена по умолчанию)



Для включения автоматического обнаружения:

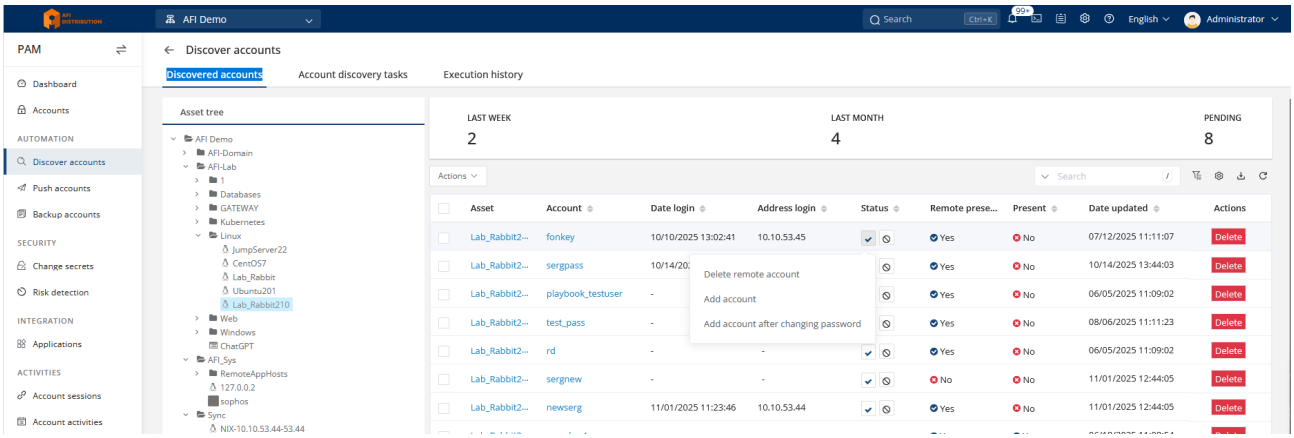
1. перейдите в раздел **PAM - Automation - Discover Accounts**
2. откройте вкладку **Account discovery tasks**
3. нажмите кнопку **Create**
4. заполните необходимые параметры:
   - **Assets:** здесь можно выбрать несколько активов, где будет выполнятся обнаружение УЗ
   - **Nodes:** выбор папки с активами, то есть JumpServer попробует обнаружить УЗ на ВСЕХ активах в выбранной папке или папках
   - **Sync to assets:**
     - **ВКЛЮЧЕНО:** JumpServer добавит обнаруженную УЗ в список учетный записей и **выполнит смену пароля этой УЗ**
     - **ВЫКЛЮЧЕНО:** вы увидите новые УЗ в списке и сможете вручную принять решение удалить УЗ с целевой системы или добавить со сменой пароля в список учетных записей
   - **Check risk:** обнаруженные УЗ появятся в разделе **PAM - Risk Detection** с отметкой **New foun**
   - **Periodic:** включить периодическое выполнение задачи обнаружения УЗ.
5. Нажмите **Submit** для сохранения задачи обнаружения УЗ

Обнаружение учетных записей

Для запуска обнаружения вручную**:**

1. перейдите в раздел **PAM - Automation - Discover Accounts**
2. откройте вкладку **Account discovery tasks**
3. нажмите кнопку **Execute** у выбранной задачи обнаружения
4. дождитесь завершения процесса

Обнаруженные УЗ вы увидите в разделе **PAM - Automation - Discover accounts** на вкладе **Discovered accounts:**



У обнаруженных УЗ в столбце **Status** доступны действия:

- **delete remote account:** учетная запись будет **УДАЛЕНА С ЦЕЛЕВОЙ СИСТЕМЫ**;
- **add account:** добавить УЗ в список учетных записей без смены пароля;
- **add account after password changing:** добавить УЗ в список учетных записей, сменив её пароль;
- **ignore:** игнорировать обнаруженную УЗ.

Изменение пути по умолчанию для SFTP подключений

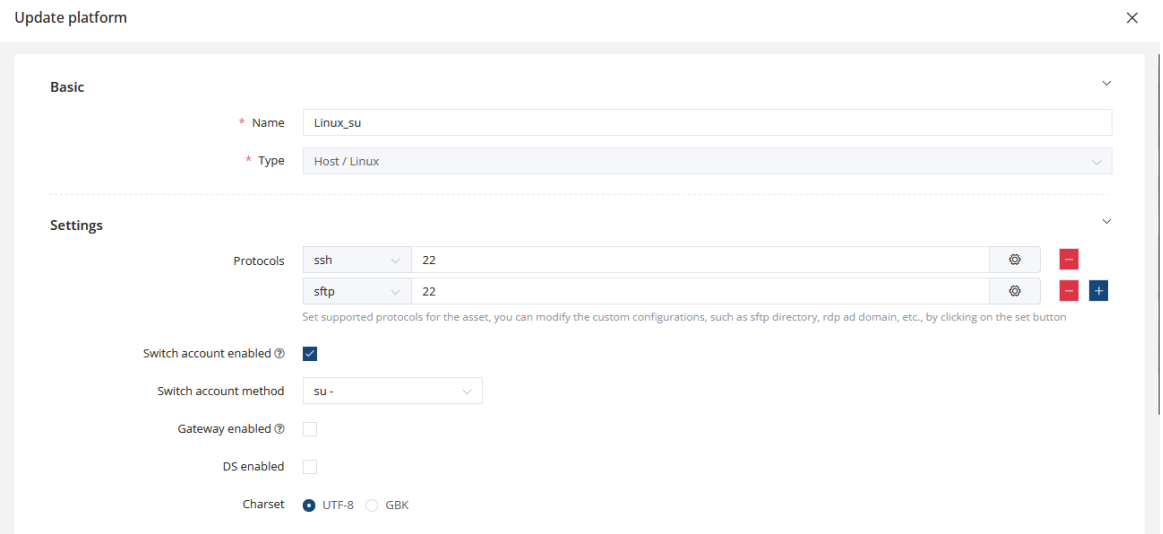
По умолчанию в настройках протокола SFTP указан путь /tmp/, то есть при подключении вы увидите только файлы в этой папке без возможности подняться на уровень выше, для перехода в другую папку.
Это сделано из соображений безопасности, чтобы файлы передавались строго в папку /tmp/ а затем в рамках SSH сессии уже переносились в нужные директории с нужными правами.

Но все же иногда требуется изменить папку по умолчанию для SFTP подключений.

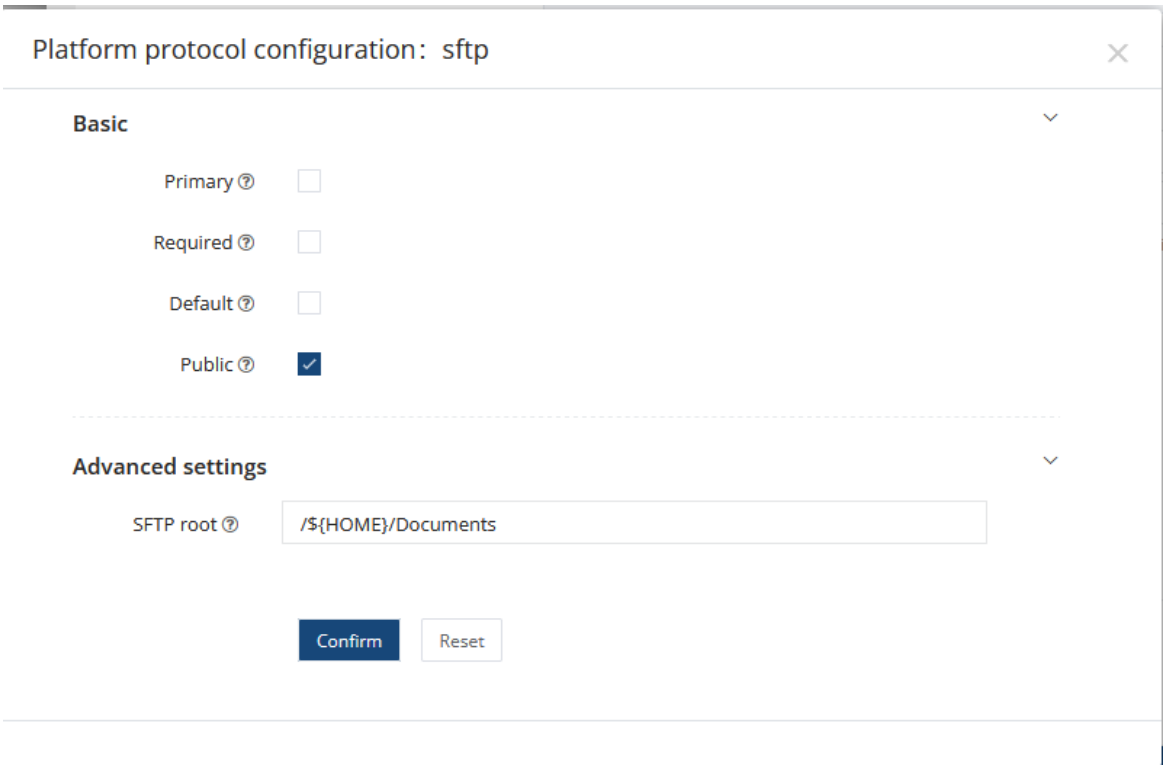
Изменение параметров SFTP подключения

Параметры протокола можно поменять в настройках платформы (System settings - Platforms), но для основных платформ настройки заблокированы, поэтому

1. Заходим в **System settings - Platforms**, находим нужную платформу (**Linux**) , нажимаем справа три точки, выбираем **Duplicate** и сохраняем копию платформы с новым именем.
2. Находим в списке нашу новую платформу, нажимаем **Edit** и открываются настройки платформы



3. В списке протоколов для протокола SFTP нажимаем значок шестеренки и вы увидите директорию, которая открывается по умолчанию в SFTP сессии



Вы можете в параметре **SFTP root** указать или конкретную папку или корневую директорию / или использовать стандартные переменные, такие как:
- **${ACCOUNT}** - имя учетной записи
- **${HOME}** - домашняя директория авторизованной учетной записи
- **${USER}** - имя пользователя

4. Сохраните изменения. Вы можете создать различные платформы с различными путями для SFTP и использовать их для разных активов.