

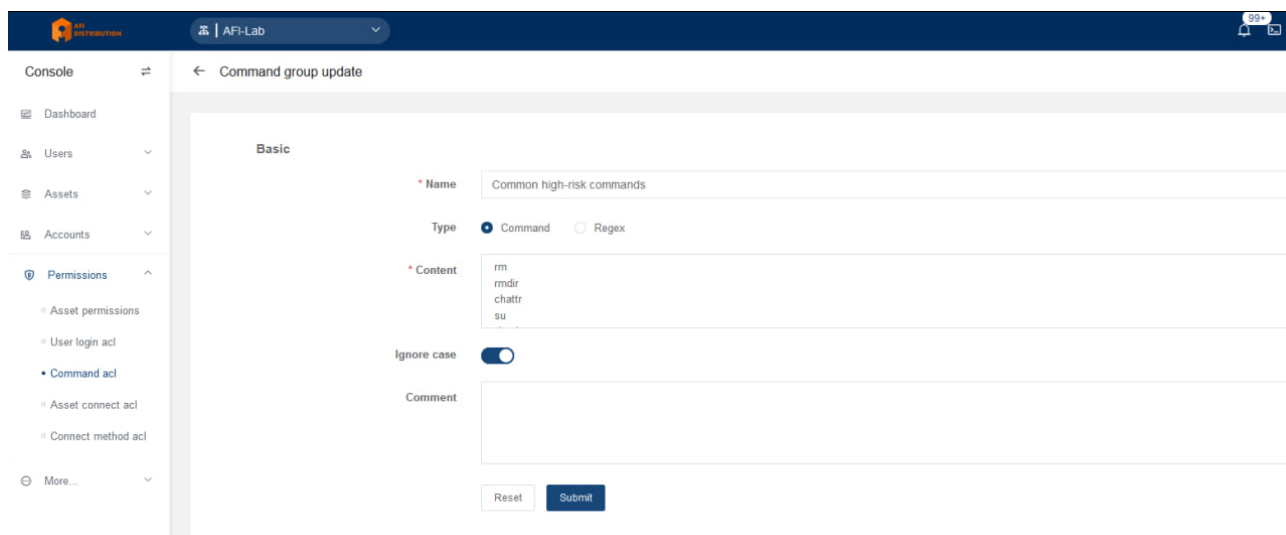
# Администрирование системы

- 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

# 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.

AFI-Platform

AFI-Lab

99%

Console

Dashboard

Users

Assets

Accounts

Permissions

Asset permissions

User login acl

Command acl

Asset connect acl

Connect method acl

More...

Basic

Name

Common high-risk commands

Priority

50

1-100, the lower the value will be match first

User

User

AllUsers

SpecificUsers

Select By Attribute

Полков Сергей(sergey)

Наталья Орлова(nlo)

Asset

Asset

AllAsset

SpecificAsset

Select By Attribute

JumpServer22(10.10.53.22)

Account

Account

All accounts

Specify account

Command group

Command group

Common high-risk commands

Action

Action

Reject

Accept

Review

Warning

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**

The screenshot shows the AFI Lab console interface. On the left is a sidebar with a menu: Console, Dashboard, Users, Assets (selected), Domains, Platforms, Accounts, Permissions, and More. The main area is titled 'Basic' and contains the following fields:

- Name:** Script Simple Form Authentication
- URL:** https://authenticationtest.com/simpleFormAuth/
- Platform:** Website
- Node:** AFI-Lab

Below the 'Basic' section is the **Selector** section with the following options:

- Autofill:** Disabled, Basic (selected), Script
- Username selector:** name=email
- Password selector:** name=password
- Submit selector:** Xpath=/html/body/div/div/div[2]/form/input

Below the 'Selector' section is the **Protocol** section with the following options:

- Protocols:** http(s) (selected), 443

At the bottom is the **Account** section with a link: [Account list](#) and a link: [Update account information in asset details](#).

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

Autofill ☐ Disabled ☒ Basic ☐ Script

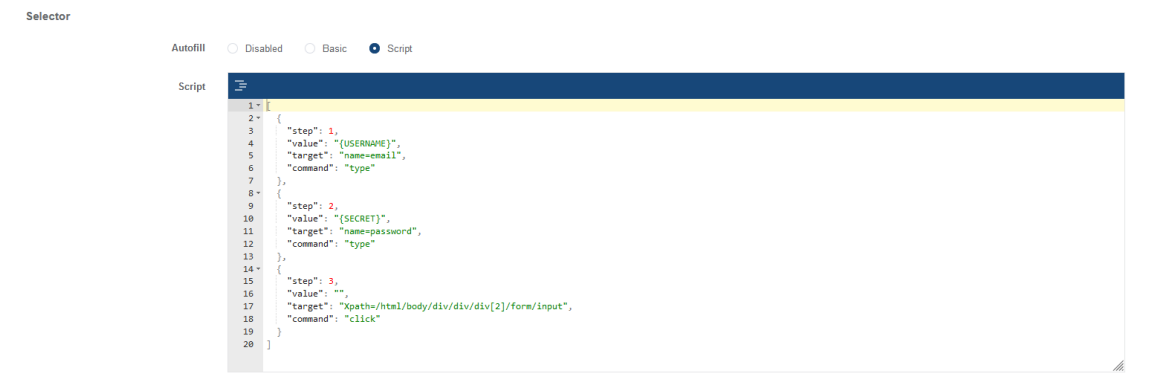
Username selector

Password selector

Submit selector

При таких настройках, имя пользователя будет введено в HTML элемент с **name="email"**, пароль будет введен 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**:

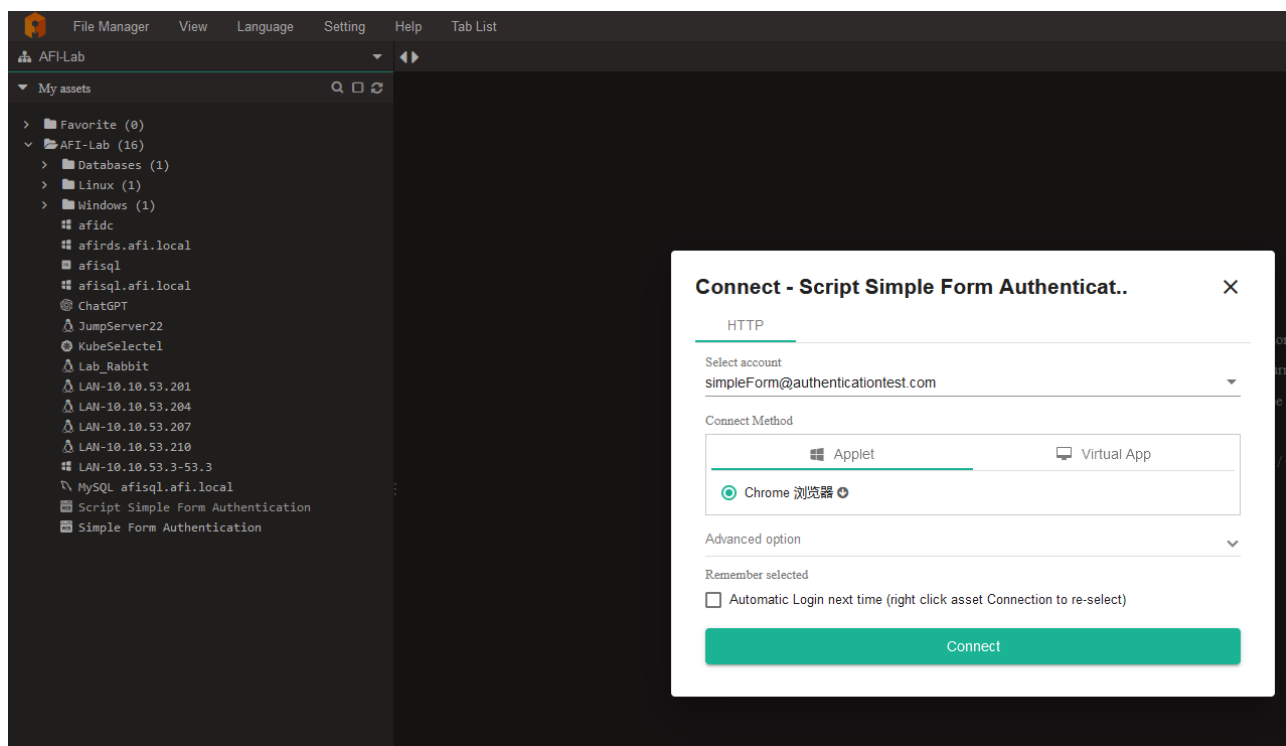


3. в разделе **Account list** нужно добавить учетную запись и пароль, которая будет использоваться при авторизации, аналогично как это делается при других типах подключения.

4. Сохранить настройки, нажав кнопку **"Submit"**.

## Подключение к веб-интерфейсам через веб-терминал

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

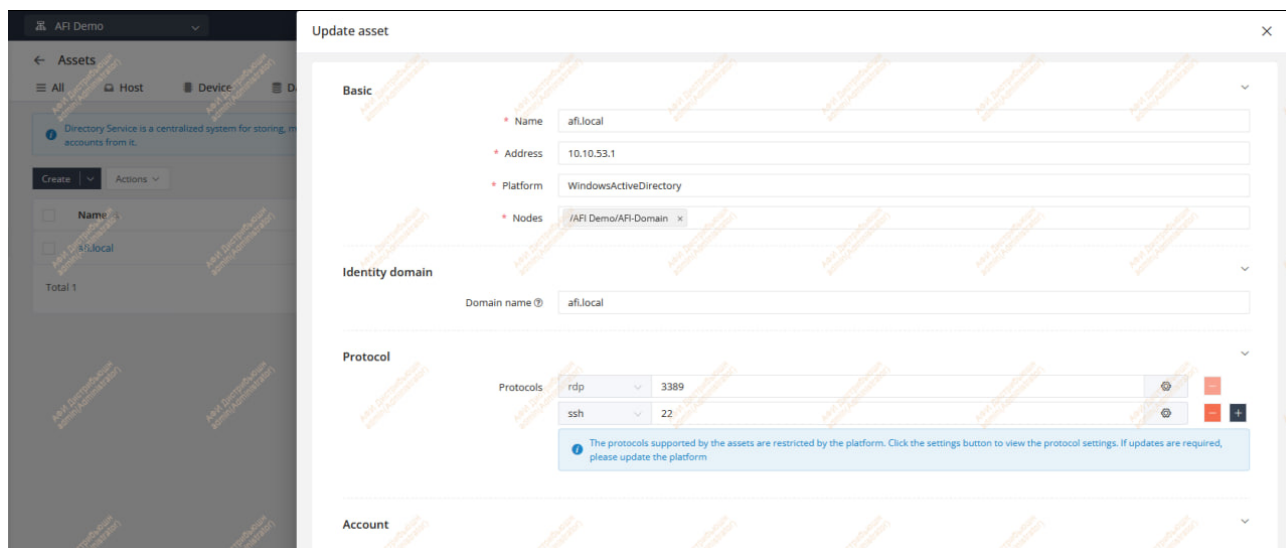


# Как подключаться к доменным активам с единой доменной УЗ?

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)

Update asset

**Basic**

\* Name: afidc

\* IP/Host: afidc.afil.local

\* Platform: Windows2016

\* Nodes: /AFI Demo/AFI-Lab x /AFI Demo/AFI-Lab/Windows x

**Protocol**

Protocols: rdp 3389 sftp 22

The protocols supported by the assets are restricted by the platform. Click the settings button to view the protocol settings. If updates are required, please update the platform

**Account**

Accounts: [Update account info in asset details](#)

**Other**

Directory service: afil.local x

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

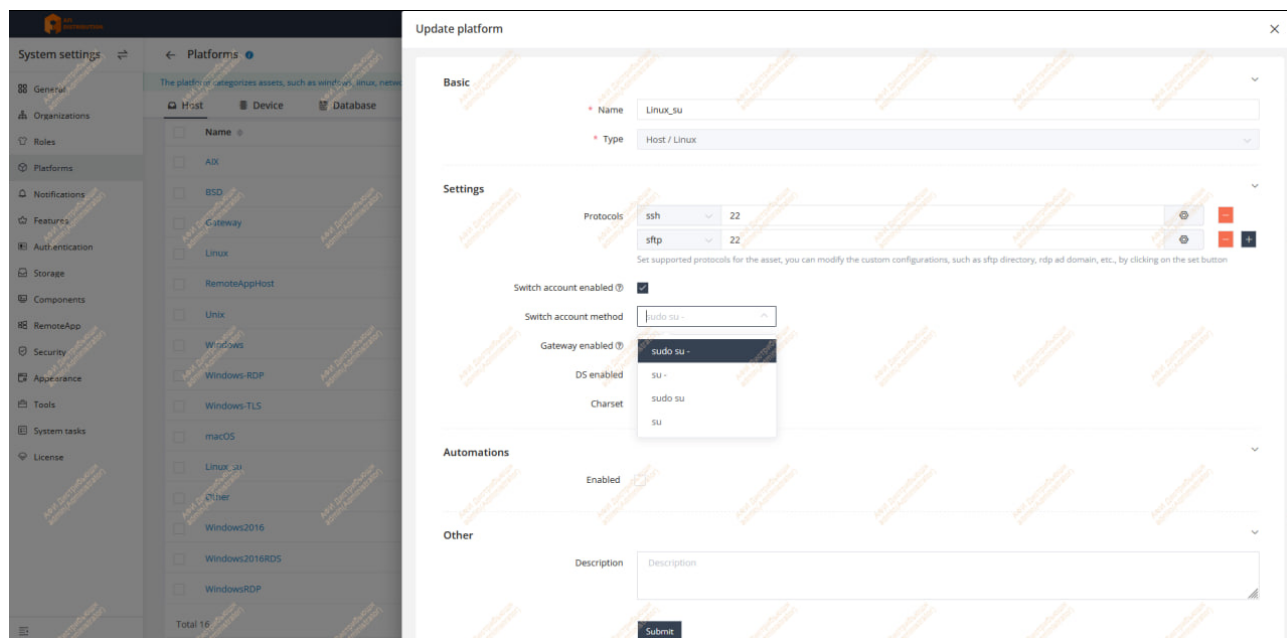
# Автоматическое повышение привилегий при подключении по SSH

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.

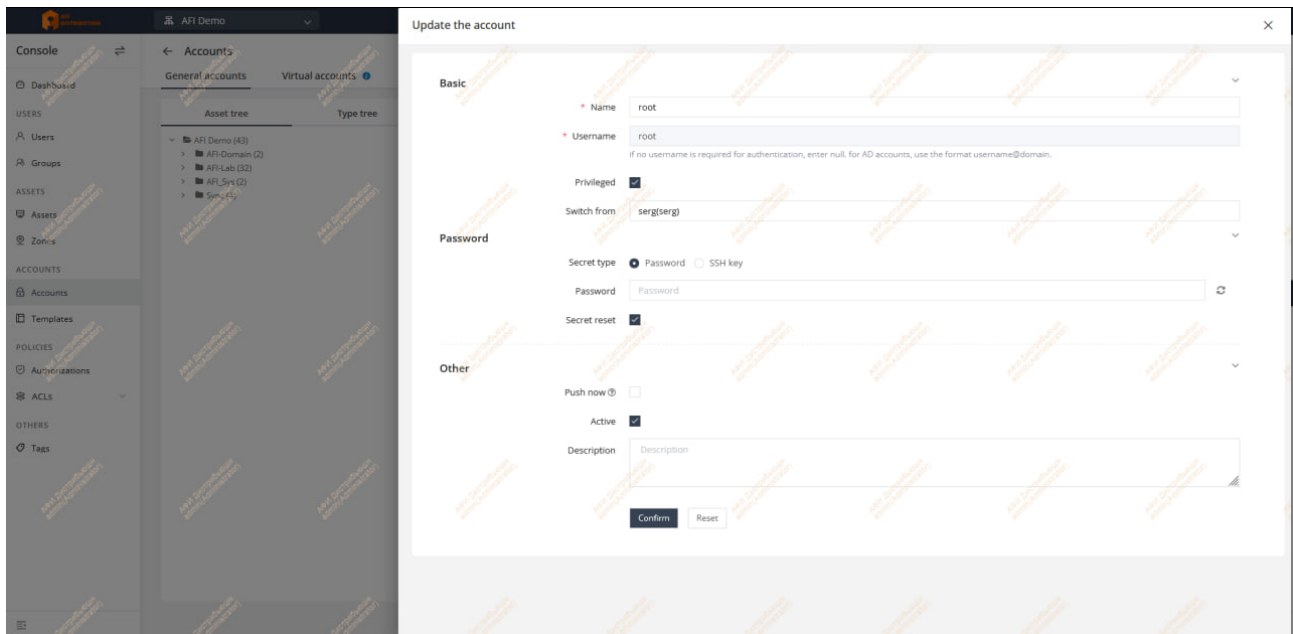
Для этого нужно:

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 запустится с УЗ serg и автоматически переключится на root после авторизации, при старте сессии вы увидите надпись **"switched to root(root)"**

