

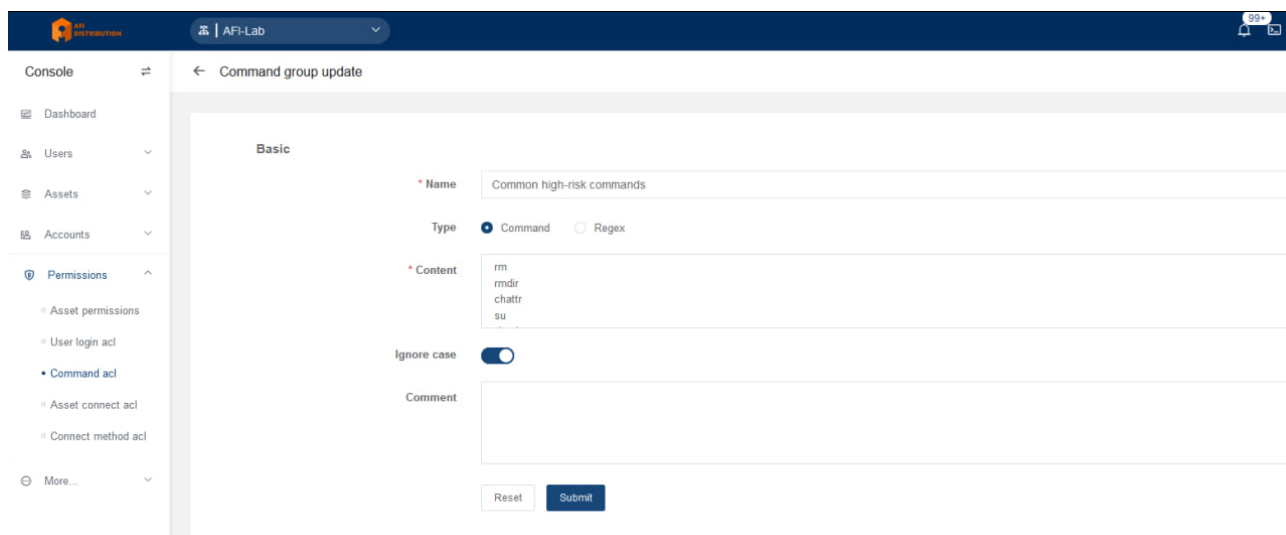
Администрирование системы

- Настройка блокировки команд SSH и запросов СУБД
- Настройка подключения к целевым системам по HTTP(веб-интерфейсы приложений)

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**".



The screenshot shows the 'Command group update' form in the AFI-Lab interface. The form is titled 'Basic' and contains the following fields:

- Name:** Common high-risk commands
- Type:** Command (selected), Regex
- Content:** rm, rmdir, chattr, su
- Ignore case:** ☒
- Comment:** (empty)

At the bottom of the form are two buttons: 'Reset' and '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 three radio buttons for 'Autofill': Disabled, Basic (selected), and Script. It includes three input fields:

- 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 a dropdown for 'Protocols' set to 'http(s)' and a port field set to '443'. A small note below states: 'Asset support protocol is limited by platform, click the Settings button to view the protocol settings. If you need to update, please update the platform.'

At the bottom is the **Account** section with a link for 'Account list' and a button for '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

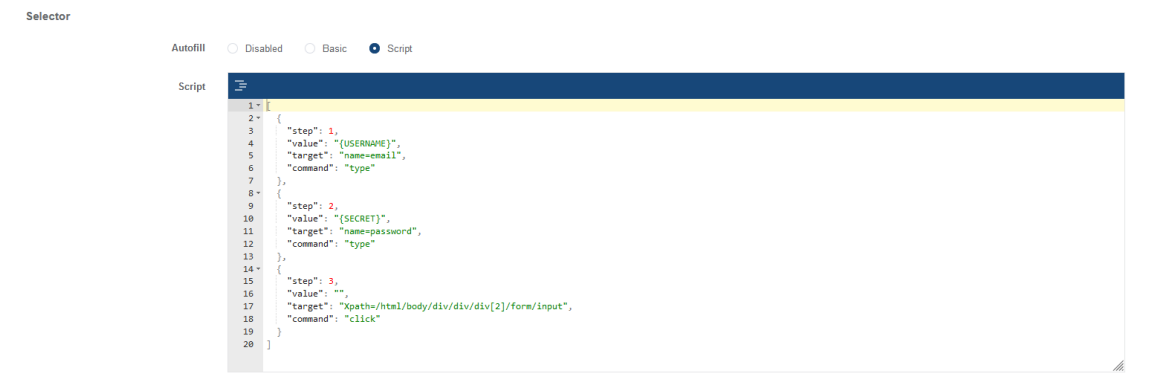
Username selector

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:

