Основные настройки

- Интеграция с Active Directory(LDAP) и синхронизация с группами AD
- Настройка блокировки команд SSH и запросов СУБД
- Включение встроенной 2-факторной авторизации(TOTP)
- Установка OpenSSH на Windows для управления УЗ Windows
- Настройка отправки событий по Syslog
- Настройка RDS (RemoteApp) для публикации приложений
- Настройка подключения к устройству по HTTP(веб-интерфейс)
- Настройка Panda для публикации приложений

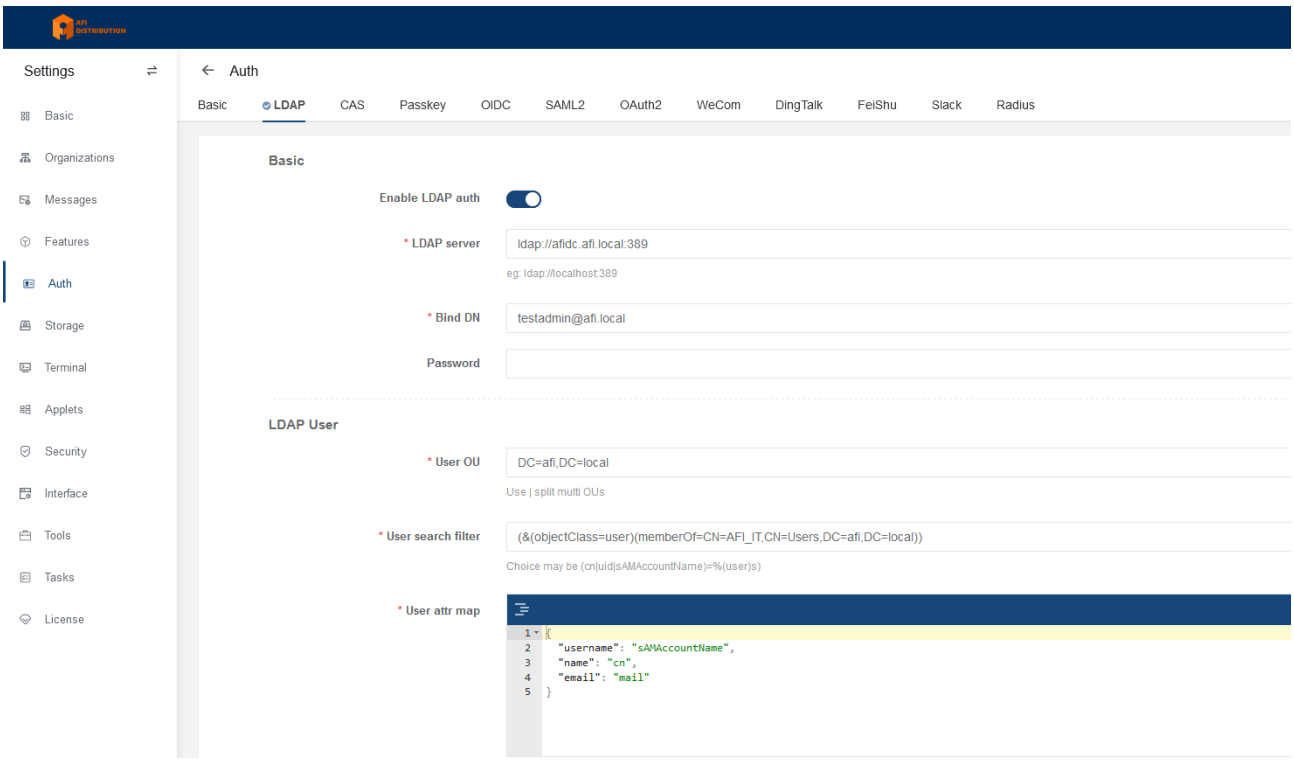
Интеграция с Active Directory(LDAP) и синхронизация с группами AD

Настройка интеграции с Active Directory

1. Зайдите в раздел **"System settings"** - **"Auth"**, выбираем вкладку **LDAP**.

2. Введите адрес LDAP сервера, учётную запись для подключения к нему и пароль от этой учётной записи.

3. Укажите OU и фильтр поиска пользователей. Пример фильтра пользователей конкретной группы смотрите на скриншоте.

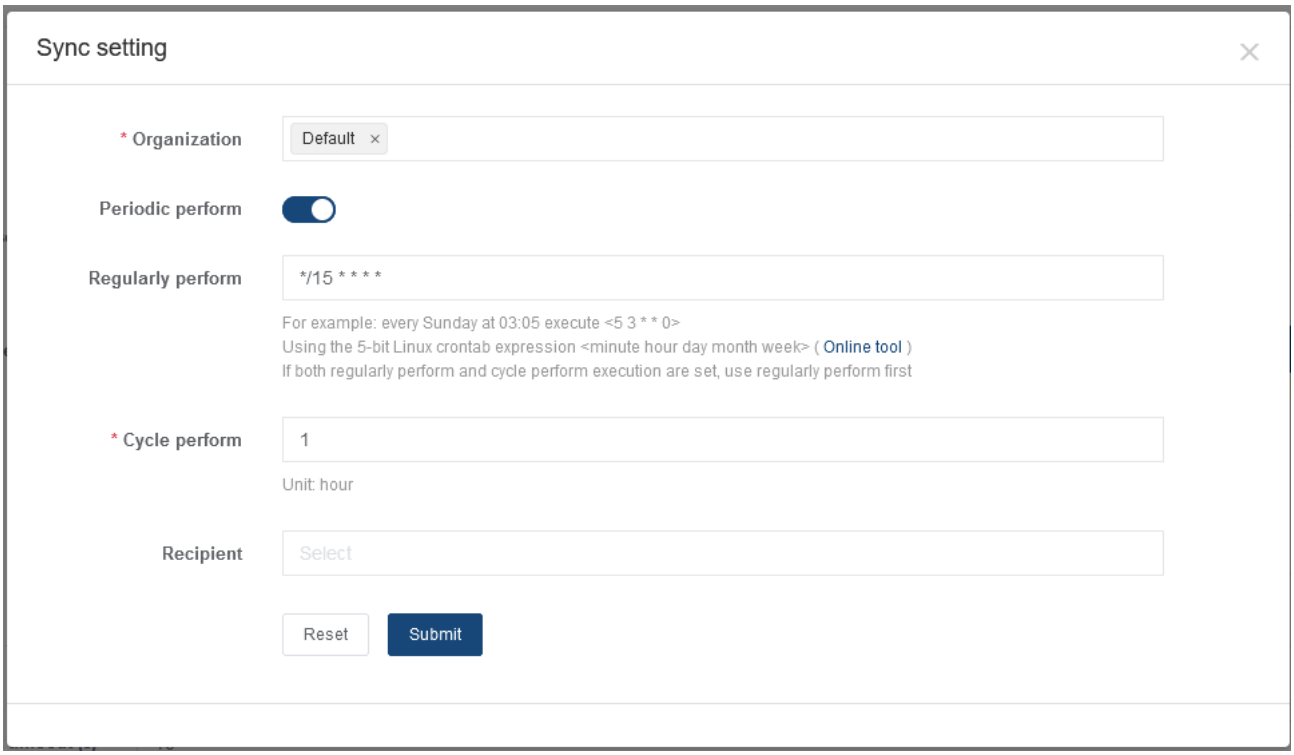


4. Нажмите кнопку **"Submit"** для сохранения настроек. Внимание: после изменения параметров и настроек нужно всегда нажимать кнопку **"Submit"** для применения настроек, иначе тест будет запускаться со старыми параметрами.

5. Нажмите кнопку **"Test connection"** для проверки настроек или **"Test login"** для проверки авторизации конкретного пользователя.

6. Нажмите кнопку **"Bulk Import"**. Вы должны увидеть пользователей группы, которые будут добавлены для авторизации в PAM. Там же можно выделить нужных пользователей и нажать **"Import"** или импортировать всех, нажав **"Import all"**.

7. Также вы можете настроить автоматическую синхронизацию пользователей, нажав кнопку **"Sync setting"**.



Синхронизация с группами Active Directory

Для чего используется синхронизация с AD группами?

Управлять правами доступа к целевым системам можно привычными группами Active Directory - добавление или удаление пользователя из таких групп будет автоматически синхронизироваться с матрицей прав в JumpServer, и пользователь будет получать или терять права доступа.

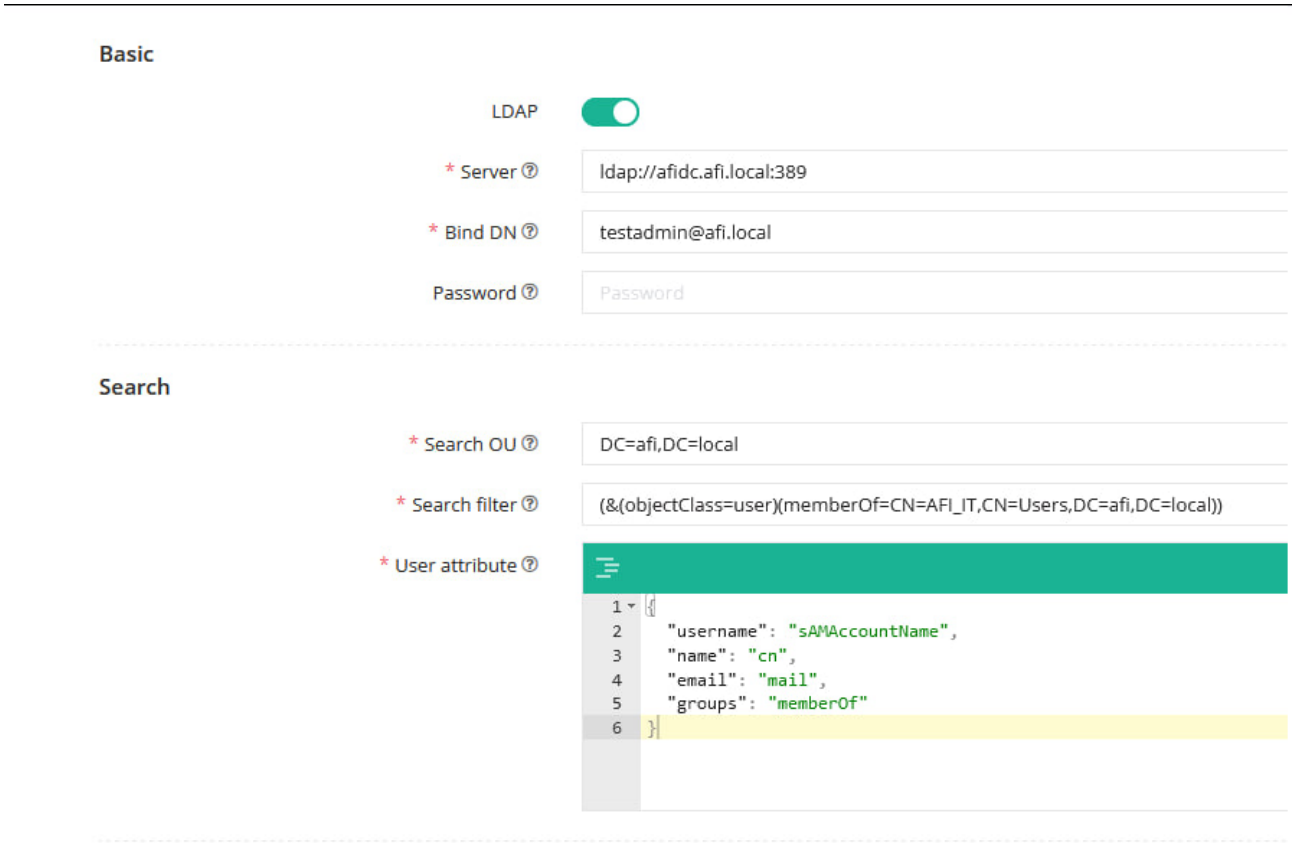
Настройка синхронизации с группами AD.

1. Зайдите в **System settings - Authentication - LDAP**

2. В поле **User attribute** добавьте параметр **groups**, так чтобы получилось:

```
{
  "username": "sAMAccountName",
  "name": "cn",
  "email": "mail",
  "groups": "memberOf"
}
```

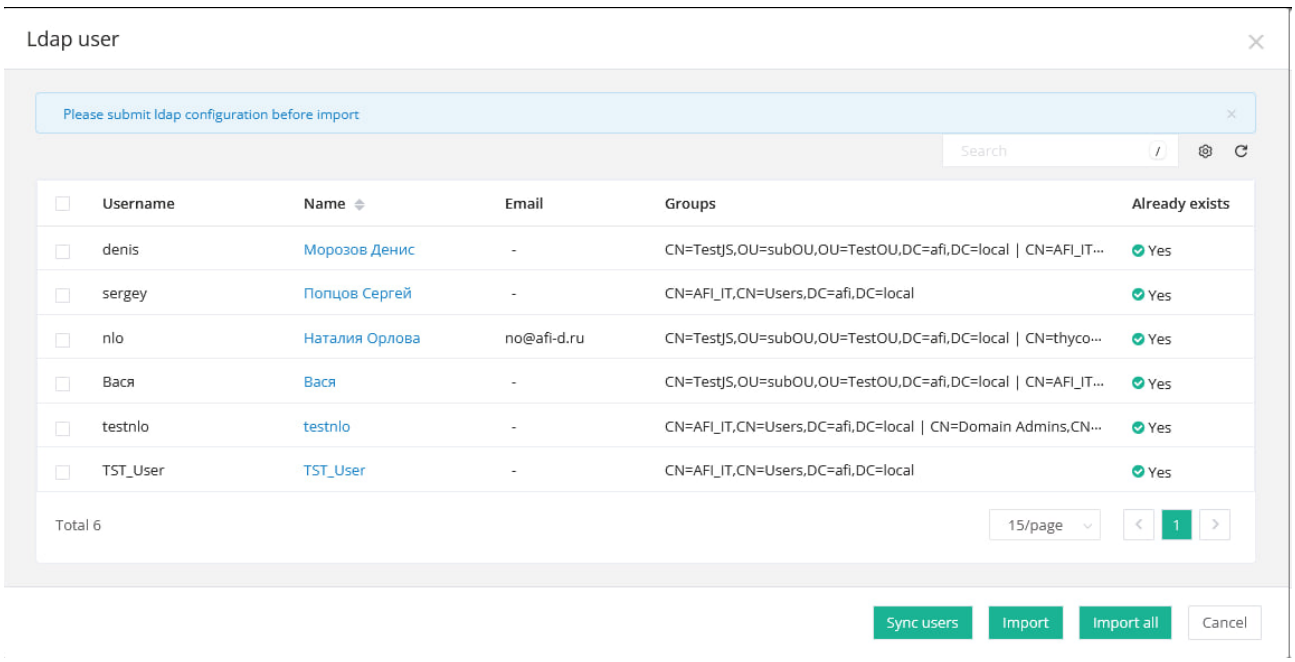
См скриншот:



3. Нажмите кнопку **Submit** для сохранения настроек

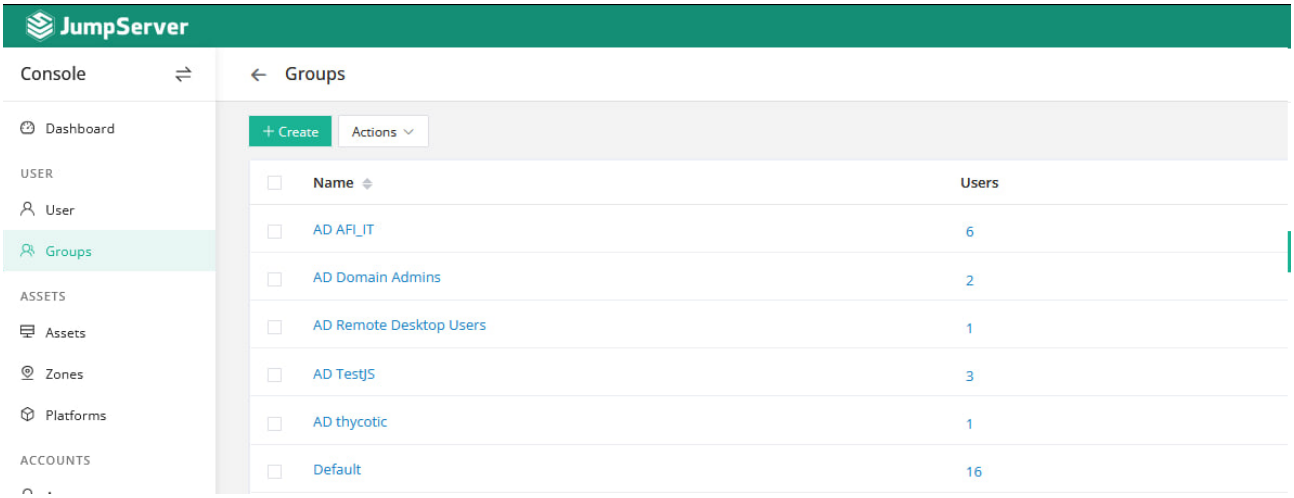
4. Нажмите кнопку **User Import** и в открывшемся окне нажмите **Sync Users**

Если все верно, вы увидите список пользователей и столбец с атрибутами групп **AD:**



5. Нажмите **Import all**, чтобы добавить пользователей в систему.

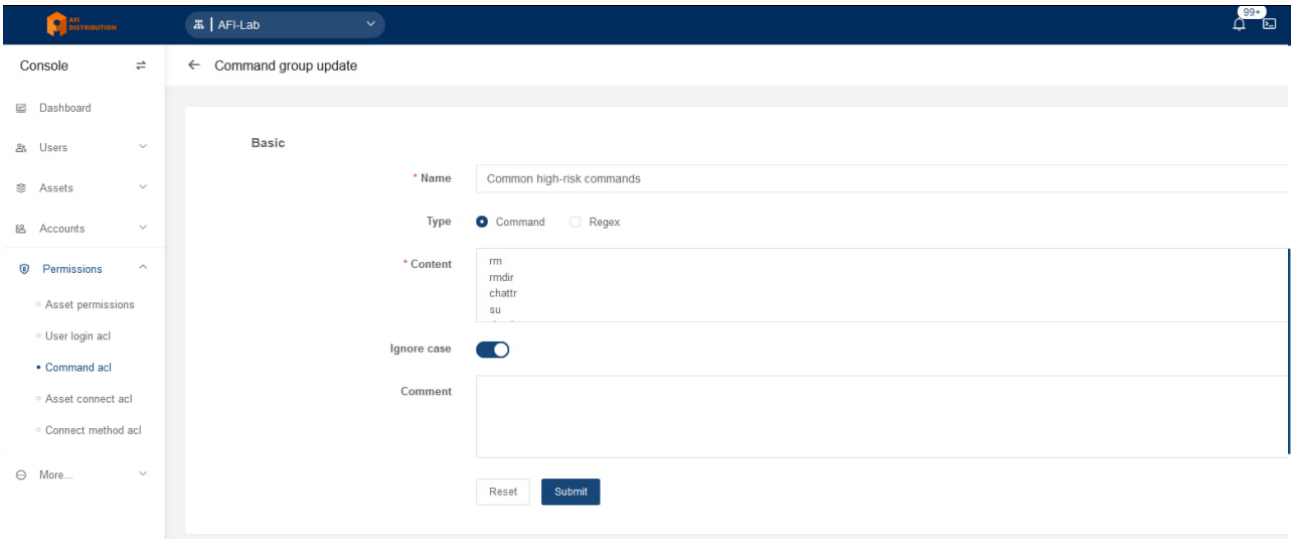
Если зайдете в **Console - User - Groups**, увидите группы пользователей JS, с именами групп AD с теми же пользователями в них:



Настройка блокировки команд SSH и запросов СУБД

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

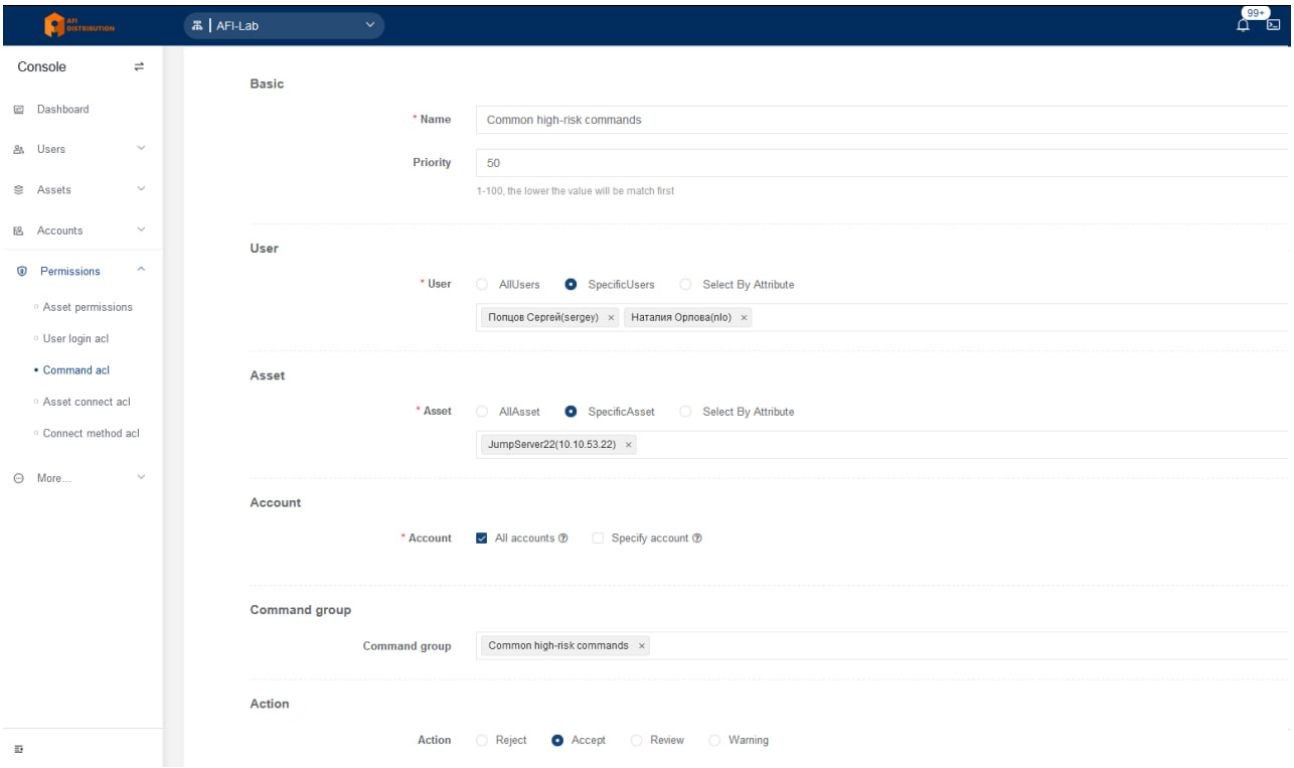
2. Нажмите кнопку **"Create"**, введите название списка, например **"Common high-risk commands"** и заполните список нужных команд или регулярных выражений (см. скриншот) и сохраните, нажав кнопку **"Submit"**.



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.



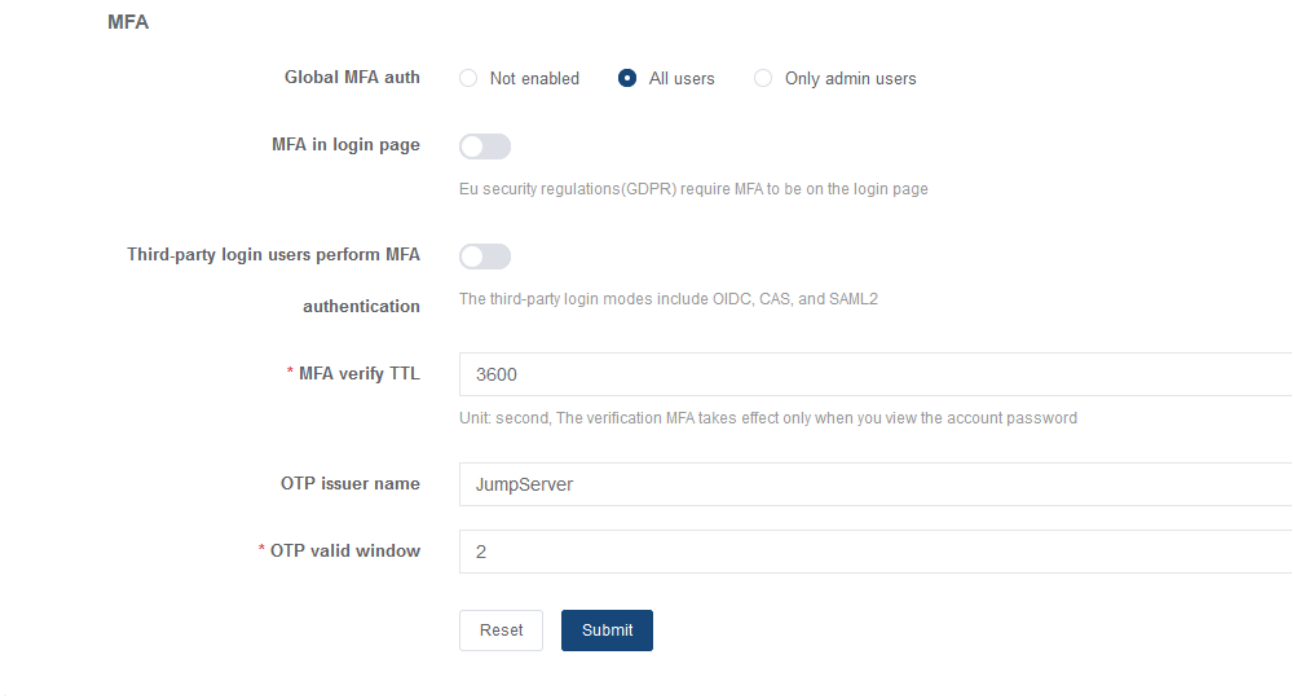
5. Нажмите **"Submit"** для сохранения настроек.

Включение встроенной 2-факторной авторизации(TOTP)

В версии **Community Edition** доступна двухфакторная авторизация через **TOTP** (Google Authenticator)

Чтобы ее включить, перейдите в раздел **System setting - Security - Auth Security**. Параметр **Global MFA auth** позволяет выключить двухфакторную авторизацию или включить ее для всех пользователей или только для администраторов.

Внимание: для корректной работы **TOTP**, на сервере JumpServer необходимо настроить NTP сервис для получения точного времени.



В **JumpServer Enterprise** также доступны другие варианты двухфакторной авторизации, например двухфакторная авторизация с помощью **RADIUS**.

Установка OpenSSH на Windows для управления УЗ Windows

Для чего устанавливать OpenSSH на Windows устройства?

OpenSSH на Windows используется для сбора информации о системе, для ротации паролей локальных УЗ Windows и для автоматического создания локальных УЗ. Если нужно подключаться по RDP, без управления учетными записями, **OpenSSH устанавливать не нужно.**

Установка OpenSSH

Вам достаточно просто запустить установочный дистрибутив OpenSSH-Win64.msi с правами администратора. Никаких настроек выполнять не нужно.

Для более безопасного подключения можно настроить авторизацию с **помощью приватного ключа**.

Настройка авторизации с помощью приватного ключа

- Настройка аутентификации на основе открытого ключа для Windows

```
ssh-keygen.exe -t rsa
cp $env:USERPROFILE\.ssh\id_rsa.pub $env:USERPROFILE\.ssh\authorized_keys
```

```
notepad C:\ProgramData\ssh\sshd_config
```

```
# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
```

```
#ListenAddress ::

#HostKey __PROGRAMDATA__/ssh/ssh_host_rsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_dsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ecdsa_key
#HostKey __PROGRAMDATA__/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
StrictModes no
#MaxAuthTries 6
#MaxSessions 10

PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile  .ssh/authorized_keys

#AuthorizedPrincipalsFile none

# For this to work you will also need host keys in %programData%/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no

# GSSAPI options
#GSSAPIAuthentication no

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
#PermitTTY yes
#PrintMotd yes
```

```
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
#PermitUserEnvironment no
#ClientAliveInterval 0
#ClientAliveCountMax 3
#UseDNS no
#PidFile /var/run/sshd.pid
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# override default of no subsystems
Subsystem   sftp    sftp-server.exe

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server

# 6C914E974E88E8CA86862124 4C
#Match Group administrators
#       AuthorizedKeysFile __PROGRAMDATA__/ssh/administrators_authorized_keys
```

```
net stop sshd
net start sshd
```

Использование приватного ключа

```
ssh user@ip -i <private_key_absolute_path>        (local users)
ssh user@domain@ip -i <private_key_absolute_path> (Domain users)
```

Настройка отправки событий по Syslog

1. Изменение конфигурационного файла JumpServer

Конфигурационные файлы JumpServer по умолчанию находятся в: `/opt/jumpserver/config/config.txt`

В конфигурацию JumpServer необходимо добавить следующие элементы:

```
# Настройка syslog
SYSLOG_ENABLE=true
SYSLOG_ADDR=10.1.12.116:514  # IP и порт сервера Syslog
SYSLOG_FACILITY=local2  # В соответствии с конфигурацией файла Syslog
```

2. Перезапуск JumpServer

После изменения конфигурационного файла JumpServer необходимо перезапустить для загрузки новых конфигураций.

Команда:

```
jmsctl restart
```

3. Проверка конфигурации

Войдите в службу JumpServer, чтобы создать журнал входа, и проверьте, есть ли вывод на сервере Syslog. Пример выходного журнала входа:

4. Анализ информации журнала Syslog

Тип события	Пример записи Syslog

Вход в систему	Apr 19 15:25:11 10.1.14.125 jumpserver: **login_log** - {"backend": "Password", "backend_display": "пароль", "city": "local", "datetime": "2023/04/19 15:18:36 +0800", "id": "cfc378e5-6337-4bf9-a8ac-15f33c2b0314", "ip": "10.1.10.35", "mfa": {"label": "отключено", "value": 0}, "reason": "", "reason_display": "", "status": {"label": "успешно", "value": true}, "type": {"label": "Web", "value": "W"}, "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, как Gecko) Chrome/112.0.0.0 Safari/537.36 Edg/112.0.1722.48", **"user name": "admin"**}
Ззагрузка файла	Apr 19 15:27:26 10.1.14.125 jumpserver: **ftp_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:20:51 +0800", "filename": "**/tmp/vmware-root/файл.pdf**", "id": "6e7721c0-2091-49fb-8853-fc18e0a2e432", "is_success": true, "operate": {"label": "uploading", **"value": "upload"**}, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}
Скачивание файла	Apr 19 15:28:08 10.1.14.125 jumpserver: **ftp_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "date_start": "2023/04/19 15:21:33 +0800", "filename": "**/tmp/vmware-root/файл.pdf**", "id": "113c0601-80c1-47d1-a053-5038fd89698c", "is_success": true, "operate": {"label": "скачивание файла", **"value": "download"**}, "org_id": "00000000-0000-0000-0000-000000000002", "remote_addr": "10.1.10.35", "user": "Administrator(admin)"}
Выполнение операции	Apr 19 15:28:44 10.1.14.125 jumpserver: **operation_log** - {"action": {"label": "update", "value": "update"}, "datetime": "2023/04/19 15:22:09 +0800", "id": "f844f014-2ac5-459d-abd0-ec8f853fa09c", "org_id": "00000000-0000-0000-0000-000000000004", "org_name": "SYSTEM", "remote_addr": "10.1.10.35", "resource": "GLOBAL", "resource_type": "System settings", "user": "Administrator(admin)"}
Смена пароля	Apr 19 15:29:58 10.1.14.125 jumpserver: **password_change_log** - {"change_by": "Administrator(admin)", "datetime": "2023/04/19 15:23:23 +0800", "id": "0cd278ed-8335-49d5-a0c3-0211e9858441", "remote_addr": "10.1.10.35", "user": "Глобальный MFA(MFA)"}
Запуск сессии доступа	Apr 19 15:31:29 10.1.14.125 jumpserver: **host_session_log** - {"account": "root(root)", "account_id": "49536b5e-bf06-4d16-bacd-7d628de3a3f2", "asset": "10.1.12.182-root(10.1.12.182)", "asset_id": "dfba9962-7988-4d29-9b04-6f82dd8e02c3", "can_join": true, "can_replay": false, "can_terminate": true, "comment": null, "date_end": null, "date_start": "2023/04/19 15:24:54 +0800", "has_command": false, "has_replay": false, "id": "4896b882-299a-4759-804e-32250f5b05b7", "is_finished": false, "is_success": true, "login_from": {"label": "веб-терминал", "value": "WT"}, "org_id": "00000000-0000-0000-0000-000000000002", "org_name": "default", "protocol": "ssh", "**remote_addr": "10.1.10.35"**, "terminal": {"id": "7076d4aa-4050-4a2f-855b-2af7a7bd6674", "name": "[KoKo]-jumpserver-v3-86c4b2fc7167"}, "type": {"label": "normal", "value": "normal"}, "user": "Administrator(admin)", "user_id": "cdeb8352-9f45-46d9-8873-b3c7c53022fd"}
Выполнение команды	Apr 19 15:34:00 10.1.14.125 jumpserver: **session_command_log** - {"account": "root(root)", "asset": "10.1.12.182-root(10.1.12.182)", "id": "28400256-e9e2-4454-8127-4880fe5b9684", **"input": "free -h", "org_id": "00000000-0000-0000-0000-000000000002", "output": "free -h\r\n total used free shared buff/cache available\r\nMem: 7.6G 4.3G 136M 28M 3.2G 3.0G"**, "remote_addr": "10.1.10.35", "risk_level": {"label": "обычный", "value": 0}, "session": "4896b882-299a-4759-804e-32250f5b05b7", "timestamp": 1681889159, "timestamp_display": "2023/04/19 15:25:59 +0800", "user": "Administrator(admin)"}

Настройка RDS (RemoteApp) для публикации приложений

Примечание: Community Edition поддерживает только режим публикации HTTP приложений.

RemoteApp - это публикация приложений на Microsoft RDS. Для ее использования вам необходим Windows Server с настроенным RDS(RemoteApp). **JumpServer** сможет подключаться к приложениям, опубликованным на RDS сервере и авторизовываться в них. В основном это актуально для приложений для работы с СУБД и веб-интерфейсами.

Для поддержки RemoteApp необходимо настроить JumpServer и сервер RDS.

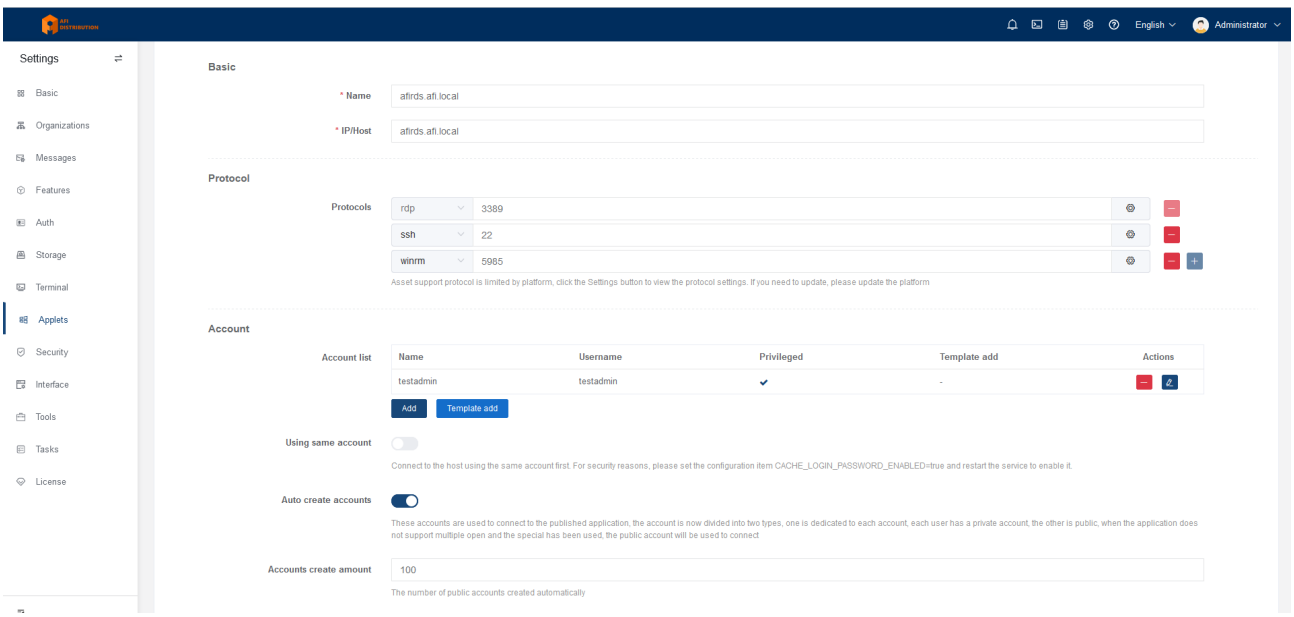
Требования:

- MS Windows Server 2016 или MS Windows Server 2019
- Установленная роль RDS (Remote Desktop Services)

Настроенный WinRM или установленный OpenSSH

Добавление сервера публикаций в JumpServer

Зайдите в **"System settings - Applets",** выберите вкладку **"Remote Hosts"** и нажмите **"Create".**



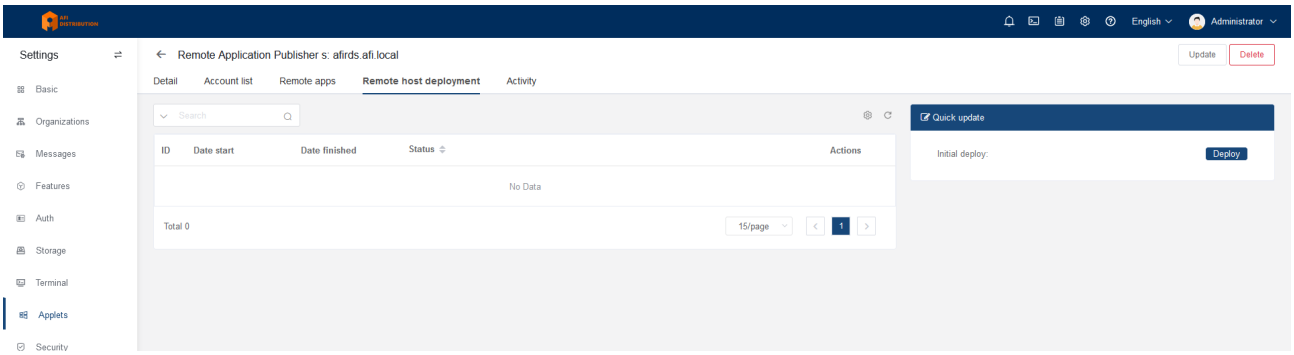
Описание параметров:

Параметр	Описание
ame	Имя устройства
P/Host	IP или сетевое имя RDS сервера
rotocol group	Протоколы и номера портов. Укажите здесь WinRM или SSH, если будет использова
ccount List	Учетная запись с правами администратора для доступа к RDS серверу
utomatically create an account	Включить автоматическое создание учетных записей для подключения к опублико
lumber of accounts created	Количество создаваемых учетных записей.
ore service address	Адрес связи между агентом машины для публикации удалённых приложений и бе Замените адрес http:127.0.0.1 на IP вашего сервера
DS license	Настройка сервера лицензирования RDS
DS License Server	Параметры сервера лицензирования RDS.
DS authorization mode	Выберите "Device" или "User" для настройки режима авторизации. A. Device: Позволяет одному устройству (любому пользователю, использующему ег публикаций удалённых приложений. B. User: Предоставляет одному пользователю доступ к серверу публикаций удалён неограниченного числа клиентских компьютеров или устройств.
DS single user single session	Выберите "Disable" или "Enable" для настройки режима одиночной сессии для одн A. Disable: Разрешить каждому пользователю подключаться к удалённому рабочем клиентских компьютеров одновременно. B. Enable: Запретить каждому пользователю подключаться к удалённому рабочему клиентских компьютеров одновременно.
DS maximum disconnect time	Если сессия достигает этого максимального времени, соединение разрывается.
DS remote application logout ime limit	Время выхода после разрыва сессии удалённого приложения.

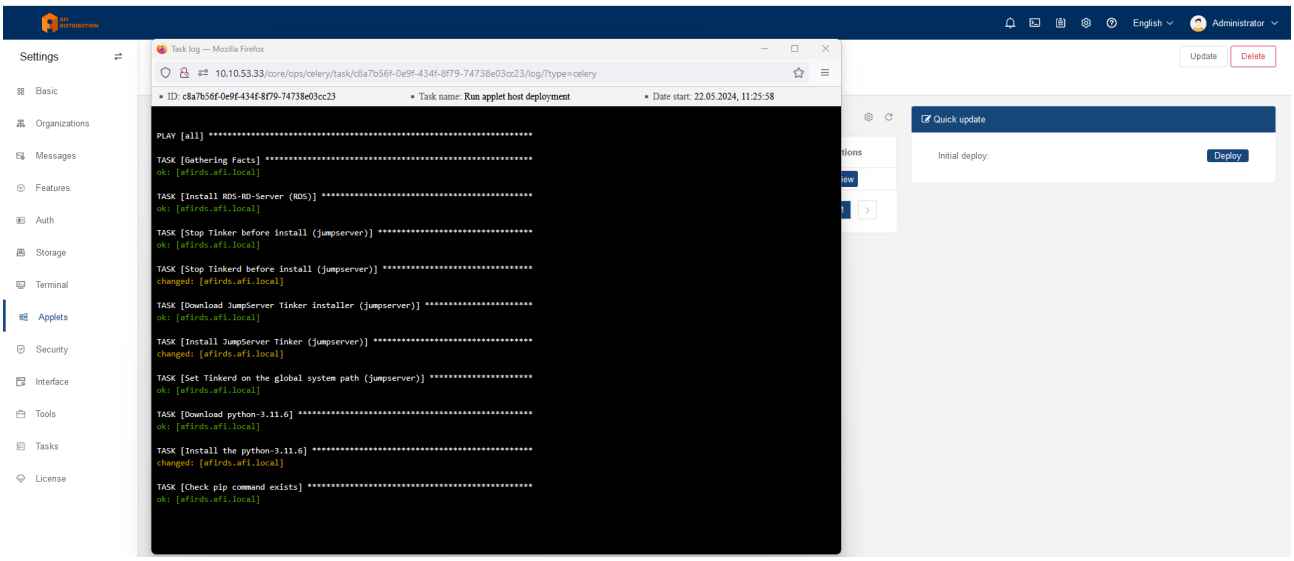
Нажмите **"Submit"** для сохранения настроек.

Установка механизма публикации приложений

Нажмите на название добавленного сервера публикаций. Откроется информация о сервере, перейдите во вкладку **"Remote host deployment"** и нажмите кнопку **"Deploy"** в правой части экрана**.**



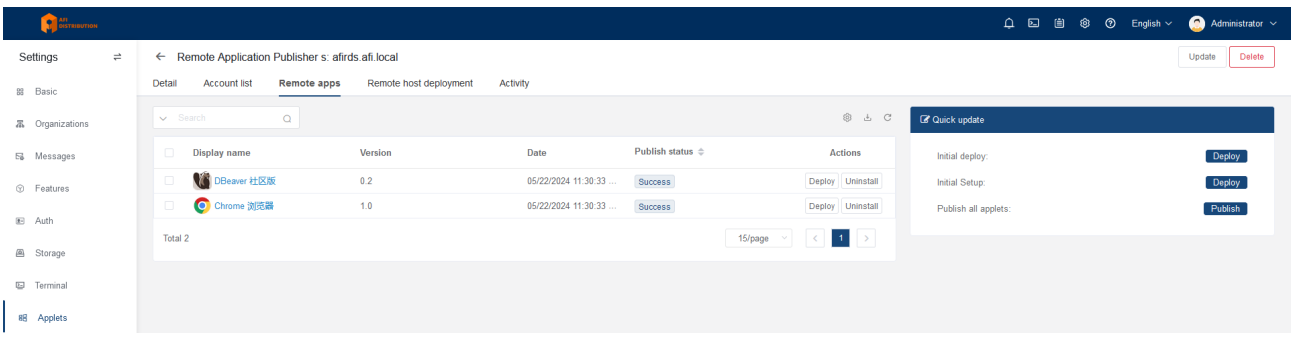
Откроется окно, где будет отображаться процесс установки:



Публикация приложений

Вам не нужно вручную устанавливать приложения на RDS сервер, у JumpServer есть готовые апплеты, которые автоматически установят и опубликуют нужные вам приложения. Существующие апплеты доступны в онлайн портале, где вы их сможете скачать.

Для публикации приложения зайдите во вкладку **"Remote Apps"**, тут вы видите список добавленных апплетов, их статус и кнопки **"Deploy"** и**"Uninstall"** для установки и удаления апплетов с сервера публикаций.



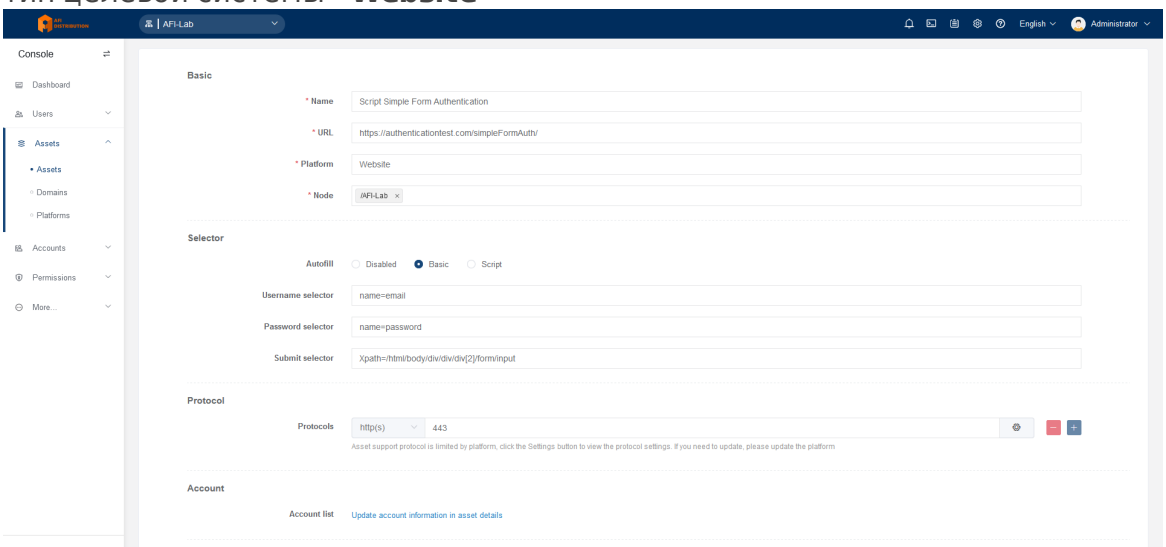
Если у апплетов статус **"Success"** то вы можете добавлять устройства и подключаться к ним с помощью соответствующих приложений. Для подключения к веб-интерфейсам(**HTTP**) можно использовать апплеты **Chrome** или **Firefox**.

Настройка подключения к устройству по HTTP(веб-интерфейс)

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

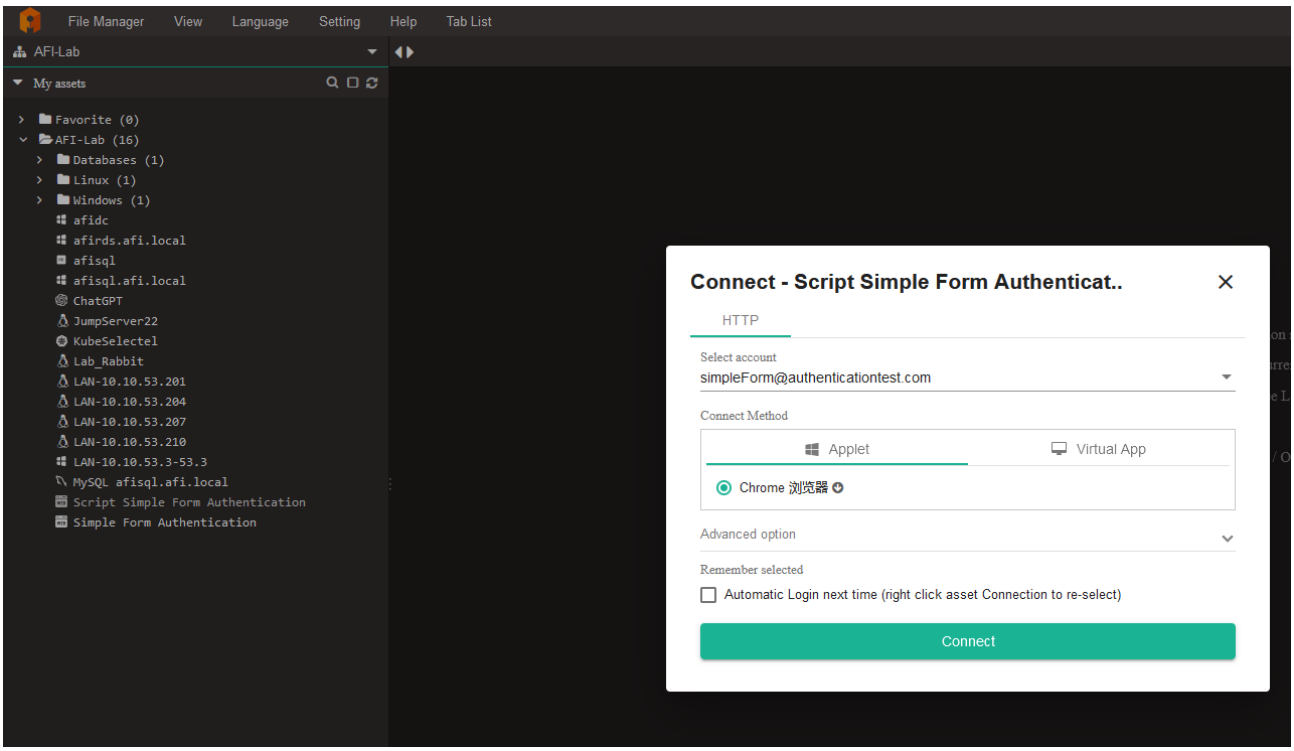
При таких настройках, имя пользователя будет введено в HTML элемент с **name="email"**, пароль будет введет в HTML элемент с **name="password"** и затем будет нажата кнопка с **Xpath=/html/body/div/div/div[2]/form/input**

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".**

Подключение к веб-интерфейсам через веб-терминал

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



Настройка Panda для публикации приложений

JumpServer поддерживает использование как Windows Server, так и Linux в качестве машины для публикации приложений,например для публикации браузеров Chrome и Firefox для HTTP сессий и различных клиентов для работы с СУБД.

Типы публикации приложений:

Microsoft RemoteApp: способ публикации приложений на базе Windows Server, обеспечивающий максимальную плавность работы. Требует дополнительной настройки Windows Server и приобретения Microsoft RDS CALs.
Panda (Виртуальное приложение): способ публикации приложений на базе Linux, характеризующийся средней плавностью работы, хорошей совместимостью и поддержкой таких операционных систем, как CentOS, RedHat, Kylin и openEuler.

Настройка Panda для публикации приложений.

Принцип работы:
Машина для публикации приложений на базе операционной системы Linux использует контейнерную технологию, которая изолирует приложение в независимой среде выполнения. С помощью компонента Panda, предоставляемого JumpServer, осуществляется управление виртуальными приложениями.

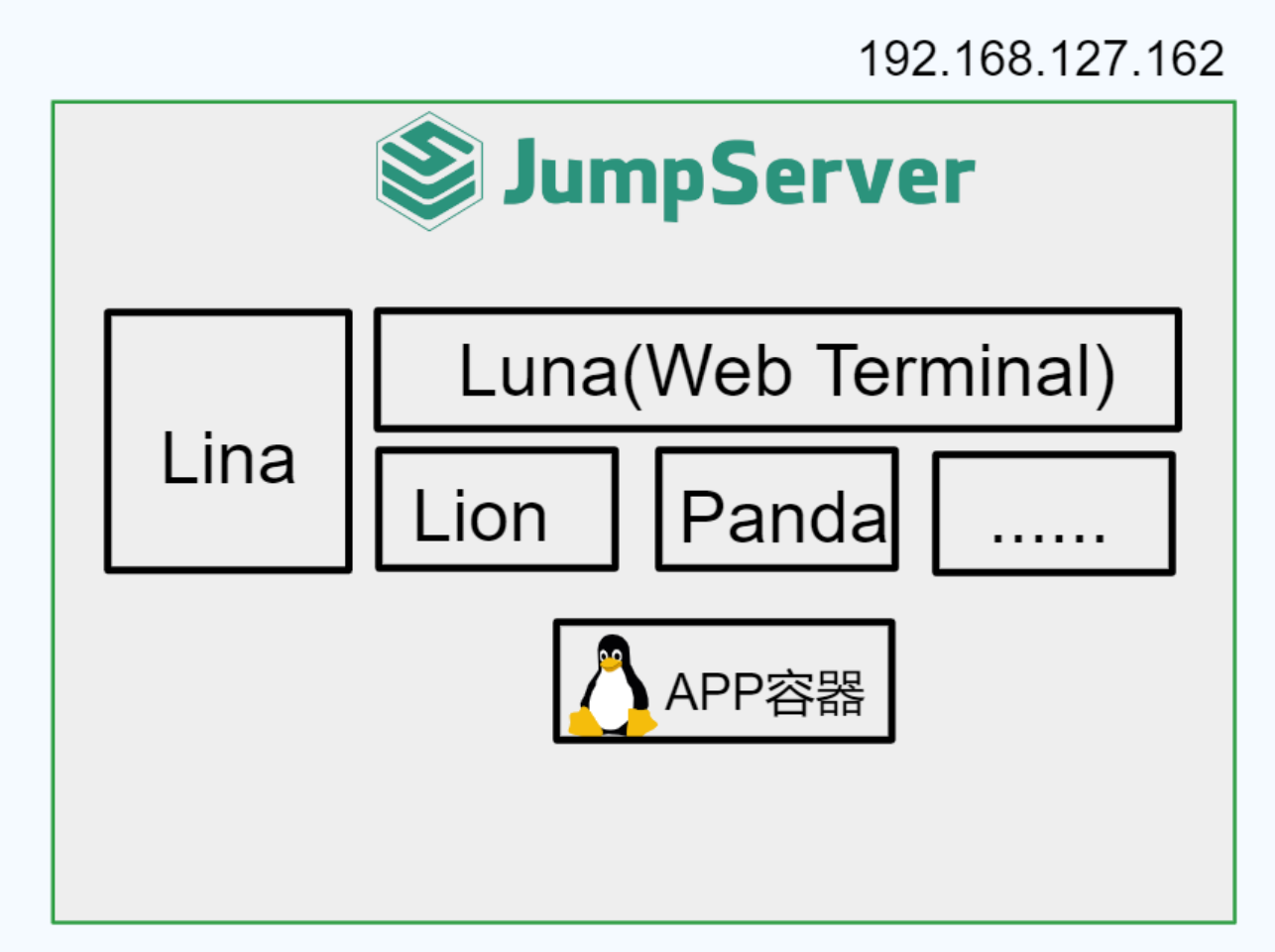
Процесс выглядит следующим образом:

1. Пользователь получает доступ к Web Terminal JumpServer и подключается выбранному виртуальному приложению.
2. Компонент Panda создает GUI-контейнер на базе VNC и передает информацию о подключении VNC компоненту Lion.
3. Компонент Lion подключается к данному контейнеру.

Схемы развертывания

Схема 1: All in One

Использование сервера, на котором развернут JumpServer, в качестве машины для публикации виртуальных приложений.



1. Настройка основного конфигурационного файла

Откройте основной конфигурационный файл JumpServer.

```
nano /opt/jumpserver/config/config.txt
```

И добавьте в него следующие параметры

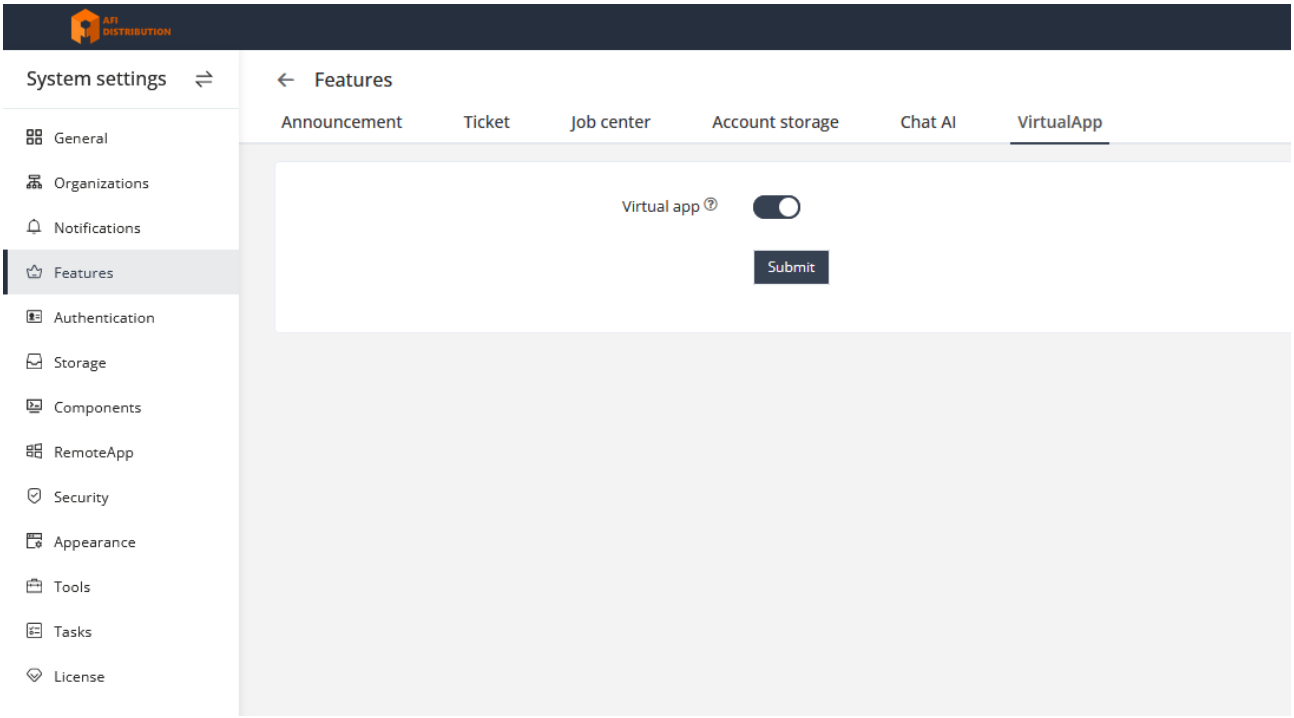
```
# Включение компонента Panda
PANDA_ENABLED=1
# Включение виртуальных приложений в ядре
VIRTUAL_APP_ENABLED=1
# IP-адрес хоста Panda (IP JumpServer)
PANDA_HOST_IP=192.168.127.162
# URL-адрес для компонента Lion к Panda
PANDA_HOST=http://panda:9001
```

Перезапустите сервис JumpServer, чтобы применить изменения.

```
[root@localhost ~]# jmsctl restart
```

2. Включение функции виртуальных приложений

В консоли управления JumpServer перейдите в **System Settings→ Features → VirtualApp** и активируйте функцию виртуальных приложений.

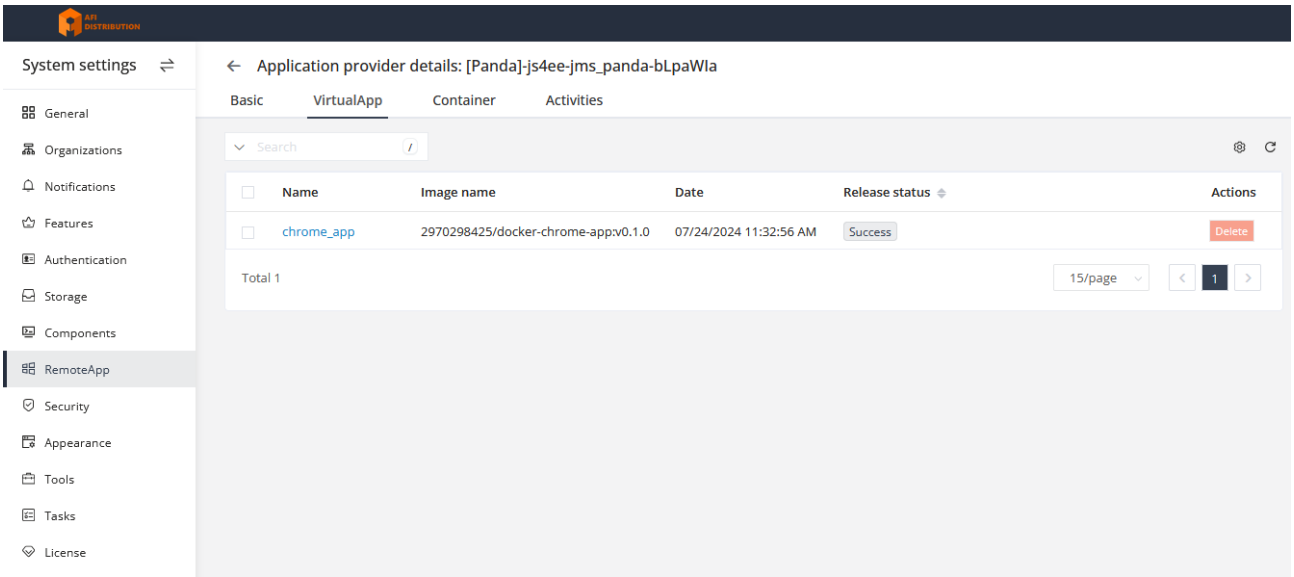


3. Загрузка виртуальных приложений

Загрузите виртуальные приложения локально. В настоящее время поддерживаются браузер **Chrome**, клиент базы данных **Dbeaver**. **Дистрибутивы этих приложений доступны на портале вендора, приложения для Panda находятся в разделе Virtual App, остальные апплеты только для RemoteApp(RDS).**

В консоли управления **JumpServer** перейдите в **System Settings → RemoteApps** и загрузите виртуальные приложения в раздел **VirtualApp**.

После короткого ожидания приложение будет автоматически развернуто на машине для публикации приложений. В консоли управления **JumpServer** в разделе **System Settings → RemoteApps → Application Providers → VirtualApp** можно увидеть успешное развертывание приложения.

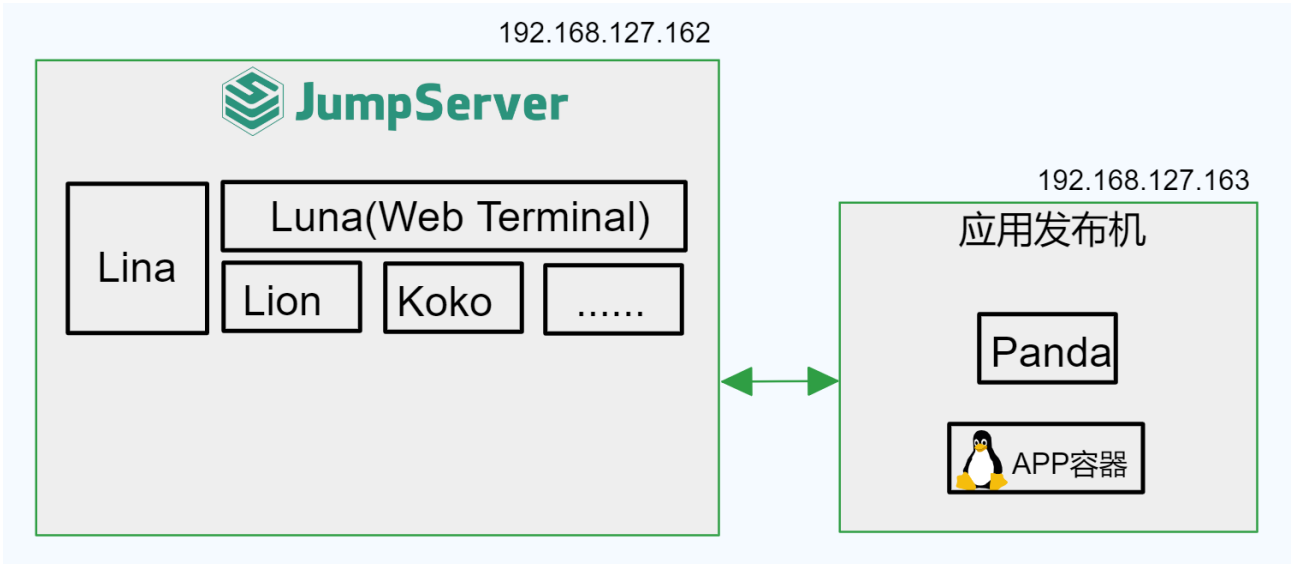


4. Использование виртуальных приложений

Подключитесь к активам, используя виртуальные приложения.

Примечание: В этот момент в сервисе JumpServer будет запущен контейнер виртуального приложения: **2970298425/docker-chrome-app:v0.1.0** (Примечание: этот контейнер весит около 1.3GB, требуется загрузка через интернет. В локальной сети можно загрузить его вручную).

Схема 2: Panda на другом сервере



1. Настройка основного конфигурационного файла

Откройте основной конфигурационный файл JumpServer.

```
nano /opt/jumpserver/config/config.txt
```

И добавьте в него следующие параметры

```
# Включение компонента Panda
PANDA_ENABLED=0
# IP-адрес Panda для компонента Lion
PANDA_HOST=http://192.168.127.163:9001
```

Перезапустите сервис JumpServer, чтобы применить изменения.

```
[root@localhost ~]# jmsctl restart
```

2. Установка Panda на сторонней машине

Распакуйте установочный пакет JumpServer на машине для публикации, установите Docker и Docker Compose, загрузите образ.

```
[root@panda ~]# tar xzvf jumpserver-offline-release-v3.10.6-amd64.tar.gz -C /opt
```

Установите Docker и Docker Compose:

```
[root@panda ~]# cd /opt/jumpserver-offline-release-v3.10.6-amd64/scripts
[root@panda scripts]# ./2_install_docker.sh
```

Загрузите образ Panda:

```
[root@panda scripts]# cd images
[root@panda images]# docker load -i panda:v3.10.6.tar
```

Создайте docker-compose для Panda:

```
[root@panda ~]# mkdir -p /data/jumpserver/panda/data
[root@panda ~]# mkdir -p panda
[root@panda ~]# cd panda
[root@panda panda]# cat docker-compose.yaml
version: '2.4'

services:
  panda:
    image: registry.fit2cloud.com/jumpserver/panda:v3.10.6
    container_name: jms_panda
    hostname: jms_panda
    ulimits:
      core: 0
    restart: always
    ports:
      - 9001:9001
    tty: true
    environment:
      - BOOTSTRAP_TOKEN=YmEyNTRkNTYtNDIyMi02OTJm
      - CORE_HOST=http://192.168.127.162
      - NAME=panda
```

```
    - PANDA_HOST_IP=192.168.127.163
  volumes:
    - /data/jumpserver/panda/data:/opt/panda/data
    - /var/run/docker.sock:/var/run/docker.sock:z
  healthcheck:
    test: "curl -fsL http://localhost:9001/panda/health/ > /dev/null"
    interval: 10s
    timeout: 5s
    retries: 3
    start_period: 10s
```

BOOTSTRAP_TOKEN берется из файла конфигурации JumpServer: /opt/jumpserver/config/config.txt

CORE_HOST - адрес вашего JumpServer

PANDA_HOST_IP - IP адрес Panda

Запустите контейнер Panda:

```
docker-compose up -d
```

3. Включение функции виртуальных приложений

Повторите шаги из раздела All in One

4. Загрузка виртуальных приложений

Повторите шаги из раздела All in One

5. Использование виртуальных приложений

Повторите шаги из раздела All in One