

Системные настройки

- [Интеграция с Active Directory\(LDAP\) и синхронизация с группами AD](#)
- [Включение встроенной 2-факторной авторизации\(TOTP\)](#)
- [Настройка отправки событий по Syslog](#)
- [Настройка RDS \(RemoteApp\) для публикации приложений](#)
- [Установка OpenSSH на Windows для управления УЗ Windows](#)
- [Как установить верные дату и время в JumpServer?](#)
- [Настройка Panda для публикации приложений](#)
- [Изменение времени жизни и повторного использования токенов подключения в JumpServer](#)
- [Настройка обнаружения активов в локальной сети и облачных платформах](#)

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.

The screenshot shows the 'Auth' configuration page with the 'LDAP' tab selected. The 'Basic' section includes a toggle for 'Enable LDAP auth' (checked), an 'LDAP server' field with the value 'ldap://afidc.afilocal:389', a 'Bind DN' field with 'testadmin@afilocal', and a 'Password' field. The 'LDAP User' section includes a 'User OU' field with 'DC=afi,DC=local', a 'User search filter' field with '(&(objectClass=user)(memberOf=CN=AFI_IT,CN=Users,DC=afi,DC=local))', and a 'User attr map' field with a JSON object:

```
{ 1: { 2: "username": "sAMAccountName", 3: "name": "cn", 4: "email": "mail" 5: }
```

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 РАМ. 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"**.

Sync setting

* Organization: Default x

Periodic perform: ☒

Regularly perform: */15 * * * *

For example: every Sunday at 03:05 execute <5 3 * * 0>
Using the 5-bit Linux crontab expression <minute hour day month week> ([Online tool](#))
If both regularly perform and cycle perform execution are set, use regularly perform first

* Cycle perform: 1

Unit: hour

Recipient: Select

Reset Submit

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:

Basic

LDAP



* Server ?

ldap://afidc.afi.local:389

* Bind DN ?

testadmin@afi.local

Password ?

Password

Search

* Search OU ?

DC=afi,DC=local

* Search filter ?

(&(objectClass=user)(memberOf=CN=AFI_IT,CN=Users,DC=afi,DC=local))

* User attribute ?

```
1 {
2   "username": "sAMAccountName",
3   "name": "cn",
4   "email": "mail",
5   "groups": "memberOf"
6 }
```

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**:

Ldap user

Please submit ldap configuration before import

Search

<input type="checkbox"/>	Username	Name	Email	Groups	Already exists
<input type="checkbox"/>	denis	Морозов Денис	-	CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=AFI_IT...	Yes
<input type="checkbox"/>	sergey	Попцов Сергей	-	CN=AFI_IT,CN=Users,DC=afi,DC=local	Yes
<input type="checkbox"/>	nlo	Наталия Орлова	no@afi-d.ru	CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=thyc...	Yes
<input type="checkbox"/>	Вася	Вася	-	CN=TestJS,OU=subOU,OU=TestOU,DC=afi,DC=local CN=AFI_IT...	Yes
<input type="checkbox"/>	testnlo	testnlo	-	CN=AFI_IT,CN=Users,DC=afi,DC=local CN=Domain Admins,CN...	Yes
<input type="checkbox"/>	TST_User	TST_User	-	CN=AFI_IT,CN=Users,DC=afi,DC=local	Yes

Total 6

15/page

< 1 >

Sync users

Import

Import all

Cancel

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:

JumpServer

Console

Dashboard

USER

User

Groups

ASSETS

Assets

Zones

Platforms

ACCOUNTS

Groups

+ Create

Actions

<input type="checkbox"/>	Name	Users
<input type="checkbox"/>	AD AFL_IT	6
<input type="checkbox"/>	AD Domain Admins	2
<input type="checkbox"/>	AD Remote Desktop Users	1
<input type="checkbox"/>	AD TestJS	3
<input type="checkbox"/>	AD thycotic	1
<input type="checkbox"/>	Default	16

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.

MFA

Global MFA auth

☐ Not enabled ☒ All users ☐ Only admin users

MFA in login page

☐

Eu security regulations(GDPR) require MFA to be on the login page

Third-party login users perform MFA authentication

☐

The third-party login modes include OIDC, CAS, and SAML2

* MFA verify TTL

Unit: second, The verification MFA takes effect only when you view the account password

OTP issuer name

* OTP valid window

Reset

Submit

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

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:

```
[root@jumpserver ~]# cat /tmp/messages
Apr 18 16:27:23 10.1.14.125 root: message:rsyslog logging From JumpServer
Apr 18 16:27:42 10.1.14.125 root: message:rsyslog logging From JumpServer(UDP)
Apr 18 16:40:42 10.1.14.125 jumpserver: login_log - {"backend": "Password", "backend_display": "密码", "city": "局域网", "datetime": "2023/04/18 16:34:08 +0800", "id": "adf0e434-e306-4693-9a51-23f256cb025d", "ip": "10.1.10.35", "mfa": {"label": "禁用", "value": 0}, "reason": "", "reason_display": "", "status": {"label": "成功", "value": true}, "type": {"label": "Web", "value": "W"}, "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/111.0", "username": "admin"}
```

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"}
Загрузка 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": "Евгений МЕН(МЕН)"}
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": "cdab8252-0f45-46d0-9872-b2c7c52022fd"}}
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\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**".

The screenshot shows the 'Applets' configuration page in JumpServer. The left sidebar contains a menu with 'Applets' selected. The main content area is divided into sections: 'Basic', 'Protocol', 'Account', and 'Using same account'. The 'Basic' section has fields for 'Name' and 'IP/Host', both set to 'afirds.afil.local'. The 'Protocol' section shows a table of protocols: rdp (3389), ssh (22), and winrm (5985). The 'Account' section includes a table with columns: Name, Username, Privileged, Template add, and Actions. The table contains one entry: testadmin, testadmin, checked, and empty. Below the table are buttons for 'Add' and 'Template add'. The 'Using same account' section has a toggle switch and a note. The 'Auto create accounts' section has a toggle switch and a note. The 'Accounts create amount' section has a text input set to 100.

Protocol	Port	Enabled	Visible
rdp	3389	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ssh	22	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
winrm	5985	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Name	Username	Privileged	Template add	Actions
testadmin	testadmin	<input checked="" type="checkbox"/>	-	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>

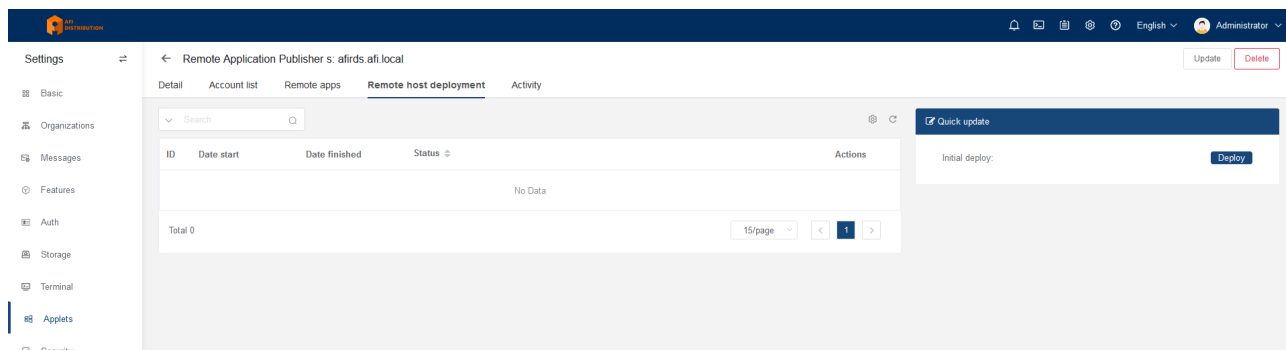
Описание параметров:

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

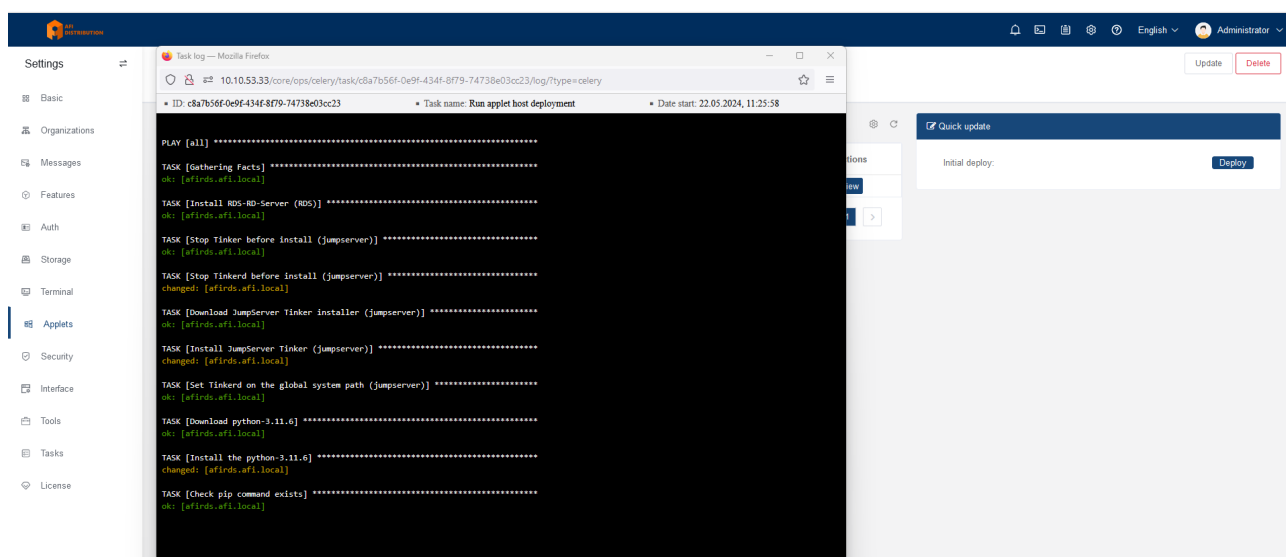
Нажмите "**Submit**" для сохранения настроек.

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.



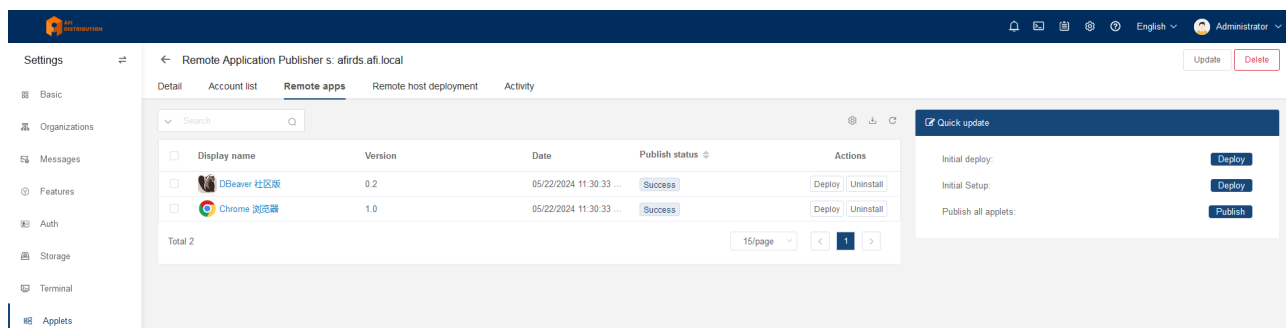
Откроется окно, где будет отображаться процесс установки:



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**.

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

# EXAMPLE
#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)
```

Как установить верные дату и время в JumpServer?

По умолчанию JumpServer устанавливается с часовым поясом Asia/Shanghai, из-за чего в различных журналах системы отображается неверное время.

Решение:

1. Установите актуальное время и часовой пояс на ОС, где установлен JumpServer

Важно, чтобы верно было не только дата, время но и часовой пояс.

Например, для Москвы в 18:11 Ubuntu Linux отвечает так:

```
root@js4ee:/home/serg# date
Wed Dec  4 06:11:33 PM MSK 2024
```

Если будет, например, Wed Dec 4 06:11:33 PM UTC 2024 - часовой пояс указан неверно.

Воспользуйтесь навыками администрирования Linux или обратитесь к администратору, чтобы настроить правильное время, часовой пояс и автоматическую синхронизацию сервера со службой точного времени (это важно в том числе для корректной работы безопасных подключений и сертификатов)

2. Откройте файл конфигурации:

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

3. В конце файла укажите ваш часовой пояс, например, для Москвы:

```
# The current running version number of JumpServer, automatically generated after installation and upgrade
#
TZ=Europe/Moscow
TIME_ZONE=Europe/Moscow
```

Внимание: если в файле только один параметр TZ, и нет параметра TIME_ZONE, то его следует добавить, чтобы было именно так как указано выше.

4. После сохранения файла конфигурации, перезапустите JumpServer:

```
# jmsctl restart
```


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. Требуется 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:

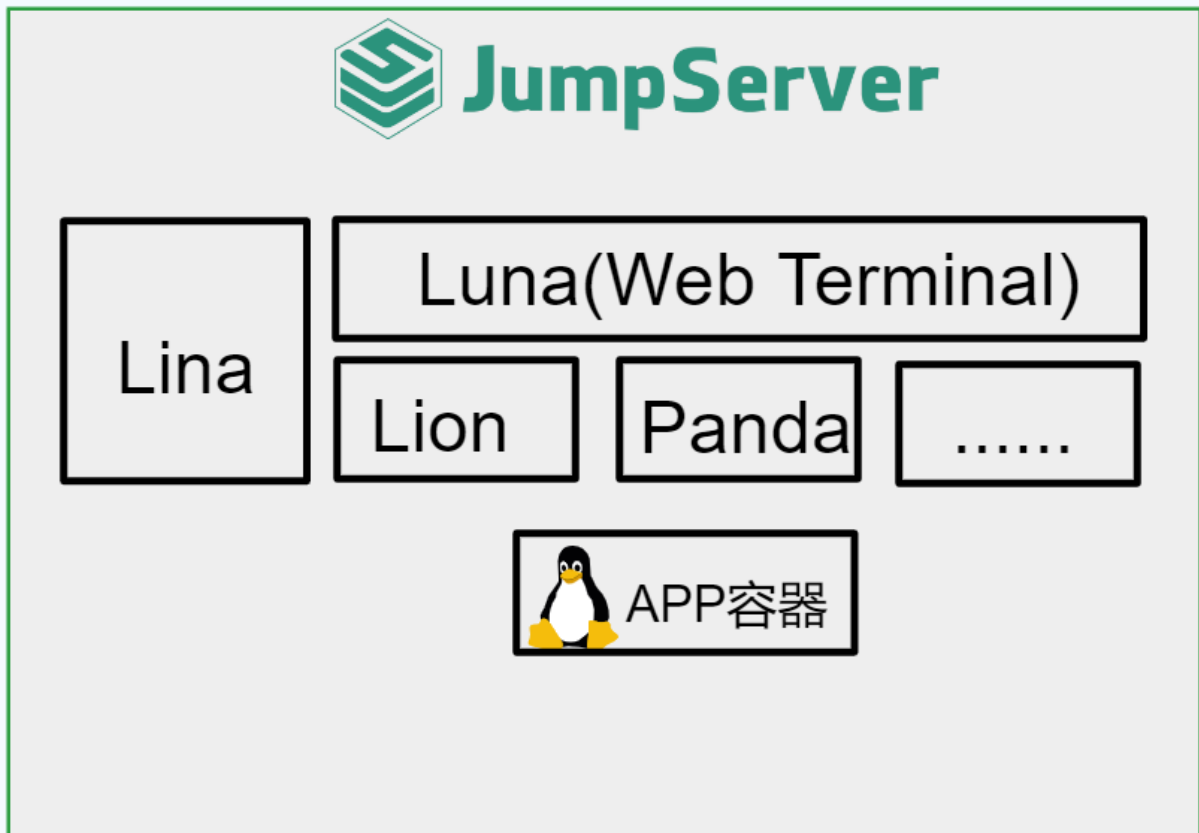
1. Пользователь получает доступ к Web Terminal JumpServer и подключается выбранному виртуальному приложению.
2. Компонент Panda создает GUI-контейнер на базе VNC и передает информацию о подключении VNC компоненту Lion.
3. Компонент Lion подключается к данному контейнеру.

Схемы развертывания

Схема 1: All in One

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

192.168.127.162



1. Настройка основного конфигурационного файла

Откройте основной конфигурационный файл JumpServer.

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

И добавьте в него следующие параметры

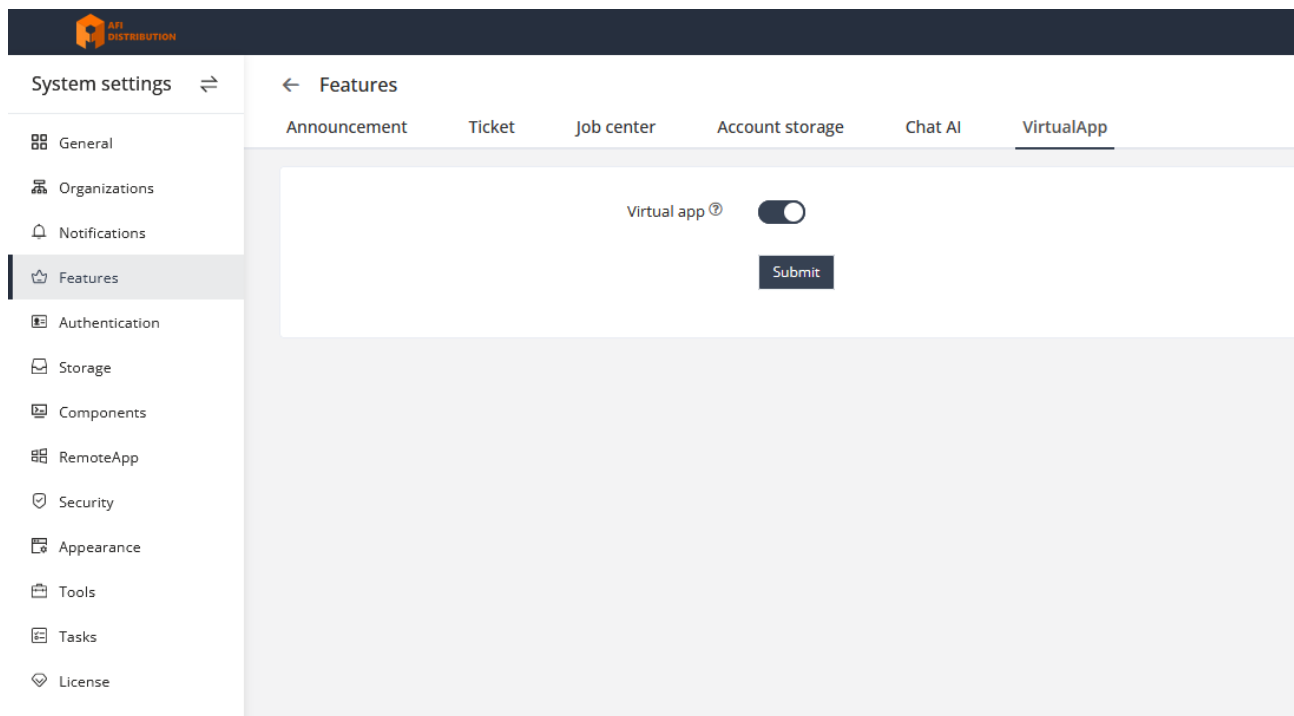
```
# Включение компонента Panda
PANDA_ENABLED=1
# Включение виртуальных приложений в ядре
VIRTUAL_APP_ENABLED=1
# IP-адрес хоста Panda (IP JumpServer)
PANDA_HOST_IP=192.168.127.162
# URL-адрес для компонента Lion к Panda
PANDA_HOST=http://panda:9001
```

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.

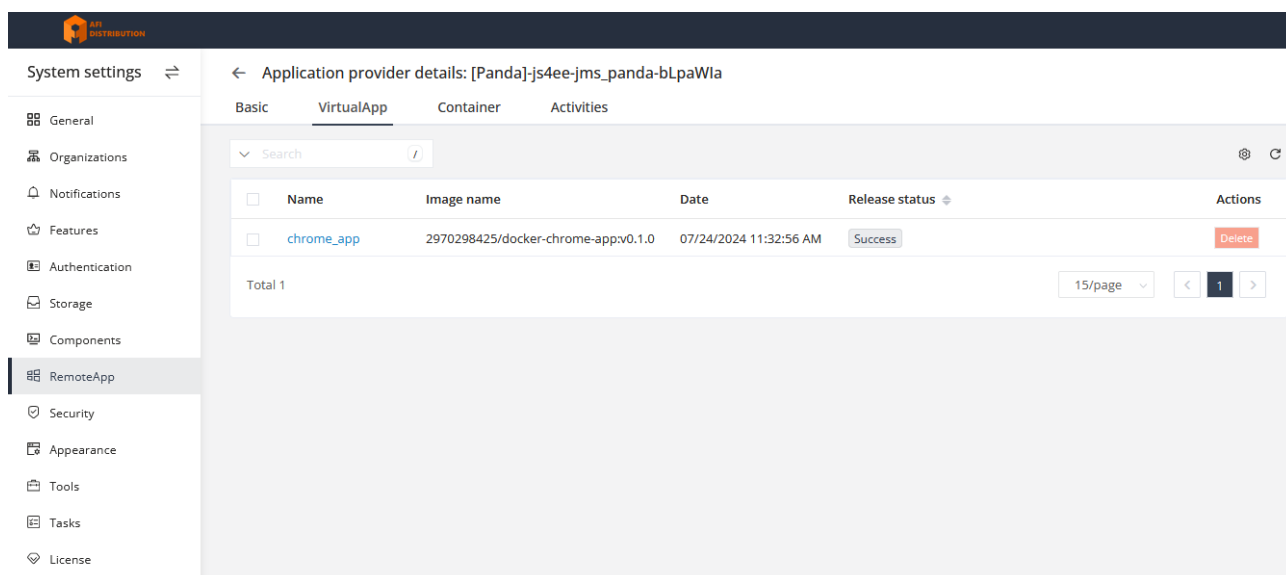


3. Загрузка виртуальных приложений

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.

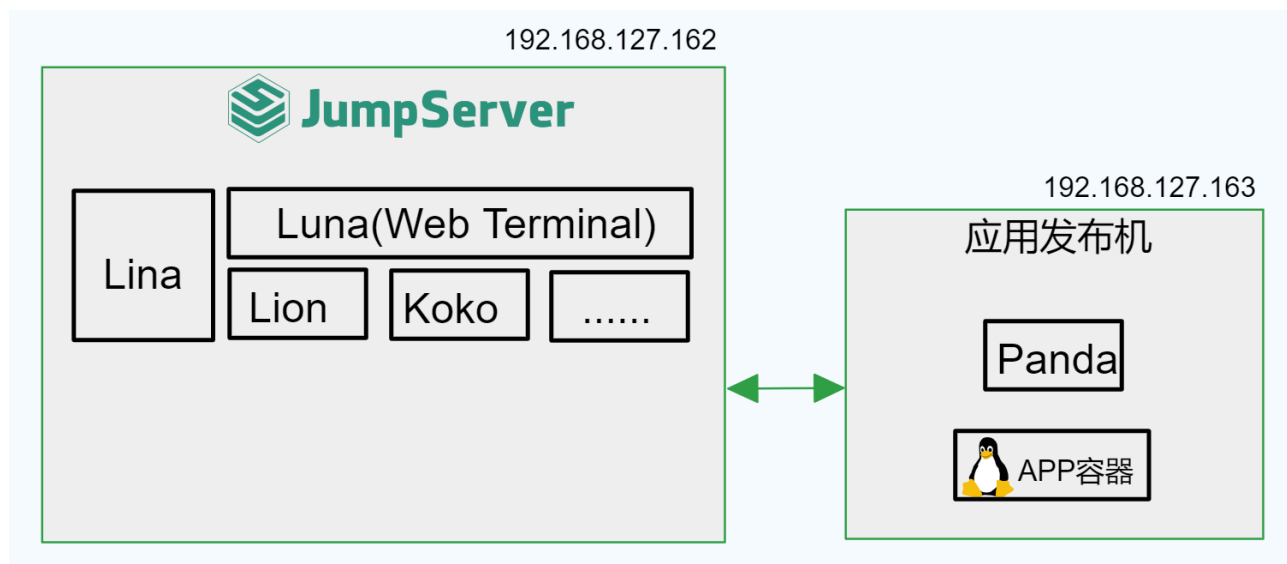


4. Использование виртуальных приложений

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

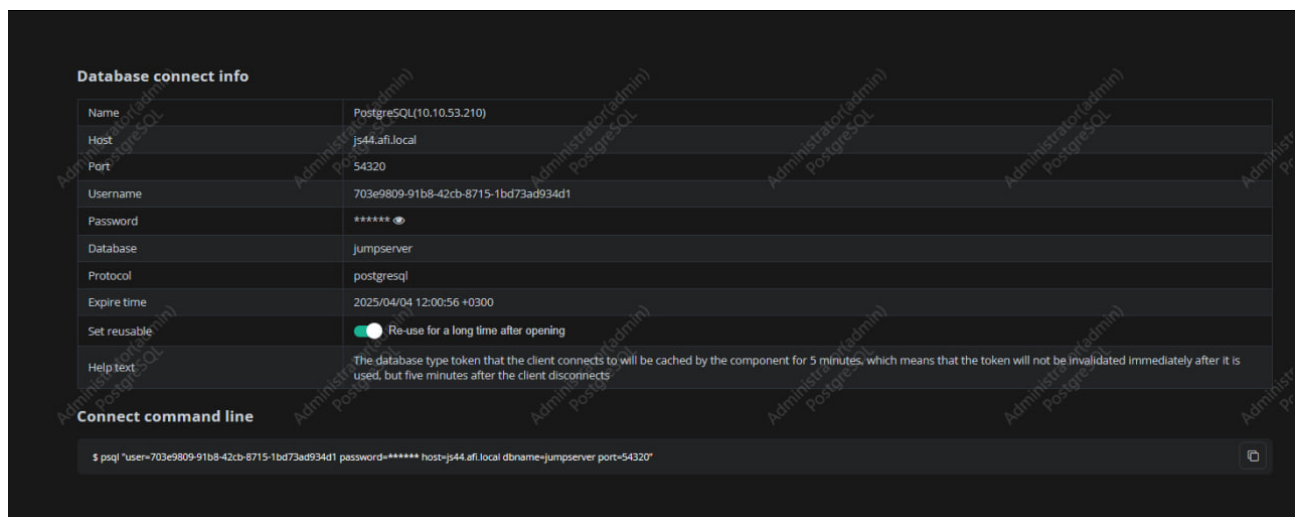
Изменение времени жизни и повторного использования токенов подключения в JumpServer

В JumpServer вы можете подключаться к целевым системам с помощью веб-интерфейса или с помощью локального клиента, например Putty, MobaXterm, Dbeaver и других, в зависимости от типа подключения.

Для подключения с помощью локального клиента вам нужно использовать одноразовые параметры авторизации, которые создает JumpServer при выборе опции "SSH Guide", "DB Guide" и тд

По умолчанию параметры подключения являются **одноразовыми** и имеют **время жизни 5 минут**, то есть при повторном подключении нужно получать новые параметры.

В некоторых случаях есть необходимость **увеличить время жизни** параметров подключения и/или разрешить повторное их использование.



Откройте файл конфигурации:

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

Добавьте в него нужные строки с нужным значением:

```
CONNECTION_TOKEN_REUSABLE=true #включение повторного использования параметров  
авторизации  
CONNECTION_TOKEN_REUSABLE_EXPIRATION=86400 #время жизни параметров авторизации в  
секундах
```

И перезапустите JumpServer:

```
jmsctl restart
```

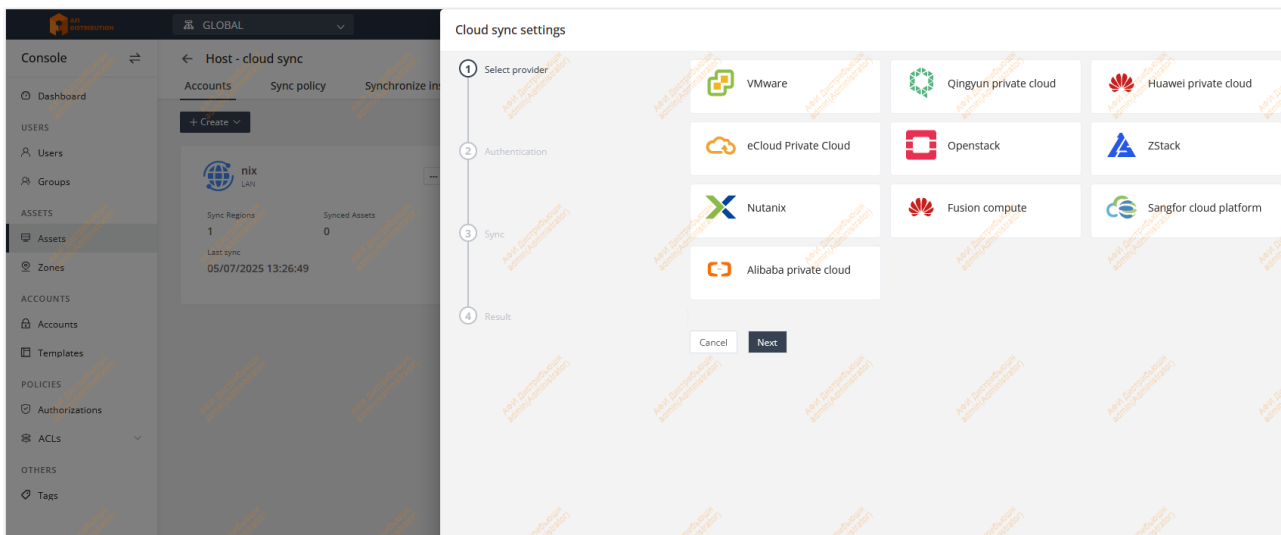
После этого при запросе новых параметров подключения вы увидите переключатель "Set reusable" и увидите, что время жизни параметров авторизации увеличивается(см скриншот).

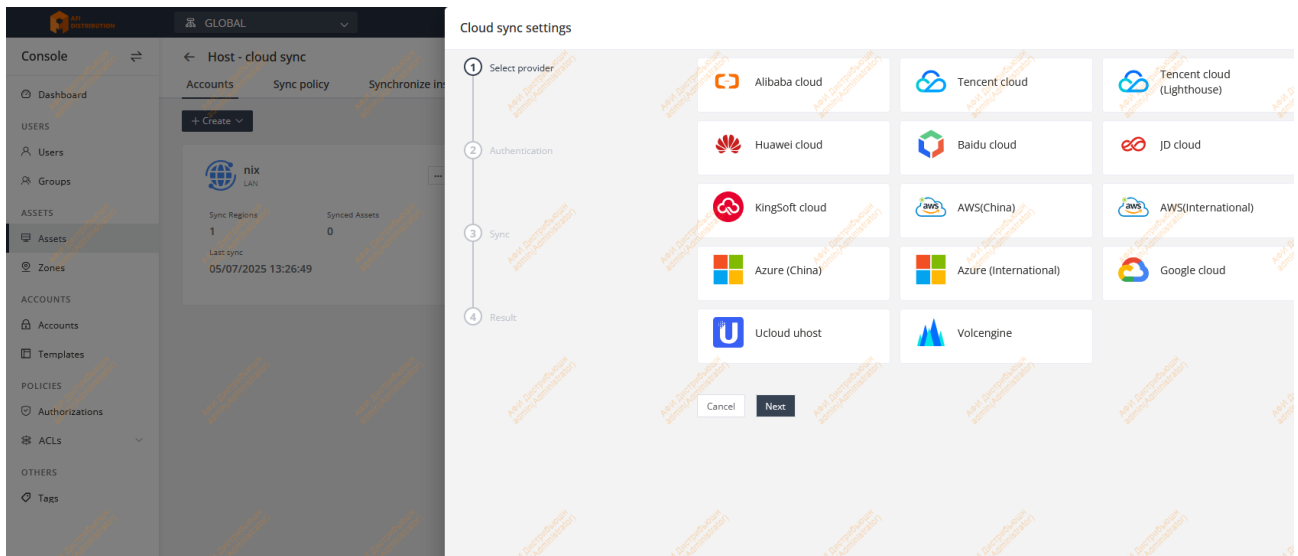
Настройка обнаружения активов в локальной сети и облачных платформах

Одна из задач при внедрении и поддержке работы PAM - это добавление и контроль списка устройств, к которым нужно организовать доступ через PAM.

JumpServer может сканировать **локальную сеть** или **облачные платформы** на наличие поддерживаемых устройств и добавлять их автоматически в список ассетов, учитывая их тип и доступные порты.

Для автоматического импорта доступны устройства, размещенные на следующих платформах(см скриншоты)

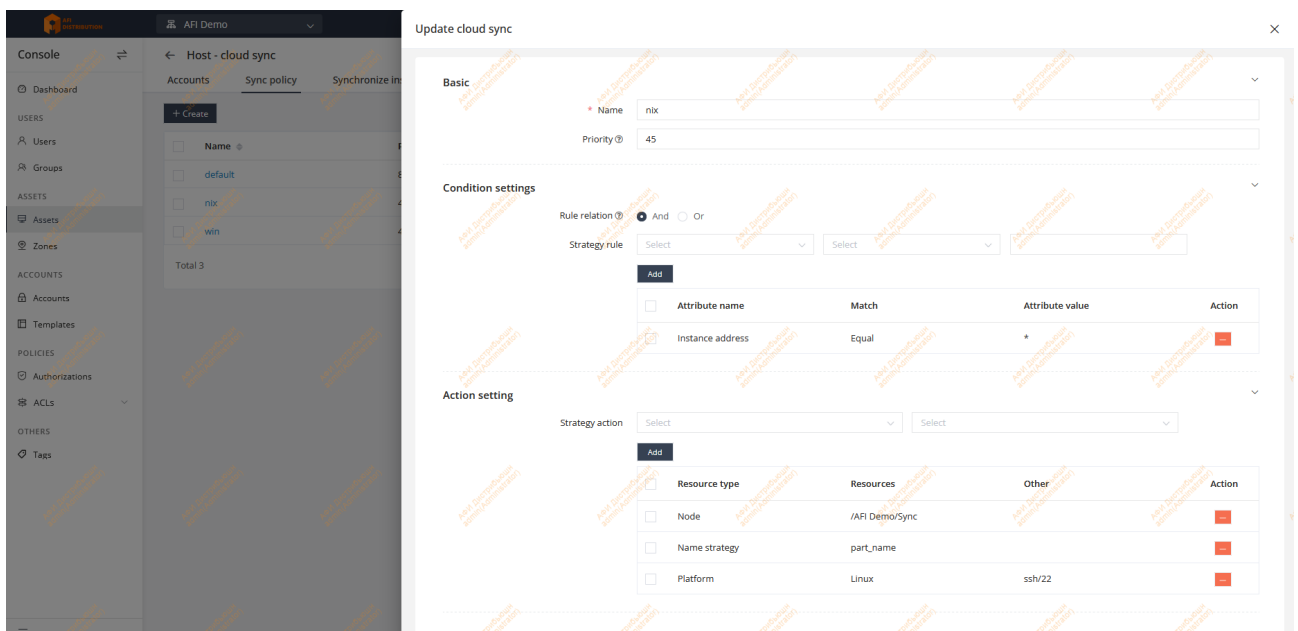




Настройка обнаружения активов в локальной сети

Настройка автоматической синхронизации

1. Зайдите в **Console - Assets - Assets**.
2. Во вкладке **Hosts** нажмите кнопку **Cloud sync**.
3. Во вкладке **Sync policy** создайте или измените существующую политику (пример на скриншоте). Политика описывает параметры, которые будут назначены активу в результате обнаружения.



4. Во вкладке **Accounts** нажмите кнопку **Create** и выберите нужный тип учетной записи - **LAN**

5. Заполните необходимые данные (см скриншот с примером сканирования локальной сети для поиска Linux систем).

Update the cloud account

Basic

* Name

Authentication

* IP segment IP segment (Enter to continue)

* Test port

* Test timeout

Hostname prefix

Other

Region [Edit \[1\]](#)

6. Нажмите **Submit** для сохранения настроек.

7. Теперь вы можете запустить обнаружение вручную (**Manually execution**) или настроить обнаружение по расписанию (**Timer execution**).

Обратите внимание на раздел **Strategy** - в нем должна быть указана ранее созданная вами политика.

Detail: nix

Basic information

ID	5d037220-act1a-4faa-845c-381c2f57c1cd
Name	nix
Provider	LAN
Category	host
Organization	AFI Demo
Validity	Yes
Date created	05/07/2025 13:03:08
Description	-
Created by	Administrator

Task details

Strategy	nix
Timer	No
Region	10.10.53.0/24
Last sync	05/07/2025 13:03:08
Date created	05/07/2025 13:03:08
Description	-

Quick update

IP type

Release assets ☐

Sync

Manually execution

Timer execution

Strategy

Select

nix