

Руководство по быстрому старту

Добавление устройств.

1. Подготовка

Приготовьте 2 устройства (для SSH и RDP) и одну СУБД для проверки функций продукта.

Например:

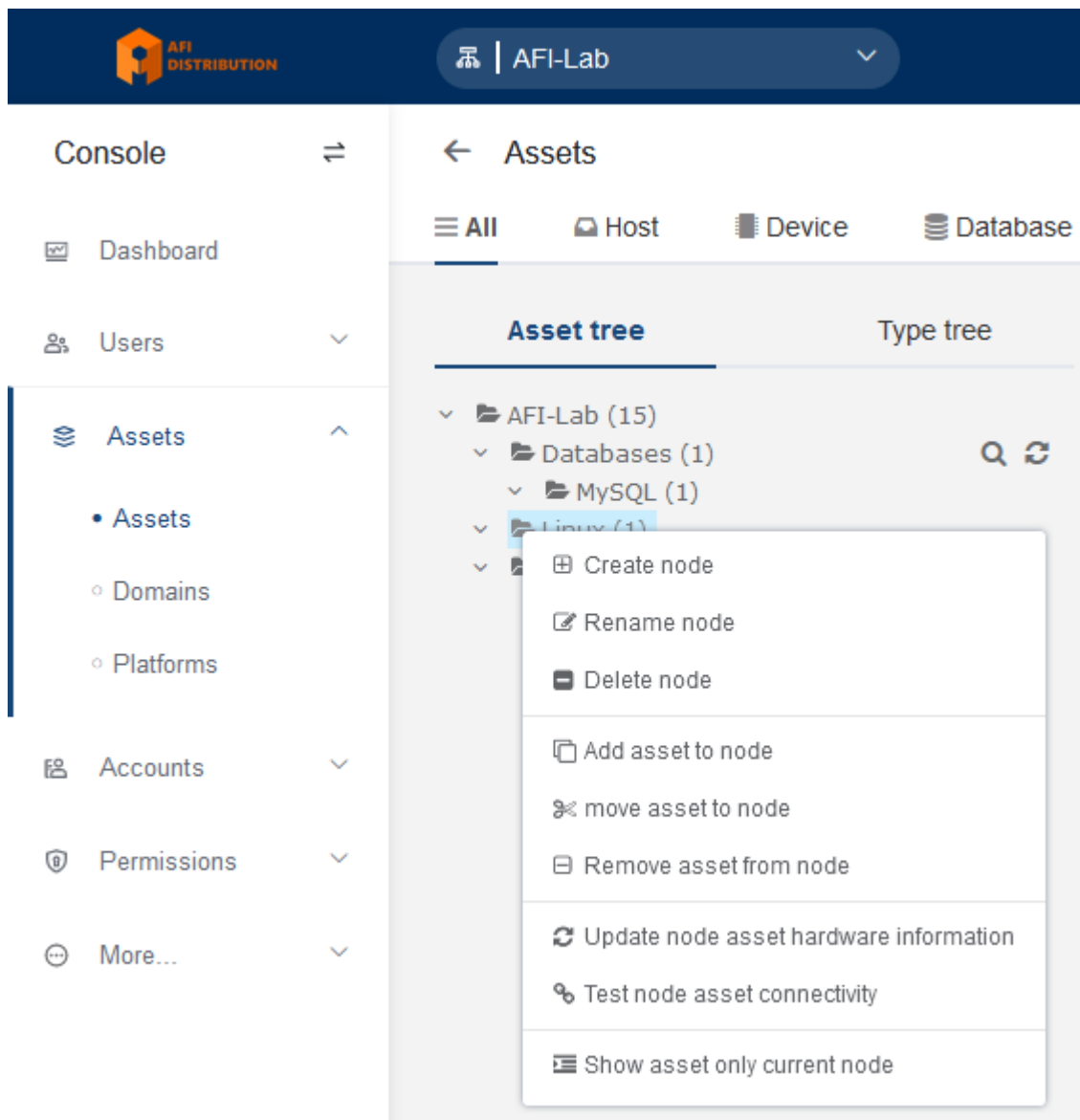
IP\Имя хоста	Порт	Тип	Учетная запись
afidc.afi.local	3389	Windows	testadmin
10.10.53.210	22	Linux	sergg
10.10.53.3	3306	MySQL	user

Если нужно, чтобы с **Windows** собиралась информация об устройстве, выполнялась смена паролей локальных УЗ, создание новых и прочие задачи, для этого необходимо настроить **SSH для Windows**.

Для подключения по **RDP** этого делать **не нужно**.

2. Редактирование дерева активов.

Перейдите в раздел **Console - Assets - Assets**, вкладка **Asset Tree**. Нажмите правую кнопку мышки в этом разделе и откроется меню редактирования дерева устройств.



Здесь вы можете создать папки(**Node**) и под-папки для ваших устройств (пункт **Create node**), все устройства можно сортировать по этим папкам.

- Одно и то же устройство может находиться одновременно в разных папках.
- Эти папки могут быть использованы при настройке политик доступа, например дать доступ ко всем устройствам в соответствующей папке.

3. Добавление активов в систему

Добавление устройства на базе Linux. Устройства Windows, MySQL и другие добавляются аналогичным образом

Нажмите кнопку **Create**, выберите тип устройства **Linux**(в разделе **Host**), заполните поля:

Name: любое понятное вам имя

IP\Host: IP адрес или DNS имя устройства

Platform: Linux

Node: папка или папки, куда будет помещено устройство при создании

Измените номера портов, если для подключения нужно использовать нестандартные порты.

The screenshot shows the APT-Infrastructure AFILab web interface. The left sidebar contains a navigation menu with the following items: Console, Dashboard, Users, Assets (expanded), Domains, Platforms, Accounts, Permissions, and More... The main content area is titled 'Basic' and contains the following sections:

- Basic:** Fields for Name (Lab_Rabbit), IP/Host (10.10.53.210), Platform (Linux), and Node (/AFILabLinux).
- Protocol:** A table with two rows. The first row has Protocol 'ssh' and Port '22'. The second row has Protocol 'sftp' and Port '22'. Below the table is a note: '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'.
- Account:** A table with the following columns: Name, Username, Privileged, Template add, and Actions. The table is currently empty, showing 'No Data'. Below the table are two buttons: 'Add' and 'Template add'.
- Other:** Fields for Domain (Select) and Label (Select).

Далее в разделе **Account**, ниже окна **Account List** нажмите кнопку **Add** для добавления учетной записи, с которой вы будете подключаться к нему. Введите имя пользователя и пароль и нажмите **Submit** для сохранения учетной записи.

Учетную запись можно будет добавить и позже или вообще не добавлять, если вы не планируете хранить пароли в PAM.

Add account



Basic

* Name

* Username

Tip: If no username is required for authentication, fill in `null`, If AD account, like `username@domain`

Privileged



Secret

Secret type



Password



SSH Key

Password



Other

Push now



Windows assets do not support pushing keys

Is active



Comment

Reset

Submit

4. Настройка разрешения доступа к устройству

Перейдите в раздел **Console - Policies - Authorization** и нажмите кнопку **Create**. Заполните нужные параметры доступа.

Console | AFI Demo

Update the asset authorization rules

Basic

Name: full access

User

Users: TST_User(TST_User) x Administrator(admin) x test-nlo(test-nlo) x testnlo.s(testnlo.s) x

Groups: AD Group_test x

Asset

Assets: Select

Nodes: /AFI Demo x

Account

Accounts: ☒ All existing accounts [Ⓢ] ☐ Specified accounts [Ⓢ] ☒ Virtual accounts [Ⓢ]

Virtual accounts

☒ Manual account [Ⓢ] ☒ Same account [Ⓢ] ☐ Anonymous account [Ⓢ]

Protocol

Protocols: ☒ All protocol ☐ Specific protocol

Name: любое удобно название для группы доступа

Users: пользователь или пользователи PAM, которые получат доступ к устройствам

Groups: группа или группы пользователей, которые получают доступ к устройствам

Assets: устройство или устройства, к которым получают доступ

Nodes: папка или папки с устройствами, к которым пользователи получают доступ

Account:

- **All existing:** разрешить подключение с любой существующей УЗ для каждого устройства
- **Specified accounts:** указать конкретные УЗ, которые можно использовать для подключения
- **Virtual Accounts:** включение дополнительных параметров авторизации
- **Manual account:** возможность ввести логин и пароль УЗ вручную, без добавления УЗ в систему
- **Same account:** подключение к целевой системе с той же УЗ, с которой пользователь авторизован в PAM (только для LDAP авторизации)
- **Anonymous account:** подключение без УЗ, обычно для подключения к веб-интерфейсам, в которых пользователи сами вводят логин и пароль

Protocol: можно ограничить протокол для подключения

Actions: если тип подключения поддерживает передачу файлов, буфер обмена или совместное использование сессии доступа, то вы можете включить или отключить эти разрешения.

Actions

- Actions
- ☒ All
 - ☒ Connect ?
 - ☒ Transfer
 - ☒ Upload ?
 - ☒ Download ?
 - ☒ Delete ?
 - ☒ Clipboard
 - ☒ Copy ?
 - ☒ Paste ?
 - ☒ Share ?

The effects of each permission vary, click the icon next to the permission to view.

Далее можно включить или выключить политику доступа и задать начало и окончание ее работы:

Other

Active ☒

Date start 2024-05-14 14:43:16

Date expired 2094-04-27 14:43:16

Comment

Save and add another

Submit

Нажмите кнопку **Submit** для сохранения настроек

5. Подключение к устройствам

Перейдите в Веб-терминал, нажав соответствующую кнопку справа сверху:



В терминале слева каждый пользователь видит только те устройства, к которым ему разрешено подключаться. Кликните на нужное устройство в списке слева, на экране появится окно выбора учетной записи и типа подключения к устройству:

Connect - MySQL afisql.afi.local

×

MYSQL

Select account

user

Connect Method

Web

Native

Applet

Web CLI

Web GUI

Advanced option

Remember selected

☐ Automatic Login next time (right click asset Connection to re-select)

Connect

Без дополнительных настроек вы сможете подключаться через веб-интерфейс по протоколам **SSH**, **RDP** и **SFTP**, а также к **MySQL** с помощью **Web CLI** или **Web GUI**. Подключения к Kubernetes, веб-интерфейсам, приложениям RemoteApp, СУБД с помощью соответствующих клиентов и другие способы будут описаны в других статьях.

Версия #7

Сергей Попцов создал 14 мая 2024 10:07:47

Сергей Попцов обновил 8 марта 2025 17:19:32