

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 for LDAP. The left sidebar contains a menu with items: Settings, Basic, Organizations, Messages, Features, Auth (selected), Storage, Terminal, Applets, Security, Interface, Tools, Tasks, and License. The main content area is titled 'Auth' and has tabs for Basic, LDAP (selected), CAS, Passkey, OIDC, SAML2, OAuth2, WeCom, DingTalk, FeiShu, Slack, and Radius. Under the 'Basic' tab, there is a section 'Basic' with a toggle for 'Enable LDAP auth' which is turned on. Below this are fields for 'LDAP server' (value: ldap://afidc.afilocal:389), 'Bind DN' (value: testadmin@afilocal), and 'Password'. A section 'LDAP User' contains a 'User OU' field (value: DC=afilocal), a 'User search filter' field (value: (&(objectClass=user)(memberOf=CN=AFI_IT,CN=Users,DC=afilocal))), and a 'User attr map' field with a JSON object: { "username": "sAMAccountName", "name": "cn", "email": "mail" }. A note below the filter field says 'Choice may be (cn|uid|sAMAccountName)=%(user)s'.

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

"username": "sAMAccountName",

2

"name": "cn",

3

"email": "mail",

4

"groups": "memberOf"

5

}

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

Groups

Dashboard

User

Groups

Assets

Zones

Platforms

Accounts

+ Create

Actions

	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

Версия #2
Сергей Попцов создал 26 апреля 2024 13:43:08
Сергей Попцов обновил 8 марта 2025 17:18:09