Интеграция Proxmox VE со службой каталога ALD Pro

06/04/2025

Содержание

Proxmox − это система виртуализации, которая дает возможность создания и управления виртуальными машинами через веб-интерфейс либо через стандартный интерфейс командной строки Linux.

В настоящей инструкции описана процедура интеграции Proxmox со службой каталога ALD Pro. Данная интеграция обеспечит возможность централизованно вести базу пользователей, аутентифицировать и авторизовывать пользователей через ALD Pro, а также управлять их доступами путем изменения членства в группах.

Инструкция предназначена для интеграции ALD Pro с системой управления виртуализацией Proxmox VE версии 7 и новее.

Интеграция осуществляется с использованием стандартного провайдера аутентификации LDAP, входящего в состав Proxmox, начиная с версии 7.

1 Описание стенда

2 Настройка

2.1 **Шаг 1**

Аутентификация и авторизация выполняются методом LDAP Bind, поэтому сначала необходимо создать сервисную учетную запись в ALD Pro, с помощью которой будет осуществляться подключение Proxmox к LDAP.

Для этого нужно подключиться по SSH к контроллеру домена и выполнить следующие шаги:

1. Создать файл с именем srv-proxmox-bind.update.
2. Внести в файл следующее содержимое:

```
dn: uid=srv-proxmox-bind,cn=sysaccounts,cn=etc,dc=test,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: srv-proxmox-bind
add:userPassword: securePassword
add:passwordExpirationTime: 20380119031407Z
add:nsIdleTimeout: 0
```

где необходимо заменить dc=test,dc=lan на параметры своего домена, а securePassword на желаемый пароль учетной записи.

3. Выполнить добавление пользователя следующей командой:

```
kinit admin && ipa-ldap-updater srv-proxmopx-bind.update
```

Такой пользователь не является POSIX-пользователем, не имеет прав на вход в компьютеры домена и не отображается в портале управления ALD Pro, а имеет права только на чтение LDAP.

2.2 **Шаг 2**

Далее необходимо настроить интеграцию на Proxmox VE. Для этого требуется зайти в «Датацентр > Разрешения > Сферы» и нажать на кнопку «Добавить», выбрав пункт «Добавить сервер LDAP» (рис. 1).

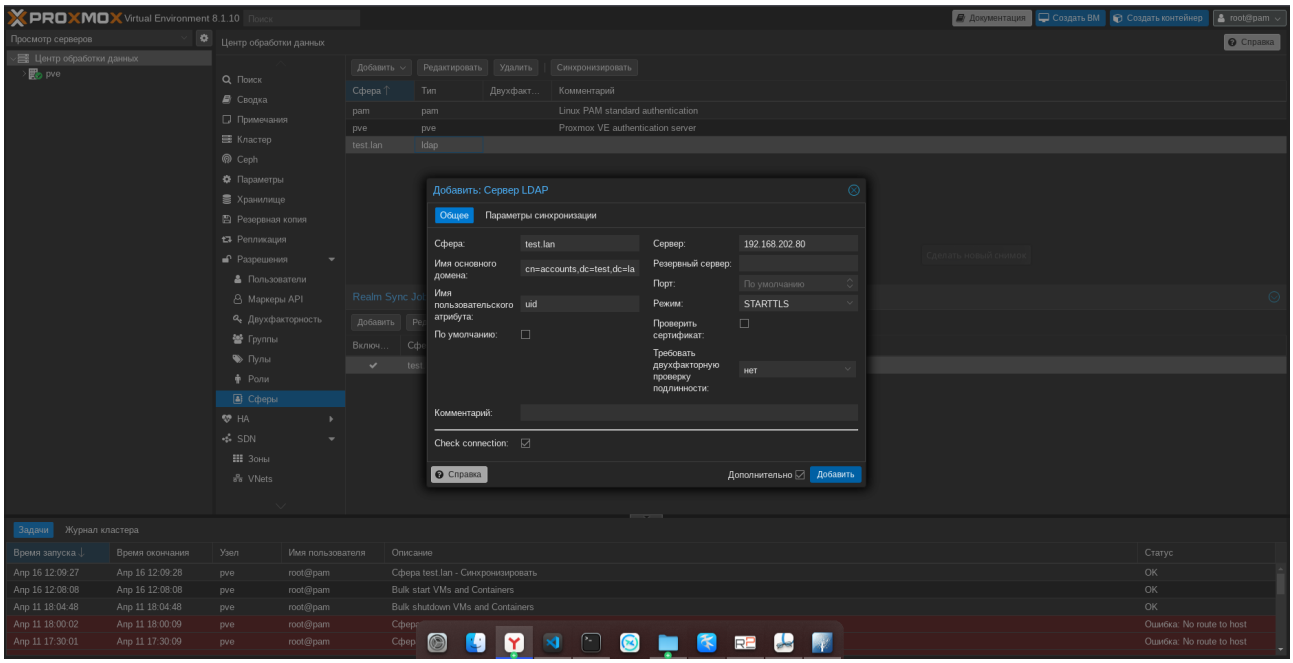

Рисунок 1 – Добавление сервера LDAP для интеграции

В появившемся окне необходимо заполнить следующие параметры (см. рис. 1):

- **Сфера** - заполнить название подключения;
- **Имя основного домена** - здесь указывается bindDN, в котором производится поиск объектов. Для ALD Pro рекомендуется указать CN=accounts,DC=test,DC=lan, где заменить dc=test,dc=lan на параметры своего домена;
- **Имя пользовательского атрибута** - атрибут, по которому определяется объект пользователя. Для ALD Pro это **uid**;
- **Сервер и Резервный сервер** - параметры, указывающие на основной и резервный контроллеры домена ALD Pro;
- **Режим** - режим подключения к LDAP. Рекомендуется использовать STARTTLS.

На вкладке «Параметры синхронизации» (рис. 2):

- **Пользователь (bind)** - сервисная учетная запись, под которой Proxmox VE выполняет запросы к LDAP. Здесь необходимо ввести DN пользователя, созданного на шаге 1. uid=srv-proxmox-bind,cn=sysaccounts,cn=etc,dc=test,dc=lan, где заменить dc=test,dc=lan на параметры своего домена;
- **Пароль (bind)** - пароль сервисной учетной записи;
- **Атрибут электронной почты** - атрибут пользователя, содержащий почтовый ящик. Для ALD Pro - mail;
- **Атрибут имени группы** - атрибут, содержащий имя группы. Для ALD Pro - cn;
- **Классы пользователей** - значение атрибута «objectClass», по которому определяется принадлежность объекта LDAP к пользователям. Для ALD Pro - posixaccount;
- **Классы групп** - значение атрибута objectClass, по которому определяется принадлежность объекта LDAP к группам. Для ALD Pro - groupOfNames;
- **Фильтр пользователей** - LDAP-фильтр для запроса пользователей. Можно оставить пустым, но рекомендуется добавить необходимых пользователей в группу на ALD Pro и указать в фильтре эту группу, чтобы не запрашивать всех пользователей домена.

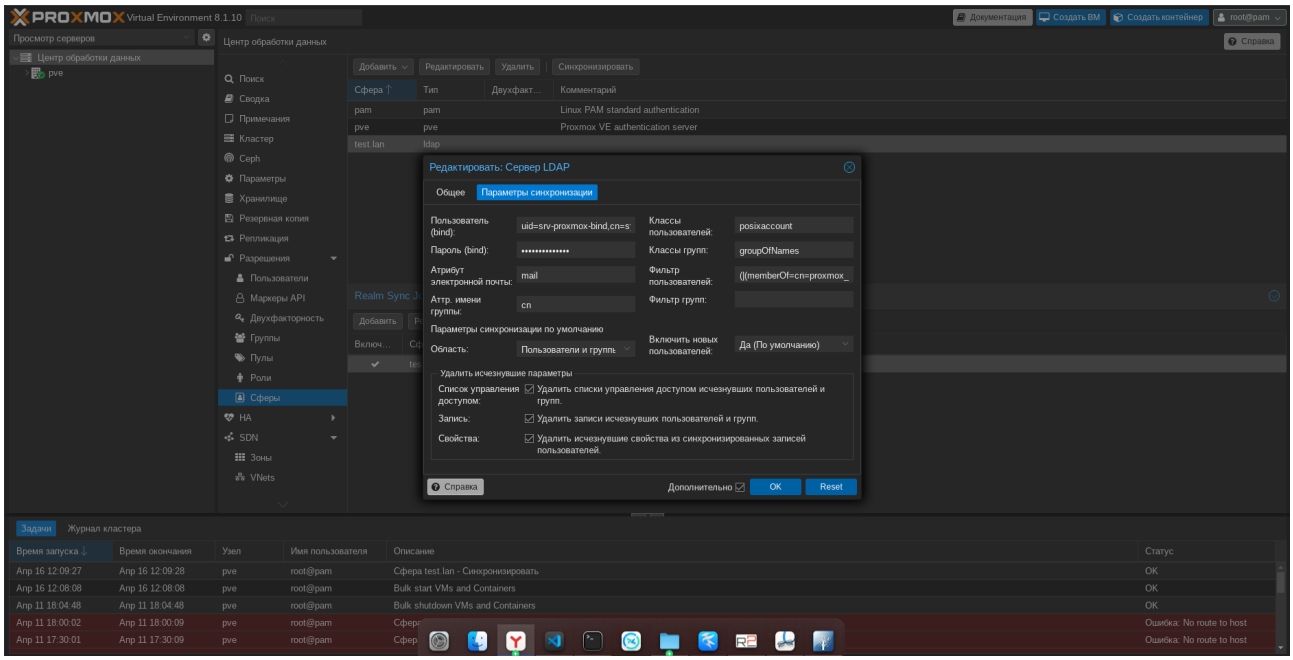

Рисунок 2 – Параметры синхронизации сервера LDAP

Пример:

```
 (|(memberOf=cn=proxmox_adm,cn=groups,cn=accounts,dc=test,dc=lan)
(memberOf=cn=proxmox_usr,cn=groups,cn=accounts,dc=test,dc=lan))
```

Здесь запрашиваются пользователи, входящие в группы proxmox_adm или proxmox_usr.

- **Фильтр групп** - аналогично предыдущему параметру, только применительно к группам.
- **Область** - определяет, какие объекты синхронизировать по умолчанию. Здесь нужно выбрать «Пользователи и группы».
- **Включить новых пользователей** - по умолчанию проставлено «Да».
- **Удалить исчезнувшие параметры** - проставить флажки напротив всех пунктов.

В графическом интерфейсе Proxmox отсутствует настройка сопоставления имени и фамилии пользователя из ALD Pro, но есть возможность ее настроить . Для этого необходимо выполнить следующую команду на сервере Proxmox VE:

```
sed -i 's/sync_attributes.*$/sync_attributes
email=mail,firstname=sn,lastname=givenName,comment=gecos/' /etc/pve/domains.cfg
```

Теперь при синхронизации будут заполняться поля имени, фамилии, почты и комментария из ALD Pro.

2.3 **Шаг 3**

Теперь, когда LDAP-подключение настроено, нужно настроить синхронизацию пользователей и групп. Для этого необходимо на этой же странице в разделе «Задания синхронизации домена» нажать кнопку «Добавить» (рис. 3, 4).

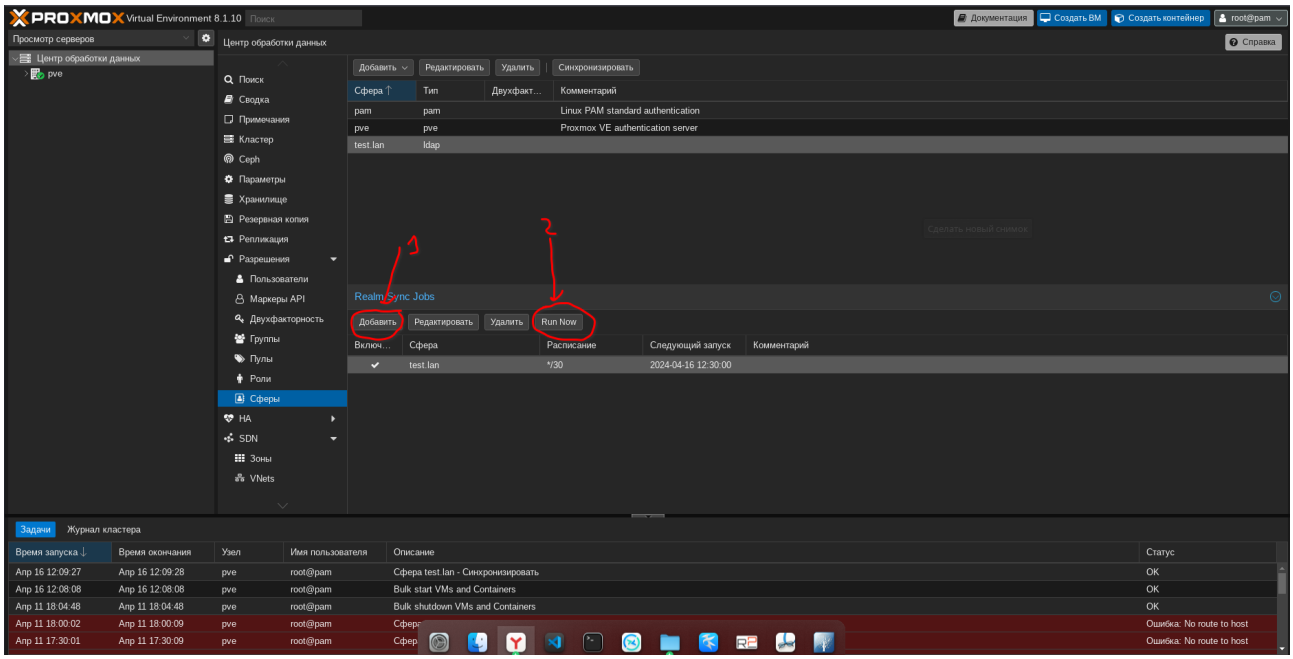

Рисунок 3 − Добавить задание синхронизации

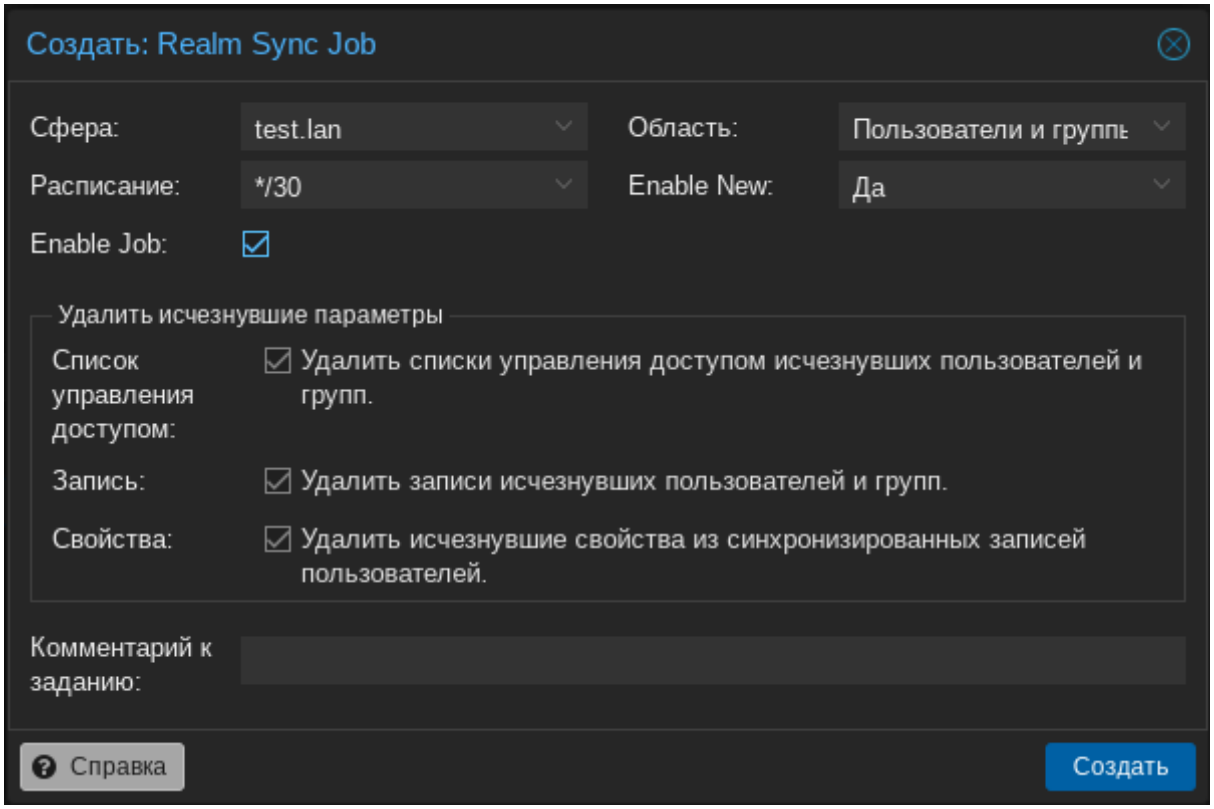

Рисунок 4 − Настройка параметров нового задания синхронизации

В появившемся окне нужно выбрать ранее созданную сферу и настроить расписание. После нажать кнопку «Выполнить сейчас», чтобы синхронизировать пользователей и группы.

2.4 **Шаг 4**

Теперь, когда группы и пользователи синхронизированы и созданы в Proxmox VE, нужно настроить им разрешения. В Proxmox это реализовано путем назначения ролей определенным группам.

Для этого необходимо перейти в раздел «Разрешения» и нажать кнопку «Добавить». В появившемся окне выбрать путь к API, группу пользователей и роль.

Пример:

Настройка административного доступа для членов группы «proxmox_adm» и пользовательского доступа для членов «proxmox_usr» (рис. 5).

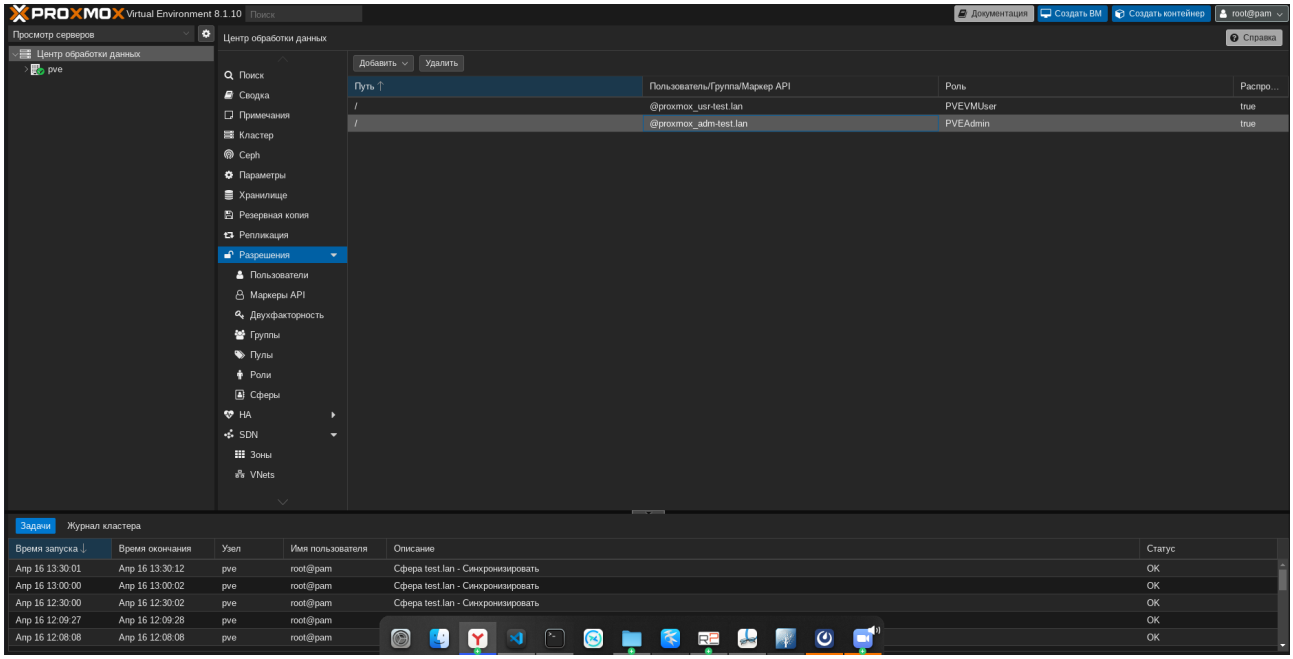

Рисунок 5 − Демонстрация примера настройки доступа

На этом настройка интеграции завершена. Теперь можно управлять правами пользователей путем изменения членства групп proxmox_adm и proxmox_usr в домене ALD Pro.