Интеграция Rocket.Chat со службой каталога ALD Pro

11/07/2025

Содержание

1 Введение

Rocket.Chat - представляет собой современную платформу для корпоративных коммуникаций и совместной работы. Она поддерживает обмен сообщениями в реальном времени, видеоконференции, аудиозвонки, управление каналами и группами. Rocket.Chat обеспечивает гибкие механизмы управления доступом, включая поддержку различных методов аутентификации и интеграцию с внешними системами каталогов.

Интеграция службы каталога ALD Pro с Rocket.Chat через протокол LDAP позволяет централизованно управлять пользователями и их доступом. При такой интеграции пользователи могут входить в Rocket.Chat с использованием своих учетных данных из ALD Pro, автоматически создаются профили пользователей с актуальной информацией (имя, фамилия, электронная почта), и пользователи распределяются по каналам и ролям в соответствии с их участием в LDAP-группах и атрибутами области подразделения.

2 Настройка сервисной учетной записи в ALD Pro

Для интеграции Rocket.Chat с ALD Pro необходимо создать сервисную учетную запись, которая будет использоваться для аутентификации и чтения данных из LDAP.

2.1 Создание сервисной учетной записи

Сервисная учетная запись не является POSIX-пользователем, не имеет прав на вход в домен и используется только для чтения LDAP. Для создания необходимо подключиться по SSH к контроллеру домена ALD Pro и выполнить следующие действия:

1. Подключитесь по SSH к контроллеру домена ALD Pro.
2. Создайте файл `ldap-bind.update` со следующим содержимым:

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

Разъяснения параметров:

- **`dn`**: уникальный идентификатор записи пользователя в LDAP;
- **`add:objectclass: account`**: добавляет базовый класс для учетной записи;
- **`add:objectclass: simplesecurityobject`**: добавляет класс для хранения пароля и атрибутов безопасности;
- **`add:uid: ldap-bind`**: уникальный идентификатор пользователя (можно изменить на требуемый);
- **`add:userPassword: securePassword`**: пароль для учетной записи (необходимо заменить на безопасный);
- **`add:passwordExpirationTime: 20380119031407Z`**:время истечения пароля;
- **`add:nsIdleTimeout: 0`**: отключает таймаут простоя.

3. Выполнить добавление пользователя следующей командой:

```
kinit admin && ipa-ldap-updater trueconf-bind.update
```

3 Настройка LDAP в Rocket.Chat

3.1 Включение LDAP

1. Войдите в Rocket.Chat с правами администратора.
2. Перейдите в раздел **Administration > Workspace > Settings > LDAP**.
3. Включите опцию Enable (Включить LDAP).

3.2 Вкладка Connection (Подключение)

Настройте параметры подключения к серверу ALD Pro:

Основные параметры:

- **Enable**: включено (True),
- **Server Type**: выберите `Other` (Другое),
- **Host**: укажите FQDN контроллера домена ALD Pro, например `dc-1.ald.company.lan`,
- **Port**: 636 (для LDAPS),
- **Reconnect**: включите для автоматического переподключения,
- **Login Fallback**: включите для возможности входа с локальной учетной записью при недоступности LDAP.

Рекомендации по безопасности: Для защиты передаваемых данных рекомендуется использовать защищенное соединение LDAPS (порт 636). При использовании SSL/TLS убедитесь, что клиент доверяет сертификату LDAP сервера.

3.3 Вкладка Authentication (Аутентификация)

Настройте параметры аутентификации:

- **Enable**: включите аутентификацию через LDAP,
- **User DN**: укажите DN сервисной учетной записи
    - *Формат: `uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan`,*
- **Password**: введите пароль сервисной учетной записи (указанный при создании).

3.4 Вкладка Encryption (Шифрование)

Настройте шифрование для защиты соединения:

Encryption: выберите метод шифрования

- **`SSL/LDAPS`** для защищенного соединения с самого начала (порт 636),
- **`StartTLS`** для обновления до защищенного соединения после подключения,
- **`plain`** без шифрования (не рекомендуется).

CA Cert: вставьте сертификат CA

- CA сертификат находится в директории **/etc/ipa/ca.crt** на контроллере домена

3.5 Вкладка User Search (Поиск пользователя)

Настройте параметры поиска пользователей в LDAP:

Search Filter (Фильтр поиска):

- **Base DN**: укажите базовый DN для поиска
  - *Пример:* `cn=accounts,dc=ald,dc=company,dc=lan`
- **Filter**: укажите фильтр для определения пользователей
  - *Рекомендуемое значение:* `(objectClass=inetOrgPerson)`
- **Scope**: `sub` (поиск по всему поддереву)
- **Search Field**: укажите атрибут для идентификации пользователей
  - *Рекомендуемое значение:* `uid`
- **Search Page Size**: 250 (количество записей на страницу)
- **Search Size Limit**: 1000 (максимальное количество записей)
- **Find user after login**: включите для подтверждения успешной аутентификации

3.6 Настройка синхронизации групп и ролей

Rocket.Chat поддерживает синхронизацию групп из LDAP с автоматическим распределением пользователей по ролям и каналам. Данная функция позволяет управлять доступом пользователей на основе их участия в группах каталога, включая возможность различного распределения участников групп по ролям в зависимости от их области (подразделения). Технические детали настройки этой функции доступны в документации Rocket.Chat.