Интеграция TrueConf со службой каталога ALD Pro

07/10/2025

Содержание

Для централизованного управления данными в крупных корпоративных структурах используют службы каталогов, работающие по протоколу LDAP. TrueConf Server поддерживает данный протокол, что упрощает администрирование и синхронизацию информации о пользователях между различными сервисами, а также использование технологии единого входа (SSO, Single Sign-On).

1 Настройка сервисной учетной записи

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

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

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

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

,где необходимо заменить dc=ald,dc=company,dc=lan на значения, соответствующие вашему домену, а securePassword — на желаемый пароль для учётной записи. При необходимости параметр passwordExpirationTime можно адаптировать в соответствии с политиками безопасности вашей организации.

3. Выполнить добавление пользователя следующей командой:

```
kinit admin && ipa-ldap-updater trueconf-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 Настройка LDAP подключения

Для настройки рекомендуется использовать подключение по защищённому протоколу LDAPS. При этом используется стандартный порт 636, и на стороне сервера потребуется установить корневой SSL-сертификат домена, в котором находится сервер ALD Pro с ролью контроллера домена, или включить TrueConf Server в домен ALD Pro

1. Откройте панель управления TrueConf Server и перейдите в Пользователи → LDAP / Active Directory.

2. В режиме хранения LDAP активируйте переключатель **Включить** и нажмите кнопку **Настройки LDAP**.

3. В открывшемся окне:

   a. В выпадающем списке Тип сервера выберите **389 Directory Server**.
   b. В поле Домен укажите FQDN или IP-адрес первого контроллера домена ALD Pro.
   c. В поле Базовый DN укажите компоненты домена, например, для доменного имени ald.company.lan значение будет dc=ald,dc=company,dc=lan (без пробелов).

4. В разделе Аутентификация выберите Простая и заполните поля Имя и Пароль. Имя должно быть указано в следующем формате:

```
uid=trueconf-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan
```

,где: uid — логин учетной записи ALD Pro с правом на чтение; cn — объекты в дереве каталога, по которым будем производить поиск пользователя; dc — атрибуты, содержащие компоненты имени сервера (FQDN) ALD Pro.

5. Нажмите кнопку **«Применить»**.

В случае успешного подключения и авторизации вам будет предложено перезагрузить сервер.

2.1 Настройка дополнительных параметров LDAP

После перезагрузки сервера раскройте вкладку **Дополнительно** и измените значение параметров, как показано ниже в таблице:

a. Обязательно (для корректного отображения групп)

LDAP-имя	Значение
Filter Disabled	(!(nsAccountLock=TRUE))
Group Member	member
Filter Group	(objectClass=groupofnames)

b. Опционально

LDAP-имя	Значение	Пояснение для ALD Pro
Display Name	displayName	Отображаемое имя
Middle Name	rbtamiddlename	Отчество
Mobile Phone	mobile	Мобильный телефон
Work Phone	telephoneNumber	Рабочий телефон
Home Phone	employeeNumber	Добавочный номер

Нажмите кнопку **Применить**. Сервер будет перезагружен.

3 Настройка Kerberos

В ALD Pro сервисная служба (SPN) привязывается к существующему узлу, по сути к A-записи DNS сервера. Поэтому, перед продолжением необходимо ввести сервер TrueConf в домен, для настройки Kerberos SSO.

3.1 Создание keytab-файла

Важно: действия, описанные в пункте c., необходимо выполнять только если сервер TrueConf ещё не был добавлен в домен ALD Pro. Если узел уже существует, переходите сразу к шагу d.

a. Откройте терминал и получите билет (kerberos-ticket) с помощью команды:

```
kinit admin # username доменного администратора
```

b. Задайте переменные с нужными значениями (без пробелов):

```
IP_ADDRESS=10.10.10.10 # IP-адрес службы (сервера TrueConf)
TRUECONF=video.adl.company.lan # Полное доменное имя сервера
FREEIPA=freeipa.adl.company.lan # Полное доменное имя контроллера домена
```

c. С помощью следующей команды добавьте узел сервера TrueConf, используя заданные переменные:

```
sudo ipa host-add --force --ip-address=$IP_ADDRESS $TRUECONF
```

d. Добавьте службу (SPN):

```
sudo ipa service-add trueconf/$TRUECONF
```

e. Для генерации keytab-файла выполните команду:

```
sudo ipa-getkeytab -s $FREEIPA -p trueconf/$TRUECONF -k trueconf.keytab
```

3.2 Настройка SSO

В разделе **Аутентификация** можно настроить способы аутентификации.

a. Нажмите на пункт **Kerberos SSO**, откроется окно добавление keytab файла.

b. Нажмите кнопку **Загрузить файл** и выберите файл, созданный на предыдущих шагах.

c. Затем нажмите **Сохранить**.

d. Включите Kerberos SSO.

Статус поменяется на **Активировано**.

3.3 Включение Kerberos SSO для различных зон

В разделе **Аутентификация**, в **Редакторе зон**, можно включить или отключать разные способы аутентификации для разных зон, для этого:

a. Выберем нужную зону и кликом по ней переходим в **Редактирование зоны**.

b. В способах аутентификации ставим галочку у Kerberos SSO.

d. Нажимаем кнопку **Сохранить**.

Теперь клиенты TrueConf, установленные на машины, подключенные к домену ALD Pro, будут автоматически проходить аутентификацию через Kerberos SSO.