Интеграция Blitz Identity Provider со службой каталога ALD Pro

09/16/2025

Содержание

1 Вводная часть

Blitz Identity Provider — российская платформа для управления идентификацией и аутентификацией пользователей, предназначенная для обеспечения безопасного доступа к корпоративным приложениям и системам. Решение поддерживает современные протоколы (SAML 2.0, OpenID Connect, OAuth 2.0, WS-Federation), единый вход (SSO), многофакторную аутентификацию (MFA) и беспарольные сценарии.

Интеграция с Astra Linux Directory Pro (ALD Pro) позволяет использовать доменные учётные записи для входа в Blitz через LDAP или Kerberos. Это упрощает администрирование, сохраняя управление доступом на стороне Blitz.

Вендор оказывает поддержку при настройке интеграции, включая помощь в пилотном тестировании и внедрении. Подробная документация доступна на официальном сайте Blitz:

- Подключение LDAP-каталога: https://docs.identityblitz.ru/latest/admin-guide/storage.html#storage
- Аутентификация по логину и паролю: https://docs.identityblitz.ru/latest/admin-guide/auth-login.html
- Аутентификация по Kerberos: https://docs.identityblitz.ru/latest/admin-guide/auth-os.html

2 Настройка сервисной учётной записи и LDAP Bind

Для подключения Blitz к ALD Pro используется метод LDAP Bind с сервисной учётной записью, которая имеет права только на чтение.

2.1 Создание сервисной учётной записи

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
```

, 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
```

2.2 Настройка LDAP Bind

- Протокол: **LDAPS** (порт 636)
- Тип сервера: 389 Directory Server
- Адрес: FQDN контроллера домена ALD Pro
- Base DN: `dc=ald,dc=company,dc=lan`
- Bind DN: **uid=ldap-bind,cn=sysaccounts,cn=etc,dc=ald,dc=company,dc=lan**

2.3 Рекомендуемые параметры LDAP

LDAP-параметр	Значение	Описание
Filter Disabled	(!(nsAccountLock=TRUE))	Исключение заблокированных учётных записей

Filter Login	(objectClass=inetOrgPerson)	Фильтр для определения учётных записей пользователя
Filter Group	(objectClass=groupofnames)	Фильтр для определения LDAP-групп
Group Member	member	Атрибут, определяющий состав группы
Member Of	memberOf	Атрибут групп, в которых состоит пользователь
Login	uid	Логин пользователя
Display Name	displayName	Отображаемое полное имя пользователя
First Name	givenName	Имя пользователя
Last Name	sn	Фамилия пользователя
Middle Name	rbtamiddlename	Отчество (специфично для ALD Pro)
Email	mail	Электронная почта пользователя
Mobile Phone	mobile	Мобильный телефон
Work Phone	telephoneNumber	Рабочий телефон
Home Phone	employeeNumber	Внутренний/добавочный номер

2.4 Настройка на стороне Blitz

После создания учетной записи подключите ALD Pro как LDAP-источник в Blitz:

- Инструкция по подключению каталога: https://docs.identityblitz.ru/latest/admin-guide/storage.html#storage
- Инструкция по аутентификации по логину и паролю: https://docs.identityblitz.ru/latest/admin-guide/auth-login.html

3 Настройка SSO

Для реализации SSO используется Kerberos.

3.1 Подготовка

Создание keytab-файла

> Важно: шаги, описанные в пункте **3.**, необходимо выполнять, только если сервер ещё не добавлен в домен ALD Pro. Если узел уже существует, переходите к следующему шагу.

1. Получите Kerberos-билет администратора домена, выполнив команду в терминале:

```
kinit admin
```

, где **admin** - имя доменного администратора.

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

```
IP_ADDRESS=10.10.10.10
HOSTNAME=service.ald.company.lan
DOMAIN_CONTROLLER=dc-1.ald.company.lan
```

, где:

- **IP_ADDRESS** - IP-адрес сервера службы;
- **HOSTNAME** - Полное доменное имя сервера;
- **DOMAIN_CONTROLLER** - FQDN контроллера домена ALD Pro.

3. Если сервер ещё не добавлен в домен, создайте запись узла с помощью:

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

4. Добавьте сервисную службу (SPN):

```
sudo ipa service-add service/$HOSTNAME
```

, где **service** - это тип службы (service principal), который нужно заменить на конкретный сервис, который вы хотите зарегистрировать, существуют стандартные типы сервисов, такие как host, http, ldap, postgres, но это не полный список, можно использовать и другие сервисы в зависимости от задач и возможностей клиента, создаваемый принципал будет использоваться вашим сервисом для аутентификации в домене Kerberos.

5. Сгенерируйте keytab-файл:

```
sudo ipa-getkeytab -s $DOMAIN_CONTROLLER -p service/$HOSTNAME -k service.keytab
```

3.2 Настройка SSO в Blitz

1. Загрузите keytab-файл в систему аутентификации Blitz.
2. Включите Kerberos SSO.
3. После этого пользователи домена ALD Pro смогут проходить аутентификацию в Blitz автоматически без повторного ввода пароля.
4. Инструкция по настройке Kerberos в Blitz: https://docs.identityblitz.ru/latest/admin-guide/auth-os.html