Интеграция Zabbix со службой каталога ALD Pro

08/11/2025

Содержание

Zabbix — это универсальная система мониторинга для отслеживания состояния компонентов ИТ-инфраструктуры, которая собирает и анализирует данные, оповещая администраторов о любых отклонениях от нормы.

Интеграция сервера Zabbix со службой каталога ALD Pro обеспечит возможность аутентификации в веб-портале управления при помощи протоколов LDAP и Kerberos V5.

Пример установки Zabbix подробно описан на странице справочного центра Astra Linux https://wiki.astralinux.ru/pages/viewpage.action?pageId=38699775

1 Создание пользователей

При настройке интеграции как LDAP, так и Kerberos пользователи должны существовать в Zabbix, и только для созданных пользователей возможно установить эти типы аутентификации. На рисунке 1 показан пример созданного пользователя admin.

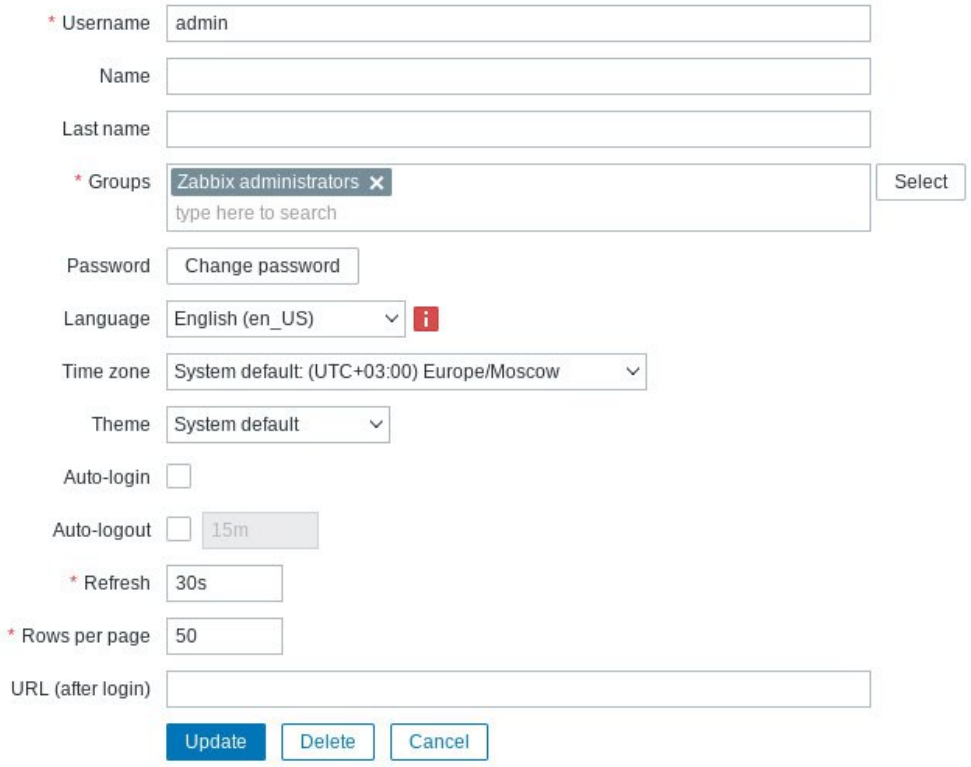

Рисунок 1 – Пользователь для доменной аутентификации

При создании пользователей нужно учитывать, чтобы их имена совпадали с именами, указанными в каталоге, и должны быть записаны в нижнем регистре.

Также для использования LDAP нужно создать сервисную учетную запись, от имени которой будет осуществляться поиск в каталоге. Для этого нужно выполнить следующее:

1. Создать файл с именем srvzabbix.update.
2. Внести в файл следующее содержимое:

```
dn: uid=zabbix,cn=sysaccounts,cn=etc,dc=test,dc=lan
add:objectclass: account
add:objectclass: simplesecurityobject
add:uid: zabbix
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 srvzabbix.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. После добавления учетной записи файл нужно удалить.

2 Интеграция LDAP

В разделе конфигурирования аутентификации нужно указать тип аутентификации LDAP, как показано на рисунке 2.

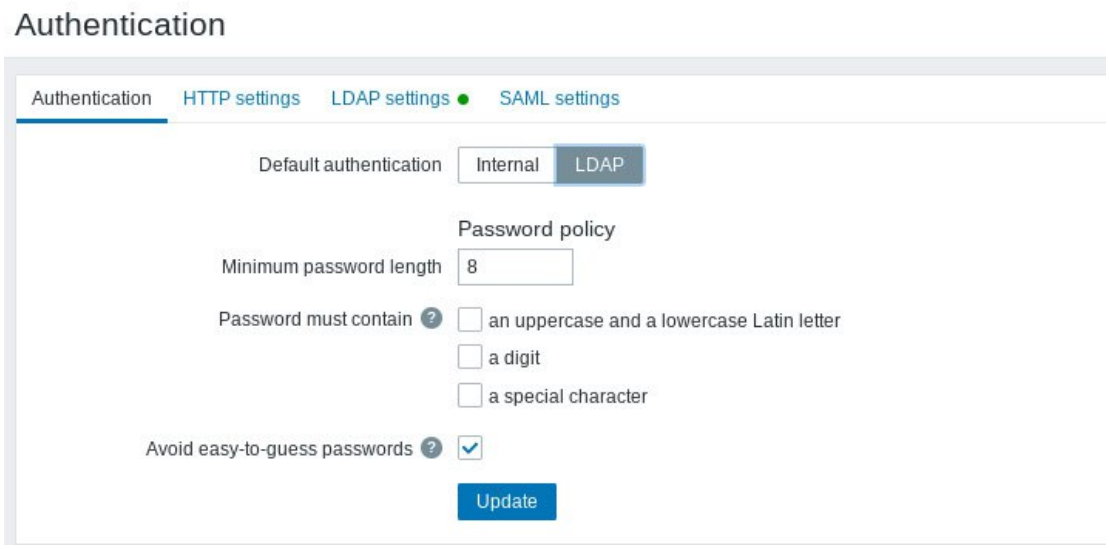

Рисунок 2 - Выбор типа аутентификации

Далее в настройках LDAP нужно указать следующую информацию:

- установить галочку в пункте **Enable LDAP authentication**;
- указать адрес контроллера домена в формате ldaps://<fqdn > (очень важно указывать с приставкой ldaps://, иначе передаваемые учетные данные будут не зашифрованы);
- указать порт соединения 636;
- **Base DN** - указать доменный суффикс;
- **Search attribute** указать **uid**;
- указать ранее созданную сервисную учетную запись;
- указать в поле **Login** и **User password** учетные данные пользовательской учетной записи для проверки работоспособности конфигурации и нажать **Update.**

Если данные указаны верно, то конфигурация обновится, и теперь можно будет заходить в интерфейс с учетной записи LDAP.

Далее нужно нажать **Update**. Список заполненных атрибутов показан на рисунке 3.

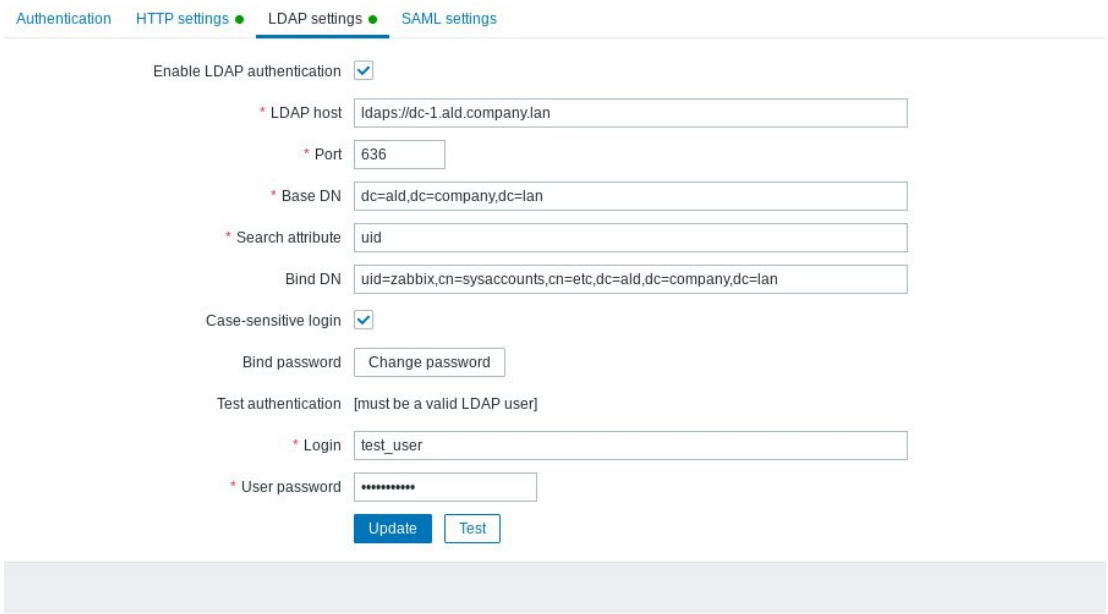

Рисунок 3 - Настройка параметров LDAP

Обратите внимание, что пользователь также должен существовать в Zabbix, однако его пароль из Zabbix не будет использоваться.

3 Интеграция Kerberos

Данная инструкция по настройке Kerberos предполагает, что сервер с установленным Zabbix введен в домен. Если это не так, то регистрация Kerberos-службы проводится самостоятельно и детали такой настройки не будут указаны.

Добавление службы проводится на сервере Zabbix от имени учетной записи с соответствующими правами.

Для работы протокола Kerberos необходимо зарегистрировать службу, сделать это можно командой

```
ipa service-add HTTP/zabbix.ald.company.lan@ALD.COMPANY.LAN
```

, где

- HTTP — класс службы;
- zabbix.ald.company.lan — FQDN сервера;
- ALD.COMPANY.LAN — зона Kerberos.

Выпустить keytab для созданной службы и выдать Apache права доступа.

```
pa-getkeytab -p HTTP/zabbix.ald.company.lan@ALD.COMPANY.LAN -k /etc/apache2/
http.keytab
chown www-data:www-data /etc/apache2/http.keytab
chmod 600 /etc/apache2/http.keytab
```

Установить модуль gssapi для apache

```
sudo apt install libapache2-mod-auth-gssapi
```

Далее в файле /etc/apache2/apache2.conf добавить следующие настройки:

```
<Location />
  AuthType GSSAPI
  AuthName "GSSAPI Single Sign On Login"
  GssapiCredStore keytab:/etc/apache2/http.keytab
  GssapiSSLonly On
  GssapiLocalName On
  require valid-user
</Location>
```

Перезагрузить службу apache командой

```
systemctl restart apache2
```

Перейти в веб-интерфейс и выбрать способ аутентификации Internal (рис. 4).

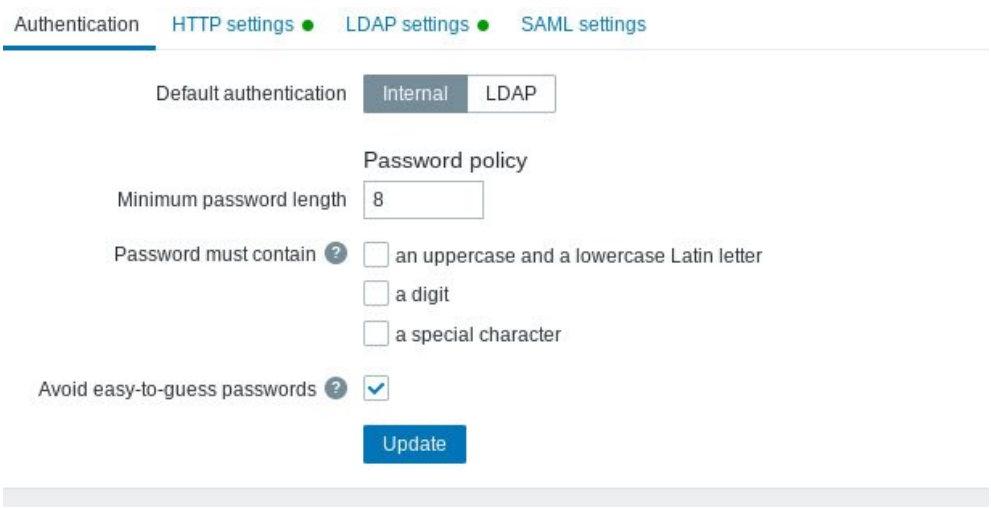

Рисунок 4 - Активация внутренней аутентификации

В **HTTP settings** поставить галочку в поле **Enable HTTP authentication** и в поле **Remove domain name** добавить используемый Kerberos Realm (рис.5).

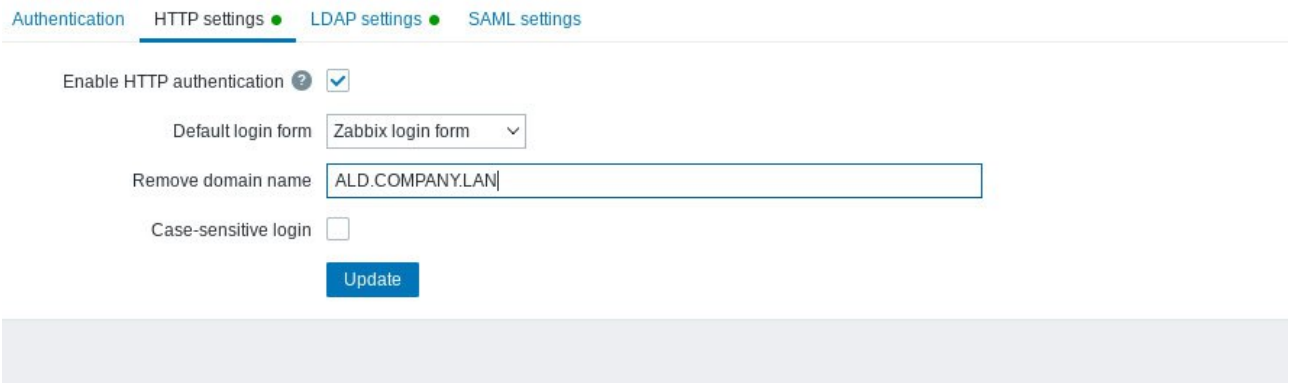

Рисунок 5 - Активация HTTP-аутентификации

На данном этапе настройка завершена. Для проверки в отдельной сессии открыть портал Zabbix, где нужно перейти по вкладке **Sign in with HTTP**, как показано на рисунке 6.

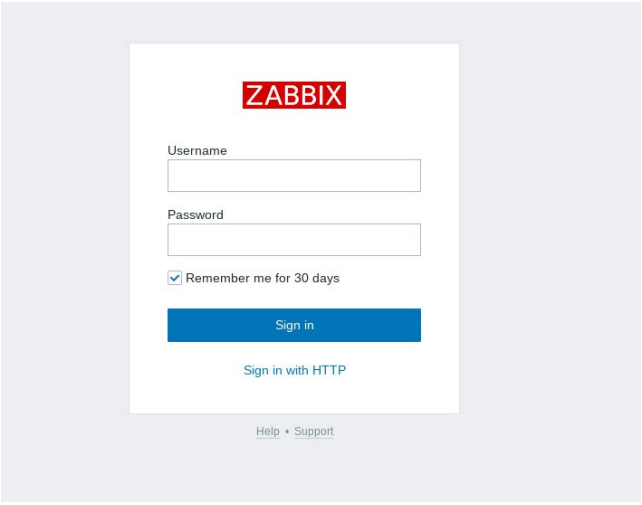

Рисунок 6 - Форма ввода учетных данных для входа в веб-портал Zabbix