

Интеграция в инфраструктуру

Авторизация через LDAP

Необходимо отредактировать файл `/home/devprom/docker/apache2/ldap.conf` (или `ldap.ssl.conf`, если планируете использовать HTTPS) и указать актуальные параметры подключения к вашему LDAP.

Затем, для подключения этой конфигурации, необходимо выполнить команды:

```
> docker exec -it alm-app bash
# a2dissite devprom
# a2ensite ldap
```

Если вы хотите использовать подключение к приложению по HTTPS, то используйте другой конфигурационный файл, который также нужно предварительно настроить

```
# a2ensite ldap.ssl
```

После переключения используемой конфигурации Apache, необходимо перезагрузить контейнер

```
> docker restart alm-app
```

Для аутентификации с использованием данного примера можно использовать следующие пары:

- nobel/password
- einstein/password

По умолчанию аутентификация работает по логину (атрибут `uid` в LDAP-каталоге). Чтобы реализовать аутентификацию по email, необходимо в конфигурационном файле `ldap.conf` (или `ldap.ssl.conf`) отредактировать параметр:

```
AuthLDAPURL ldap://ldap.forumsys.com:389/dc=example,dc=com?mail??(objectClass=*)
```

между знаками вопроса указать `mail` (атрибут, отвечающий за хранение Email) вместо `uid`.

Устранение возможных проблем

В случае возникновения проблем с авторизацией необходимо отредактировать конфигурационный файл веб-приложения Apache, например, `/etc/apache2/sites-available/ldap.conf` и установить повышенный уровень логирования: `LogLevel debug`

Затем, необходимо перезапустить контейнер `alm-app` или сервис `apache2`, авторизоваться повторно и изучить проблему в логе `/var/www/devprom/logs/error.log`, возможно некорректно заданы параметры подключения к LDAP-каталогу.

Поддержка нескольких LDAP-каталогов

При использовании нескольких LDAP-каталогов, в которых хранится аутентификационная информация, необходимо немного изменить настройку - добавить несколько конфигураций в секциях `AuthnProviderAlias`:

```
<AuthnProviderAlias ldap alpha>
  AuthLDAPURL "ldap://localhost:10389/ou=system?uid??(objectClass=*)"
  AuthLDAPBindDN "uid=admin,ou=system"
  AuthLDAPBindPassword "secret"
  AuthLDAPBindAuthoritative on
```

```
AuthLDAPRemoteUserIsDN on
LDAPReferrals Off
</AuthnProviderAlias>

<AuthnProviderAlias ldap beta>
AuthLDAPBindDN "cn=read-only-admin,dc=example,dc=com"
AuthLDAPBindPassword "password"
AuthLDAPURL "ldap://ldap.forumsys.com:389/dc=example,dc=com?uid??(objectClass=*)"
AuthLDAPBindAuthoritative on
AuthLDAPRemoteUserIsDN on
LDAPReferrals Off
</AuthnProviderAlias>
```

Включить использование дополнительной секции в директиве:

```
AuthFormProvider alpha beta anon
```

Использование NTLM, Kerberos

Для реализации встроенной аутентификации посредством протоколов NTLM или Kerberos выполните настройку Apache, как описано в этой [инструкции](#).

Для автоматической регистрации пользователей в файле `htdocs/settings_server.php` необходимо добавить константу:

```
define('AUTH_NTLM_CREATEVISITOR', true);
```

Загрузка пользователей из LDAP

При настроенном подключении к LDAP любой доменный пользователь может войти в приложение. Для отключения этой возможности, необходимо перейти в настройки приложения (Администрирование - Настройки - Приложение) и снять галочку "Создавать учетную запись для доменного пользователя".

Для импорта учетных записей пользователей, которые могут авторизовываться в системе по доменной учетке, необходимо перейти в модуль Администрирование - Пользователи - Импорт из LDAP.

Модуль представляет собой мастер, состоящий из нескольких шагов, и доступен в разделе "Администрирование", в меню "Настройки":

- На первом шаге необходимо указать параметры подключения к LDAP-серверу, тип LDAP-каталога и указать домен верхнего уровня, начиная с которого будет выполняться поиск объектов.
- На втором шаге необходимо уточнить метаданные, используемые для получения информации из каталога, название атрибута, отвечающего за имя учетной записи пользователя в домене, и название атрибута, в котором хранится адрес электронной почты. Также необходимо указать запрос поиска объектов в каталоге. По умолчанию подставляются значения, соответствующие выбранному типу LDAP-каталога.
- На третьем шаге отображается иерархия объектов, загруженных из каталога. Организационные единицы и группы отмечены иконками с изображением папки. Учетные записи отображаются без иконок. Вам необходимо отметить галочками те узлы, которые необходимо

импортировать, при этом, учетные записи будут импортированы как пользователи, а организационные единицы - как группы пользователей.

- На четвертом шаге отображается содержимое лога, сформированного в результате импорта данных из каталога. В логе отображается информация о том какие пользователи были созданы, какие обновлены, какие группы созданы и в какие группы были включены пользователи. Вы также можете отметить галочкой создание задачи по периодическому обновлению импортированных ранее учетных записей. При выполнении этой задачи будут обновляться адрес электронной почты, описание пользователя.

Использование SSL/TLS

При использовании протокола ldaps или поддержке команды START TLS необходимо учесть особенности работы с самоподписными сертификатами. Это можно сделать в настройках PHP, в файле /etc/php7.4/apache2/conf.d/devprom.ini необходимо добавить два параметра:

```
openssl.cafile=/var/www/devprom/devprom_ru.pem  
openssl.capath=/var/www/devprom
```

Тонкая настройка

Различные службы каталогов могут по-разному определять атрибуты, классы объектов и т.п.

Подобные специфические параметры определены в файлах настроек, соответствующих типу LDAP-каталога:

- Active Directory - htdocs/conf/plugins/ee/settings_ldap_ad.php
- OpenLDAP - htdocs/conf/plugins/ee/settings_ldap_openldap.php
- Apache DS - htdocs/conf/plugins/ee/settings_ldap_apacheds.php

```
// имя LDAP-сервера  
define(LDAP_SERVER, localhost:10389);  
  
// учетная запись, под которой выполняется подключение к LDAP-серверу  
define(LDAP_USERNAME, имя пользователя);  
  
// пароль учетной записи, для подключения к LDAP-серверу  
define(LDAP_PASSWORD, secret);  
  
// путь к домену верхнего уровня, с которого начинается построение дерева каталогов  
// компании company.ru  
define(LDAP_DOMAIN, OU=Users,DC=company,DC=ru);  
  
// запрос поиска объектов в каталоге, используемый для отображения состава каталога  
define(LDAP_ROOTQUERY, (|(objectClass=organizationalUnit)  
(objectClass=groupOfUniqueNames)(objectClass=person)(objectClass=group)));  
  
// запрос дочерних узлов по идентификатору родительского узла (%1)  
define(LDAP_TREEQUERY, (memberOf=%1));  
  
// атрибут определяющий название группы (организационной единицы)  
define(LDAP_GROUP_ATTR, cn);  
  
// атрибут определяющий название учетной записи пользователя (имя пользователя)  
define(LDAP_TITLE_ATTR, cn);  
  
// атрибут определяющий логин пользователя в Windows  
define(LDAP_LOGIN_ATTR, userprincipalname);  
  
// атрибут определяющий адрес электронной почты учетной записи  
define(LDAP_EMAIL_ATTR, mail);
```

```

// атрибут определяющий описание учетной записи пользователя
define(LDAP_DESCRIPTION_ATTR,title);

// название атрибута OU
define(LDAP_ATTR_OU,ou);

// название атрибута DN
define(LDAP_ATTR_DN,dn);

// название атрибута CN
define(LDAP_ATTR_CN,cn);

// название атрибута, определяющей вхождение объекта в другой объект
define(LDAP_ATTR_MEMBEROF,memberOf);

// список классов, соответствующих учетной записи пользователя
define(LDAP_CLASS_OP,organizationalPerson,person);

// список классов, соответствующих организационной единице (группе)
define(LDAP_CLASS_OU,organizationalUnit,groupOfUniqueNames,group);

```

Журнал подключений к LDAP

По умолчанию, лог-файл с информацией о подключении к LDAP-серверу расположен по пути `/var/www/devprom/logs/ldap.log`

В файле `htdocs/conf/logger.xml` прописан путь к логу подключений к LDAP-серверу. При необходимости вы можете его использовать для выявления проблем при импорте объектов из службы каталогов.

Авторизация через SSO (OpenID, OAuth)

Выполните установку необходимых модулей Apache:

```
$ sudo apt-get install libapache2-mod-auth-openidc
```

Включите использование модуля:

```
$ sudo a2enmod auth_openidc
```

В файле настройке сайта добавьте следующие строки:

```

...
LoadModule auth_openidc_module modules/mod_auth_openidc.so

<VirtualHost *:80>
...

    OIDCClaimPrefix "OIDC-"
    OIDCResponseType "id_token"
    OIDCScope "openid email"
    OIDCProviderMetadataURL "..."/>

```

```
</LocationMatch>  
</VirtualHost>
```

Пример заполнения параметров для аутентификации через Gmail

OIDCProviderMetadataURL	https://accounts.google.com/.well-known/openid-configuration
OIDCClientID	ClientID можно получить по ссылке https://console.cloud.google.com/apis/credentials для зарегистрированного приложения, где в качестве RedirectURI необходимо прописать путь к приложению <a href="http://<devprom-alm-server>/openid/auth">http://<devprom-alm-server>/openid/auth
OIDCClientSecret	ClientSecret можно получить вместе с ClientID

Дополнительные настройки

В файле `htdocs/settings_server.php` вы можете добавить следующие константы, чтобы настроить работу аутентификации через SSO-сервер.

<code>define('AUTH_OPENID_USED', true);</code>	Отобразить кнопку SSO на странице авторизации для входа через SSO-сервер.
<code>define('AUTH_OPENID_ONLY', true);</code>	Использовать только аутентификацию через SSO, без возможности аутентифицироваться по паре логин/пароль.
<code>define('AUTH_OPENID_CREATE_VISITOR', true);</code>	Автоматически создавать учетную запись для посетителя, успешно аутентифицировавшегося через SSO-сервер.

Пример настройки Keycloak

Настройки клиента Test

KEYCLOAK Admin

Master

Configure

- Realm Settings
- Clients
- Client Scopes
- Roles
- Identity Providers
- User Federation
- Authentication

Manage

- Groups
- Users
- Sessions
- Events
- Import
- Export

Clients > test

Test

Settings | Credentials | Roles | Client Scopes | Mappers | Scope | Revocation | Sessions | Offline Access | Clustering | Installation

Client ID: test

Name:

Description:

Enabled:

Always Display in Console:

Consent Required:

Login Theme:

Client Protocol: openid-connect

Access Type: confidential

Standard Flow Enabled:

Implicit Flow Enabled:

Direct Access Grants Enabled:

Service Accounts Enabled:

Authorization Enabled:

Root URL:

Valid Redirect URIs:

Base URL:

Admin URL:

Web Origins:

Backchannel Logout URL:

Backchannel Logout Session Required:

Backchannel Logout Revoke Offline Sessions:

Fine Grain OpenID Connect Configuration

Access Token Signature Algorithm:

ID Token Signature Algorithm:

ID Token Encryption Key Management Algorithm:

ID Token Encryption Content Encryption Algorithm:

User Info Signed Response Algorithm: unsigned

Request Object Signature Algorithm: any

Request Object Required: not required

Valid Request URIs:

OpenID Connect Compatibility Modes

Exclude Session State From Authentication Response:

Use Refresh Tokens For Client Credentials Grant:

Advanced Settings

Access Token Lifespan: Minutes

Client Session Idle: Minutes

Client Session Max: Minutes

Client Offline Session Idle: Minutes

Client Offline Session Max: Minutes

OAuth 2.0 Mutual TLS Certificate Bound Access Tokens Enabled:

Proof Key for Code Exchange Code Challenge Method:

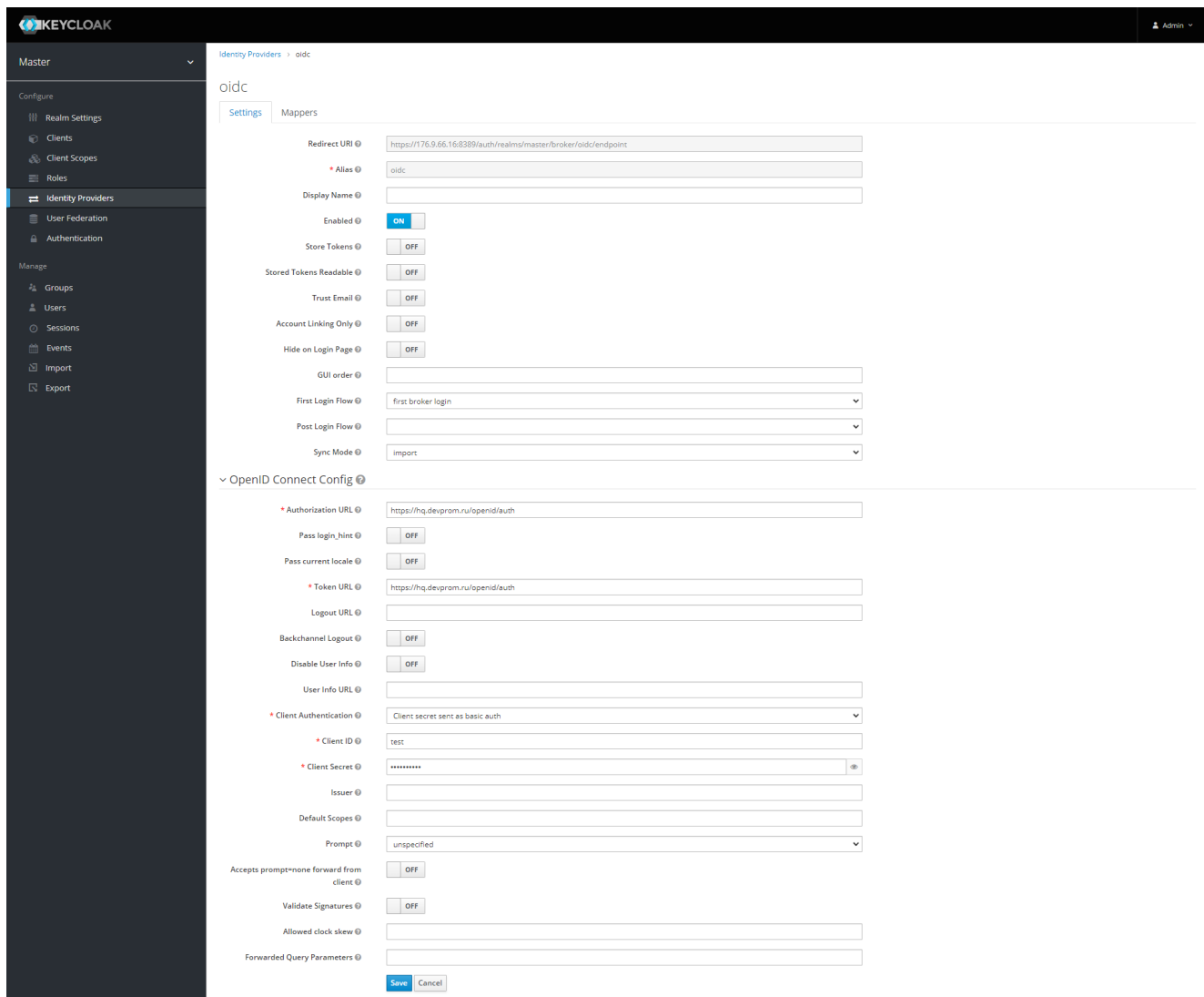
Authentication Flow Overrides

Browser Flow:

Direct Grant Flow:

Save Cancel

Настройки Identity Provider



Настройки Apache

```
...
OIDCClaimPrefix "OIDC-"
OIDCResponseType "code"
OIDCScope "openid email"
OIDCProviderMetadataURL
"https://176.9.66.16:8389/auth/realms/master/.well-known/openid-configuration"
OIDCClientID "test"
OIDCClientSecret "*****"
OIDCRedirectURI "https://hq.devprom.ru/openid/auth"
OIDCSSLValidateServer "Off"
OIDCCryptoPassphrase openstack
...
```

Подключение S3-хранилища

По умолчанию пользовательские файлы (аттачменты) хранятся на файловой системе сервера, в отдельном каталоге, обычно `/var/www/devprom/files`

Вы можете использовать корпоративное или облачное S3-хранилище, для хранения пользовательских файлов.

Для подключения S3-хранилища необходимо:

1. Создать бакет для хранения пользовательских файлов ALM
2. Настроить ALM для использования S3, как в примере далее

В файле `/var/www/devprom/htdocs/settings_server.php` необходимо прописать следующие константы:

```
define('FILE_STORAGE_TYPE', 'STORAGE_S3');
define('FILE_STORAGE_ENDPOINT', 'http://minio:9000');
define('FILE_STORAGE_BUCKET', 'bucket');
define('FILE_STORAGE_LOGIN', 'devprom');
define('FILE_STORAGE_PASSWORD', 'devprom_pass');
putenv('AWS_SUPPRESS_PHP_DEPRECATION_WARNING=true');
```

После внесения изменений необходимо нажать кнопку "Очистить кеш" в разделе Администрирование - Настройки - Приложение.

Подключение сборочного сервера

Если сборка приложения и выполнение модульных или автоматических тестов у вас автоматизирована при помощи сборочного сервера ("сборщика"), то вы можете настроить интеграцию с целью:

- автоматического добавления сборки в список сборок Devprom
- публикации статуса сборки: в работе, готова, сломана, развернута и т.п.
- публикации отчетов от средств автоматизированного тестирования

Интеграция возможна с любым сервером сборки, например, Jenkins или TeamCity посредством Devprom REST API.

Создание сборки

Перейдите в модуль Сборки и откройте подсказку снизу, на ней приведен пример выполнения команды сURL, которая создает сборку, например:

```
curl -X POST -H "Devprom-Auth-Key: 714adb764994a678ab31a3e52d51c200" \
      -H "Content-Type:application/json" https://uat.myaln.ru/pm/demo/api/v1/builds \
      -d '{"Caption": "%build.number%", "BuildRevision": {"Version": "%build.vcs.number %"}}, "State": "inprogress"}
```

В тело запроса (текст после ключа `d`) вы можете вставить любые доступные данные: номер сборки, коммита, описание, логи, переменные окружения и т.п., все что предоставляет конкретный сборщик.

Изменение статуса сборки

Чтобы сообщить вашей команде о статусе сборки, вы можете обновить статус на соответствующем шаге процесса сборки. Возможны следующие значения статусов:

- inprogress
- success
- failed
- deployed

Например, команда для изменения статуса сборки может иметь вид:

```
curl -X POST -H "Devprom-Auth-Key: 714adb764994a678ab31a3e52d51c200" \
```

```
-H "Content-Type:application/json" https://uat.myalm.ru/pm/demo/api/v1/builds \
-d '{"Caption": "%build.number%", "State": "success"}'
```

Публикация отчетов о тестировании

В процессе выполнения тестов образуются отчеты (файлы), которые вы можете импортировать в приложение, чтобы показать команде качество сборки и последние результаты тестирования.

Откройте модуль "Запуски тестов", откройте подсказку снизу списка и скопируйте команду, публикующую отчет по тестированию в Devprom, например,

```
curl -X POST -H "Devprom-Auth-Key: 714adb764994a678ab31a3e52d51c200" \
  --data-binary @testng-results.xml \
  "https://uat.myalm.ru/pm/demo/module/testing/convert?version=%build.number
  %&environment=<название-окружения>"
```

В ключе --data-binary необходимо указать путь к файлу с результатами тестирования. Приложение поддерживает импорт отчетов NUnit, TestNG.

Подключение репозитория исходного кода TFS

Для подключения Devprom к репозиторию исходного кода TFS необходимо предварительно выполнить следующие шаги:

1. Развернуть на сервере свежую версию JRE (или JDK)
2. Скачать компонент Visual Studio Team Everywhere по ссылке <http://devprom.ru/download> и распаковать архив. Убедитесь, что у приложения apache есть доступ на чтение и запись в каталог и все его содержимое.
3. Открыть на редактирование файл htdocs/settings_server.php и добавить определение константы, указывающее на расположение компонента

```
define( SERVER_TFS_CLI_PATH, /var/www/devprom/tools/tee-clc );
```

Подключение к домену организации

Если вы хотите использовать "облачный" вариант Devprom ALM, но разместить его в домене вашей организации, например, devprom.company.ru, то нужно выполнить следующие шаги.

1. Вам необходимо отредактировать настройки домена вашей компании и добавить там CNAME-запись, ссылающуюся на адрес вида <аккаунт>.myalm.ru
2. Сообщить нам в поддержку новый адрес сервиса и передать данные сертификата (приватный ключ и родительские сертификаты), для организации https-подключения.
3. Новый адрес сервиса необходимо прописать в настройках приложения, в административном разделе.

Отправка почты через NTLM

Если необходимо отправлять почту с использованием NTLM-аутентификации, то необходимо настроить приложение следующим образом:

1. Убедиться, что установлено расширение PHP с названием bcmath, проверьте это выполнив команду `apt-get install php-bcmath`

2. В файле `htdocs/co/bundles/Devprom/ApplicationBundle/Resources/config/settings.yml` задать параметр `mailer_auth_mode` как в примере ниже:

```
parameters:
  mailer_encryption: null
  mailer_host: 127.0.0.1
  mailer_port: 25
  mailer_user: ''
  mailer_password: ''
  mailer_auth_mode: ntlm
```