Инструкция к установке

1.1.Подготовка виртуалки.

 Зайти в консоль под рутом - sudo bash

*Необходимо ввести пароль root пользователя*

Скопировать архив пакетов на сервер

*Предположим что в папку /home/test*

Установить пакет разархиватор - apt-get install unzip unrar zip rar

*Вопрос: Do you want to continue? [Y/n]*

*Действие: Вводим “y” и жмем Enter*

Распаковать архив - unzip /home/test/DOC\_PACK.zip -d /tmp

**В 14.04 у пользователя www-data нету шела. Даем**

chsh www-data -s /bin/bash

1.2 Добавляем репозиторий для постгреса

|  |
| --- |
| sudo nano /etc/apt/sources.list.d/pgdg.list |

1. 3 Прописываем в него  ( для 14.04 использовать "trusty" вместо "precise")

|  |
| --- |
| deb http://apt.postgresql.org/pub/repos/apt/ precise-pgdg main |

1.4 Добаляем публичный ключ

|  |
| --- |
| wget --quiet -O - https://www.postgresql.org/media/keys/ACCC4CF8.asc | \  sudo apt-key add - |

1.5 Обновление

sudo apt-get update -o Dir::Etc::sourcelist="sources.list.d/pgdg.list" -o Dir::Etc::sourceparts="-" -o APT::Get::List-Cleanup="0"

1.6 Установка.

sudo apt-get install postgresql-9.4

1.7 Редактируем файл /etc/postgresql/9.4/main/postgresql.conf

|  |
| --- |
| listen\_addresses = '\*' |

 Редактируем файл /etc/postgresql/9.4/main/pg\_hba.conf

|  |
| --- |
| # IPv4 local connections:       host    all         all         127.0.0.1/32          md5       host    all         all         0.0.0.0/0           trust |

Перезапуск Postgres

|  |
| --- |
| sudo service postgresql restart |

Конфигурируем БД (бд. роли, схемы) - dpkg -i /tmp/kck-res-db-config\_amd64.deb

########### Db config for PGU ##########

Which setting you wish to reconfigure?

1. Password for liferay\_user abcd1234

2. Password for res res

3. Password for siu siu

4. Password for mvv mvv

0. None

########################################

Please select:

*Действие: - вводим “0“ и жмем Enter.*

sudo -u postgres psql -c "ALTER USER postgres PASSWORD 'postgres';"

# Установка OpenLdap

Устанавливаем пакет

 aptitude purge -y slapd; rm -rf /var/lib/ldap/\* /etc/ldap/\*; aptitude install -y slapd; dpkg-reconfigure slapd; aptitude install ldap-utils; dpkg -i /tmp/kck-siu-openldap\_amd64.deb; dpkg -i /tmp/kck-backup\_amd64.deb

*Вопрос: If you enable this option, no initial configuration or database will be created for you.‚*

 *Omit OpenLDAP server configuration?*

*Действие: жмем Enter*

*Вопрос The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create в”‚в”‚ the directory with 'dc=foo, dc=example, dc=org' as base DN. DNS domain name: foo.examle.org*

*Действие: жмем Enter*

*Вопрос Please enter the name of the organization to use in the base DN of your LDAP directory. Organization name: foo.examle.org*

*Действие: жмем Enter*

*Вопрос Please enter the password for the admin entry in your LDAP directory.*

*Administrator password:*

*Действие: Вводим “abcd1234” и жмем Enter*

*Вопрос Please enter the admin password for your LDAP directory again to verify that you have typed it correctly.*

*Cofirm password:*

*Действие: Вводим “abcd1234” и жмем Enter*

*Вопрос The HDB backend is recommended. HDB and BDB use similar storage formats, but HDB adds support for subtree renames. Both в”в”‚ support the same configuration options. In either case, you should review the resulting database configuration for your needs. See /usr/share/doc/slapd/README.DB\_CONFIG.gz for more details. Database backend to use: BDB*

 *HDB (выделено)*

*Действие: жмем Enter*

*Вопрос Do you want the database to be removed when slapd is purged?*

*<Yes> <No> (выделено)*

*Действие: жмем Enter*

*Вопрос There are still files in /var/lib/ldap which will probably break the configuration process. If you enable this option, the maintainer scripts will move the old database files out of the way before creating a new database. Move old database?*

 *<Yes>(выделено) <No>*

*Действие: жмем Enter*

*Вопрос The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and users should upgrade to LDAPv3. If you have old programs which can't use LDAPv3, you should select this option and 'allow bind\_v2' will be added to your slapd.conf ‚ file.*

 *<Yes> <No> (выделено)*

*Действие: жмем Enter*

Which of settings needs to be reconfigured?

1. baseDN:      dc=domain,dc=ru ваше доменное имя

2. login:       cn=admin

3. password:        abcd1234

0. None

Please select:

# Установка Nginx

# Может понадобиться ibssl0.9.8 (apt-get install ibssl0.9.8 )

Установка из пакета - dpkg -i /tmp/kck-nginx\_amd64.deb

Создаем файл настроек

nano /opt/nginx/conf/sites-available/en\_default

Заменить ХОСТ на хостнейм

*server {*

 *listen 80;*

 *server\_name ХОСТ С ПОРТАЛОМ;*

 *location / {*

 *proxy\_set\_header Host $host;*

 *proxy\_set\_header X-Real-IP $remote\_addr;*

 *rewrite ^(.\*)$ https://{ХОСТ С ПОРТАЛОМ}$1 permanent;*

 *}*

 *}*

 *server {*

 *listen 443;*

 *server\_name localhost;*

 *ssl on;*

 *ssl\_certificate /opt/nginx/ssl/cert.pem;*

 *ssl\_certificate\_key /opt/nginx/ssl/cert.key;*

 *ssl\_session\_timeout 5m;*

 *ssl\_protocols SSLv2 SSLv3 TLSv1;*

 *ssl\_ciphers ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP;*

 *location /cas/ {*

 *proxy\_pass https://{ХОСТ ДЛЯ CAS}:8443;*

 *proxy\_set\_header Host $host;*

 *proxy\_set\_header X-Real-IP $remote\_addr;*

 *proxy\_redirect off;*

 *}*

 *location / {*

 *proxy\_pass https://{ХОСТ С ПОРТАЛОМ}:8181;*

 *proxy\_set\_header Host $host;*

 *proxy\_set\_header X-Real-IP $remote\_addr;*

 *proxy\_redirect off;*

 *client\_max\_body\_size 50M;*

 *}*

*}*

*Действие: нажимаем ctrl+x*

*Вопрос: Save modified buffers [Y/n]*

*Действие: Вводим “y” и жмем Enter*

Подготовка сертификата

* + Идём в папку cd /opt/nginx/ssl/
	+ Создаем сертификат

sudo openssl req -new -x509 -days 3650 -nodes -out cert.pem -keyout cert.key

*\*в процессе конфигурации сгенерированный сертификат будет импортирован в хранилища glassfish и java (поэтому если glassfish и tomcat  с cas находятся на той же машине его можно не импортировать в соответствующих пунктах инструкций)*

*\*Во время создания сертификата при запросе страны, организации и т.д. вводить данные не обязательно, но при запросе имени необходимо ввести полное доменное имя сервера Common Name (e.g. server FQDN or YOUR name) []:NGINX-SERVER.dv.kck.ru т.е. в конечном итоге должно быть так CN=NGINX-SERVER.dv.kck.ru (остальное не важно).*

Перезагружаем nginx sudo service kck-nginx restart

# Установка CAS

1. Устанавливаем пакет kck-siu-cas - dpkg -i /tmp/kck-jdk7\_7.55-4\_amd64.deb; dpkg -i /tmp/kck-jdk-7.55\_7.55-2\_amd64.deb; dpkg -i /tmp/kck-tomcat-7\_7.0.33-95\_amd64.deb; dpkg -i /tmp/kck-tmof-fix\_1.0-8\_amd64.deb; dpkg -i /tmp/kck-siu-cas\_amd64.deb
2. В появившемся меню прописываем настройки:

*1. serverUrl:        localhost:389*

*2. baseDN:      dc=kck,dc=ru ваше доменное имя*

*3. login:        cn=admin*

*4. password:        abcd1234*

*5. filter:        cn=%u*

*6. identifier:        $CN*

*7. trustedPattern:    ^.\*CN=dv.\**

*8. People:        ou=people*

*9. ESB operators:    cn=SPU\_ESB\_OPERATORS*

*10. ESIA enabled:    false*

*\*serverUrl - хост и порт, где установлен LDAP*

*\*people - название ветки в LDAP (+ baseDN), где будут лежать пользователи*

*\*ESB operators - название* *группы в LDAP (+ baseDN), для пользователей с ролью "ESB Оператор".*

*Вопрос* *0. Done configuring settings*

*s. Skip configuration*

*Действие: вводим “0”, жмем Enter*

NGINX-SERVER будет обращаться к CAS по https, что необходимо для корректной работы SSO, поэтому настроим HTTPS на Tomcat сервере:

* cоздаем самоподписанный сертификат c алиасом tomcat. CN (firstName) в конечном итоге должен быть равен полному доменному имени сервера tomcat. Пароль на хранилище сертификатов 'changeit' –

sudo /opt/jdk/bin/keytool -genkey -alias siu-cas -keypass changeit -keyalg RSA -keystore /opt/tomcat/conf/tomcat.jks -validity 730

*Вопрос: Enter keystore password*

*Действие: вводим “changeit”, жмем Enter*

*Вопрос: What is your first and last name?*

 *[Unknown]:*

*Действие: вводим hostname ,остальное можно пропустить жмем Enter и соглашаемся*

.   Добавляем сертификат nginx в список доверенных на Tomcat/ Для Tomcat Application сервера этот сертификат необходимо импортировать в keystore JAVA под которой исполняется Tomcatи проимпортируем сертификат. Пароль хранилища по умолчанию "changeit".

|  |
| --- |
| sudo /opt/jdk/bin/keytool -import -alias siu-nginx -file /opt/nginx/ssl/cert.pem -keystore /opt/jdk/jre/lib/security/cacerts |

Перезапускаем сервер - sudo /etc/init.d/kck-tomcat stop && sudo /etc/init.d/kck-tomcat start

# Установка Liferay

1. Установка Liferay 6.2 - dpkg -i /tmp/kck-liferay-6.2\_6.2-22\_amd64.deb

*Вопрос: Which of settings needs to be reconfigured?*

*1. DB Host: localhost*

*2. DB Name: liferay\_kck*

*3. DB User: liferay\_user*

*4. DB Pass: abcd1234*

*0. None
Действие: Если все правильно вводим «0», и жмем Enter
Если нужно поменять параметр, вводим соответствующий цифровой код и вносим изменения*

Устанавливаем сертификат - /opt/jdk/bin/keytool -import -alias siu-nginx -file /opt/nginx/ssl/cert.pem -keystore /opt/liferay/glassfish/domains/domain1/config/cacerts.jks

*Вопрос: Enter keystore password:*

*Действие: вводим “changeit”, жмем Enter*

*Вопрос: Trust this certificate? [no]:*

*Действие: вводим “y”, жмем Enter*

1. Стартуем портал - sudo service kck-liferay start
2. Заходим на портал <liferay server ip:8080>и авторизиуемся test/abcd1234
3. Переходим Управление (Admin) -> Панель управления (Control Panel) -> Конфигурация (Configuration)-> Настройки (Portal Settings)
	* Общий (General)

*Домашний URL (Home URL) -> /c/portal/login*

*Начальная страница после авторизации (Default Landing Page) -> /web/guest/*

* + Аутентификация (Authentification)

*Как пользователи будут аутентифицироваться? (How do users authenticate) -> По экранному имени (By screen name)*      - Ldap ->
*Включен (EnabledRequired)*

*Импорт включен (Import Enabled) Включен импорт при запуске (Import on Startup Enabled)* Добавить (Add new) -> Прописать настройки подключения к Лдапу

*\*Прописать настройки LDAP*

      - Cas ->
*EnabledImport from LDAP*
*Login URL* -> [https://{ХОСТ С NGINX}/cas/login?locale=ru](https://vm-bpm-d2-dev.dv.kck.ru/cas/login)
*Logout URL* -> [https://](https://vm-bpm-d2-dev.dv.kck.ru/cas/logout?url=https://vm-bpm-d2-dev.dv.kck.ru/c/portal/login)[{ХОСТ С NGINX}](https://vm-bpm-d2-dev.dv.kck.ru/cas/login)[/cas/logout?url=https://](https://vm-bpm-d2-dev.dv.kck.ru/cas/logout?url=https://vm-bpm-d2-dev.dv.kck.ru/c/portal/login)[{ХОСТ С NGINX}](https://vm-bpm-d2-dev.dv.kck.ru/cas/login)[/c/portal/login&service=https*://{*ХОСТ С NGINX}/c/portal/login](https://vm-bpm-d2-dev.dv.kck.ru/cas/logout?url=https://vm-bpm-d2-dev.dv.kck.ru/c/portal/login)

1. Конфигурируем Glassfish - dpkg -i /tmp/kck-res-gf-config\_amd64.deb
2. Рестарт портала - sudo service kck-liferay stop && sudo service kck-liferay start
3. Устанавливаем тему - dpkg -i /tmp/kck-res-main-theme\_amd64.deb
4. Добавляем Файловый сервер - dpkg -i /tmp/kck-fs-web-server\_amd64.deb
5. Устанавливаем почтовый сервер - dpkg -i /tmp/kck-mm-mail-server\_amd64.deb
6. Устанавливаем  Журнал событий - dpkg -i /tmp/kck-el-web-server\_amd64.deb
7. Устанавливаем Организации и персонал - dpkg -i /tmp/kck-oip-all-portlets\_amd64.deb; dpkg -i /tmp/kck-oip-personal-rest\_amd64.deb
8. Устанавливаем СИУ-МВВ 2 - dpkg -i /tmp/kck-res-siu-server\_amd64.deb; dpkg -i /tmp/kck-res-mvv-server\_amd64.deb; dpkg -i /tmp/kck-res-calendar-server\_amd64.deb; dpkg -i /tmp/kck-res-calendar-management\_amd64.deb; dpkg -i /tmp/kck-res-mvv-control\_amd64.deb; dpkg -i /tmp/kck-res-mvv-drafts\_amd64.deb; dpkg -i /tmp/kck-res-mvv-events-logger\_amd64.deb; dpkg -i /tmp/kck-res-mvv-execution\_amd64.deb; dpkg -i /tmp/kck-res-mvv-liferay-settings\_amd64.deb; dpkg -i /tmp/kck-res-mvv-mnemonics\_amd64.deb; dpkg -i /tmp/kck-res-mvv-reference-book\_amd64.deb; dpkg -i /tmp/kck-res-mvv-rights\_amd64.deb; dpkg -i /tmp/kck-res-mvv-start\_amd64.deb; dpkg -i /tmp/kck-res-mvv-statistic\_amd64.deb; dpkg -i /tmp/kck-res-mvv-tc-library\_amd64.deb; dpkg -i /tmp/kck-res-mvv-wd-management\_amd64.deb; dpkg -i /tmp/kck-res-siu-completed\_amd64.deb; dpkg -i /tmp/kck-res-siu-control\_amd64.deb; dpkg -i /tmp/kck-res-siu-drafts\_amd64.deb; dpkg -i /tmp/kck-res-siu-events-logger\_amd64.deb; dpkg -i /tmp/kck-res-siu-liferay-settings\_amd64.deb; dpkg -i /tmp/kck-res-siu-myoffice-vlkz\_amd64.deb; dpkg -i /tmp/kck-res-siu-operating\_amd64.deb; dpkg -i /tmp/kck-res-siu-reference-book\_amd64.deb; dpkg -i /tmp/kck-res-siu-start\_amd64.deb; dpkg -i /tmp/kck-res-siu-statistic\_amd64.deb; dpkg -i /tmp/kck-res-siu-tasks\_amd64.deb; dpkg -i /tmp/kck-res-siu-tc-library\_amd64.deb; dpkg -i /tmp/kck-res-siu-wd-management\_amd64.deb; dpkg -i /tmp/kck-res-siu-rights\_amd64.deb; dpkg -i /tmp/kck-res-all-portlets\_amd64.deb
9. Устанавливаем портлеты шины - dpkg -i /tmp/kck-esbclient-current-ds-keys\_amd64.deb; dpkg -i /tmp/kck-esbclient-external-esb-requests\_amd64.deb; dpkg -i /tmp/kck-esbclient-external-esb-services\_amd64.deb; dpkg -i /tmp/kck-esbclient-internal-esb-requests\_amd64.deb; dpkg -i /tmp/kck-esbclient-internal-esb-services\_amd64.deb; dpkg -i /tmp/kck-esbclient-all-portlets\_amd64.deb
10. Заходим на портал администратором и размещаем прямо на главной страничке портлет "МВВ - Настройка системы" -> обновляем страничку -> кликаем на "Перестроить меню"
11. Повторяем тоже самое для "СИУ- Настройка системы"
12. Если нужно работать с модулем "Организации и Персонал" - добавляем, через контроль управления, нужному оператору роль OP\_ADMINISTRATOR
13. Удаляем первую страничку с лайфрея куда мы складывали Настройки системы