СИГМА.ЦУС

Инструкция по установке СИГМА.ЦУС

1. Введение

Данная инструкция посвящена подготовке серверов на операционной системе Alt Linux с последующей инсталляцией ПО СИГМА.ЦУС.

Система может быть развернута на большом количестве вариантов конфигураций. В общем случае требуются следующие виртуальные или реальные машины, классифицированные по ролям:

1. Web-сервер (NGINX)
2. Сервер баз данных (MariaDB)
3. Сервер приложений (PHP-FPM)
4. Сервер – файловое хранилище (SSHFS)

Одним из самых простых вариантов развёртывания - может быть в рамках одного сервера или виртуальной машины:

Дополнительно могут быть развернуты сервера хранения бекап-данных, дополнительные сервера любой роли.

Для каждой машины необходимо указание фиксированного IP-адреса, а также создание комплекта авторизационных пар логин-пароль. В случае настройки на виртуальных машинах количество и качество подключенных виртуальных жестких дисков может отличаться и выбирается по соображениям целесообразности.

Любые перечисленные роли серверов могут быть совмещены в рамках одной виртуальной или реальной машины.

В следующих пунктах данного раздела приведена универсальная конфигурация машин, которая позволяет добиться высокой надежности и быстродействия, в частности, каждая из машин: web-сервер, сервер баз данных, сервер приложений – дуплицируется и размещается на разных реальных серверах для повышения надежности.

Сервер – файловое хранилище настраивается в соответствии с требованиями заказчика стандартными методами. Клиентская операционная система может быть любой по выбору заказчика. В случае если сервера приложений и сервер файлового

хранилища - разные, на файловом хранилище должно быть развернуто пространство для file sharing, протокол взаимодействия – SMB, NFS, sshfs.

Данная инструкция применима как к bare metal среде, в которой будет разворачиваться приложение, так и в виртуализированной среде.

2. Развертывание системы

Операционная система

Используемая система - ALT Server, необходимая версия соотносится с версией дистрибутива используемого в продуктивной среде. На момент последней правки, используется ALT Server 10.1.

Развертывание выполняется любым удобным способом, к примеру, из установочного образа в iso-файле, скачанного с https://getalt.org/en/alt-server в виде iso-образа полной редакции.

При установке используется следующая конфигурация:

- Язык – Русский;
- Раскладка клавиатуры – английская/русская;
- Часовой пояс – Москва;
- Конфигурация сети – статический IP адрес (DHCP при его наличии);
- Таблица разделов жесткого диска.

Разбивка носителей

Разбивку диска можно либо произвести заранее, либо воспользоваться установщиком.

Выбор виртуализации данных (RAID) зависит от объёма и количества дисков.

Назначение раздела	Точка монтирования	Объём	Расчет объёма	Комментарий
Хранение backup-копий	/backup	От 60 GB	Удвоенный минимальный объем /var	Необходим на сервере БД

Назначение раздела	Точка монтирования	Объём	Расчет объёма	Комментарий
Хранение основных файлов БД и логов	/var	От 30 GB	30 GB – на 3-5 лет работы при загрузке до 5000 активных объектов	Необходим на сервере БД
Основные системные файлы	/	От 10 GB	Оптимально 16 GB	Необходим на каждом сервере
Домашний каталог web	/home	От 10 GB	Оптимально 32 GB + необходимый размер хранилища файлов, если совмещен	Необходим на сервере приложений
Системный UEFI	---	От 512 MB	---	Необходим на каждом сервере
Раздел подкачки	---	Объём RAM	---	Необходим на каждом сервере при объеме памяти < 32 GB, в остальных случаях по желанию
Раздел хранения файлов пользователей	---	---	Объем файлов в перспективе 5 лет	---

Пользователи

В качестве пользователей в установщике создаются пользователь root и обычный пользователь с заданными им паролями. Рекомендуется сразу указать пароли со сложной комбинацией в целях защиты сервера.

Этап установки "5/12"

На данном этапе можно выбрать дополнительные компоненты для установки (например, графическое окружение), но в сценарии к данной документации был выбран профиль "Минимальная установка". Выбор данного профиля обусловлен схожестью со стандартной установкой Debian без графического окружения.

После установки ALT Linux необходимо произвести обновление системы от пользователя root:

```
apt-get update && apt-get -y dist-upgrade
```

Также необходимо установить пакет openssl и firewall UFW:

```
apt-get update && apt-get -y install openssl ufw
```

3. Настройка NGINX

На машинах ролей: web-сервере, сервере БД, сервере приложений, - разворачивается proxy web-сервер NGINX.

Установка NGINX:

```
apt-get install -y nginx
```

После установки скопируйте файлы fastcgi.conf, fastcgi_params, gzip.conf, block.conf в каталог /etc/nginx. Примеры конфигурацонных файлов находятся во вложении.

Также создайте один из конфигурационных файлов соответствующий роли машины и скопируйте его в каталог /etc/nginx/sites-available.d

В случае настройки отдельно стоящего web-сервера, особенно в ситуациях с диспетчеризацией запросов, необходимо скорректировать IP-адреса Upstream серверов приложений и критерии их выбора. По умолчанию система отправляет все запросы на первый сервер приложений, в случае его отключения – на второй. Это делается правкой скопированного конфигурационного файла – секции Upstream.

Создайте символьную ссылку на скопированный файл в каталоге /etc/nginx/sites-enabled.d, к примеру:

```
root@server:/etc/nginx/sites-enabled.d# ln -s ../sites-available.d/default
```

Далее необходимо запустить NGINX, включить его автозагрузку и проверить статус работы:

```
systemctl start nginx
systemctl enable nginx
systemctl status nginx
```

4. Настройка PHP

На машинах ролей: сервер БД, сервер приложений, - разворачивается PHP-FPM7.3.

Для установки PHP-FPM7.4 необходимо установить следующие пакеты:

```
apt-get install -y php7-zip php7-gd php7-pdo_mysql php7-mbstring php7-libs php7-mysqlnd php7-mysqlnd php7-opcache php7-fpm-fcgi php7-pdo php7-devel php7-redis php7-imagick php7-xmlreader php7-curl php7-pdo_odbc php7
```

Скопируйте конфигурационный файл PHP-FPM в каталог /etc/fpm7/php-fpm.d/, пример конфигурационного файла находится во вложении.

В конфигурационном файле выберите режим работы с дочерными процессами у PHP-FPM (https://www.php.net/manual/en/install.fpm.configuration.php). Если используется режим dynamic, то выставьте необходимое количество pm.max_children, pm.start_servers, pm.min_spare_servers, pm.max_spare_servers.

После включите PHP-FPM сервис, добавьте его в автозагрузку и проверьте стасус работы:

```
systemctl start php7-fpm
systemctl enable php7-fpm
systemctl status php7-fpm
```

Для хранения некритических бизнес-данных в ЦУС (например, сессий пользователей) используется NoSQL СУБД Redis.

Установка Redis:

```
apt install redis
```

Конфигурационный файл Redis расположен в /etc/redis/redis.conf

Определите прослушиваемый адрес Redis'ом в строке bind и пароль для аутентификации в requirepass.

Для установки пароля рекомендуется воспользоваться переводом произвольного текста в sha256 сумму следующей командой:

```
echo "text to sha256" | sha256sum
```

Установите полученное значение для директивы requirepass.

Перезапустите сервис после изменения конфигурационного файла:

```
systemctl restart redis
```

Модуль igbinary отсутствует в репозиториях ALT Linux. Его необходимо собрать.

Установливаем компилятор GCC и git:

```
apt install  gcc git
```

Клонируем исходный код:

```
git clone https://github.com/phadej/igbinary.git
```

Сборка:

```
1. phpize
2 ./configure CFLAGS="-O2 -g" --enable-igbinary
3. make
4. make test
5. make install
```

Скомпилированный файл кладём в /usr/lib64/php/7.4.33/extensions/

В директории /etc/php/7.4/cli/php.d создаём файл igbinary.ini со следующим содержанием:

```
[igbinary]
extension=igbinary.so
```

5. Установка первоначального дампа БД и создание пользователей

Создайте в MySQL трех пользователей с именами: buh, buh_users, buh_main с правами доступа "ALL PRIVILEGES".

Также создайте базы данных buh_main, buh_users и buh_tasks.

После создания баз данных нужно скопировать необходимые дампы баз данных и выполнить в директории их нахождения следующую команду для импорта, где параметр password - пароль, указанный для пользователя, root , а параметр database - имя импортируемой базы данных:

```
ls | while read i; do mysql -u root --password=password --database=databasename<$i;done
```

После выполните очистку истории команд bash для сокрытия пароля:

```
history -c
history -w
```

В таблице hosts базы buh_main необходимо изменить единственную запись на то доменное имя, которое будет использоваться для работы с системой. Без доменного имени система не сможет определить предпочитаемые настройки пользователей и не сможет работать (IP-адрес не подходит).

- buh_main - содержит в себе список всех клиентских БД и связи пользователей с ними;
- buh_users - содержит в себе список всех пользователей, данные входа и другую служебную информацию;
- buh_tasks - БД для модуля задачника (этот модуль работает для всех клиентских баз, то есть не зависит от клиентской БД, в которой сейчас находишься).

6. Подключение файлового сервера

Подключение осуществляется по SSHFS с использованием команды mount и файла /etc/fstab

Пример монтирования в /etc/fstab, где user@ip - пользователь и ip-адрес конечной точки монтирования, а /home/ext_files директория монтирования. Также используется SSH ключ для аутентификации.

```
user@ip:/home/ext_files /home/www/ext_files fuse.sshfs identityfile=/root/.ssh/id_rsa,defaults,allow_other,_netdev 0 0
```

7. Резервное копирование

Базы данных

Для примера на Production сервере ЦУС в CRON установлено следующее действие:

```
12 */2 * * * php /home/www/db_backup.php && rsync -avhrz --ignore-existing /backup/* backup@NAS2:/backup
```

Каждые 2 часа в 12 минут происходит вызов скрипта db_backup.php для резервного копирования баз данных, после выполнения скрипта данные направляются на второй файловый сервер, выступающий дополнительной точкой хранения.

db_backup.php - универсальный скрипт учитывающий изменения в базах данных, вычищающий устаревшие бэкапы (остаются бэкапы сделанные в течении дня только за идущую неделю, за прошлые недели и месяцы остаётся один бэкап).

На втором файловом сервере, куда происходит копирование файлов после успешного выполнения резервного копирования с использованием db_backup.php, находится скрипт clean_backup.php для удаления копий аналогично первому серверу (остаются бэкапы сделанные в течении дня только за идущую неделю, за прошлые недели и месяцы остаётся один бэкап).

Пользовательские файлы

Тут всё просто - rsync синхронизация с NAS2 на NAS1 каждую ночь в 03.30 :

```
30 3 * * * rsync -avhr --ignore-existing /home/ext_files/* www-data@192.168.100.5:/home/ext_files
```

8. Подключение к БД

Для подключения к БД в директории: /home/www/devcontrol/имя_директории с приложением, находится файл config_db.php

Где:

```
//Подключение к buh_main
$db_main_host="ADDRESS";
$db_main_user="buh_main";
$db_main_pwd="PASSWORD";
$db_main_base="buh_main";

//Подключение для пользоватея buh
$db_local_host="localhost";
$db_local_user="buh";
$db_local_pwd="";
$db_local_base="";

//Подключение к buh_user
$mss_db_host = "ADDRESS";
$mss_db_login = "buh_users";
$mss_db_password = "PASSWORD";
$mss_db_db = "buh_users";

//RabbitMQ
$AMQP_CREDS["tasks"]=array("host"=>"ADDRESS","login"=>"buh_amqp","pass
word"=>"PASSWORD","port"=>5672);```
```

9. Установка dart-sass

Dart-sass используется для динамической сборки CSS-файлов в системе. Приложение работает с версией dart-sass 1.20.1, установленной в каталог /usr/share/sass Рекомендуется установка именно этой версии.

Выполните следующие команды:

```
wget https://github.com/sass/dart-sass/releases/download/1.20.1/dart-sass-1.20.1-linux-x64.tar.gz
```

```
tar –xf dart-sass-1.20.1-linux-x64.tar.gz
mkdir /usr/share/sass
cp dart-sass-1.20.1-linux-x64.tar.gz /usr/share/sass
# Проверка:
/usr/share/sass/sass --version
```

Также установите дополнительное программное обеспечение:

```
apt install mupdf mupdf-tools
apt install p7zip-full unzip zip
```

10. Директории расположения

Дистрибутив приложения разворачивается после настройки nginx, php-fpm и других сервисов.

Создайте каталоги приложения в /home/www/, после чего смените пользователя каталогов на www-data:

```
mkdir /home/www
chown –R www-data:www-data /home/www
```

Также скопируйте папку .composer в /home/www/ и скопируйте файл rewrite.conf в /home/www/

Откройте файл /home/www/devcontrol/config_vars.php и пропишите путь для каталога файлового хранилища. По умолчанию это /home/www/ext_files

Откройте файл /home/www/devcontrol/config_db.php и пропишите параметры доступа для каждого пользователя БД. Параметры доступа группируются в массивы, один элемент массива на каждый развернутый сервер БД. Система сама выберет работающий в момент запроса сервер, перебирая их по порядку. В случае развертывания более одного сервера приложений рекомендуется указывать первым тот сервер БД, который будет отвечать быстрее.

После регистрации пользователей с административными правами рекомендуется удалить первого пользователя.