ПРОГРАММНЫЙ КОМПЛЕКС

«Bars.Up.Access Manager»

Инструкция по установке экземпляра программного обеспечения

Листов 11

2024

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

Сокращение	Описание
DNS	Domain Name System – компьютерная распределенная система для получения информации о доменах.
HTML	HyperText Markup Language – стандартизированный язык разметки документов в сети Интернет.
HTTP	HyperText Transfer Protocol — «протокол передачи гипертекста» — протокол прикладного уровня передачи данных.
HTTPS	Расширение протокола HTTP, поддерживающее шифрование. Данные, передаваемые по протоколу HTTP, «упаковываются» в криптографический протокол SSL, тем самым обеспечивается защита этих данных.
IP	Internet Protocol — уникальный сетевой адрес узла в компьютерной сети, построенной по протоколу IP.
IP-адрес	Сетевой адрес в цифровом виде, уникальное число, назначающееся каждому компьютеру, подключенному к Интернет.
JSON	JavaScript Object Notation — простой формат обмена данными, удобный для чтения и написания как человеком, так и компьютером.
SSL	SSL (Secure Socket Layer) стандартная интернет-технология безопасности, которая используется, чтобы обеспечить зашифрованное соединение между веб-сервером (сайтом) и браузером.
SSO	Single Sign-On - технология, при использовании которой пользователь переходит из одного раздела портала в другой без повторной аутентификации.
URL	Uniform Resource Locator – стандартизированный способ записи адреса ресурса в сети Интернет.
Администратор	Пользователь, которому присвоена роль администратора в одном домене с привилегиями администратора только в группе проектов этого домена.
БД	База данных
Домен	Метод объединения проектов в независимые группы.
ОС	Операционная система
ПК	Программный комплекс
Пользователь	Сотрудник, который использует программный комплекс «Bars.Up.Access Manager».

ВВЕДЕНИЕ

Область применения

Программный комплекс «Bars.Up.Access Manager» (далее — ПК «Bars.Up.Access Manager», ПК, Изделие или ОО) предназначен для защиты от несанкционированного доступа к информации прикладных web-приложений, идентификации и аутентификации пользователей, разграничения доступа (авторизованного доступа) к данным защищаемых прикладных приложений, регистрации событий безопасности.

1. Подготовка к установке

1.2 Уровень подготовки администратора

Для выполнения установки АМ специалист должен обладать следующими знаниями и опытом:

Для установки в автономном режиме

- администрирование серверов под управлением ОС семейства Linux/Unix
- администрирование Postgres

Для установки в режиме домена

- требуемые для установки в автономном режиме
- администрирование локальных вычислительных сетей
- администрирование кластеров серверов

1.3 Выбор варианта установки

1.3.1 Установка в автономном режиме

Данный вариант установки используется при ожидаемой невысокой нагрузке на экземпляр АМ, отсутствию необходимости обеспечения бесперебойного режима работы экземпляра АМ. Например, при тестовой установке.

При использовании данного режима установки возможна развертывание всех необходимых компонент экземпляра АМ на один сервер.

1.3.2 Установка в режиме домена

Для обеспечения бесперебойности работы и обеспечения необходимого уровня производительности при высокой нагрузке на экземпляр АМ следует использовать данный режим установки.

При использовании данного режима работы предполагается развертывание компонент экземпляра АМ на группу серверов по узлам.

1.4 Требования к среде развертывания

1.4.1 Характеристики серверов

Таблица 2 - Характеристики серверов

Элемент	Параметр
Сервер БД	Количество ядер процессора – не менее 2. ОЗУ – не менее 8 Гбайт. Свободное место на жестком диске – не менее 64 Гбайт.
Сервер кластерного домена (Master Wildfly)	Количество ядер процессора – не менее 2. ОЗУ – не менее 4 Гбайт. Свободное место на жестком диске – не менее 40 Гбайт. (рекомендуется кластер из нескольких нод для повышения отказоустойчивости и производительности)
Сервер кластера ядра платформы	Количество ядер процессора – не менее 2. ОЗУ – не менее 8 Гбайт. Свободное место на жестком диске – не менее 40 Гбайт.
Web-сервер	Количество ядер процессора – не менее 2. ОЗУ – не менее 8 Гбайт. Свободное место на жестком диске – не менее 40 Гбайт. (рекомендуется кластер из нескольких нод для повышения отказоустойчивости и производительности)
Сервер-балансировщик	Количество ядер процессора – не менее 1. ОЗУ – не менее 4 Гбайт. Свободное место на жестком диске – не менее 40 Гбайт.

1.4.2 Локальная сеть

Для установки в режиме домена требуется, чтобы в сети домена работал multicast.

1.4.3 Операционная система

Для серверов используется Ubuntu 20.04.2 LTS (x86/x64) или Astra Linux Special Edition;

2. Установка

2.2 Сборка Изделия

Сборка Изделия осуществляется из исходных кодов, поставляемых на оптическом диске.

Для сборки Изделия необходимо в терминале последовательно выполнить следующие команды:

```
1  sudo apt install openjdk-8-jdk -y
2  echo export JAVA_HOME=/usr/lib/jvm/java-8-openjdk-amd64 >> ~/.bashrc
3  source ~/.bashrc
4  sudo apt install maven -y
5  cd ~/build
6  sudo ./scripts/clean.sh
7  sudo ./scripts/compile.sh
```

Если будет производится пересборка путём выполнения скриптов «clean.sh» и «compile.sh», то необходимо будет переустановить Изделие выполнив пункт 3.2.2 и 3.2.3.

Результатом сборки будут артефакты в директории ~/build/target.

Также в ~/build создаётся архив bam-N.N.N.zip содержащий артефакты сборки.

2.3 Автономный режим

Для работы доменное имя системы с IP-адресом сервера автономной установки должно быть прописано в DNS-сервере или в файле hosts клиента.

2.3.1 Настройка ОС

Выполнить настройки командами:

```
1  sudo sh -c 'echo "net.core.wmem_max = 1048576" >> /etc/sysctl.conf'
2  sudo sh -c 'echo "net.core.rmem_max = 26214400" >> /etc/sysctl.conf'
3  reboot
```

Для применения настроек требуется перезагрузка ОС.

2.3.2 Подготовка файлов дистрибутива

Распаковать архив **bam-N.N.N.zip**

Содержание директории:

- bam-doc-N.N.N.tar.gz - документация АМ;
- bam-install-N.N.N.tar.gz – установочные бинарные файлы;
- bam-sources-N.N.N.tar.gz – установочные бинарные файлы;
- checksum.md5 – файл с контрольными суммами.

Распаковать архив bam-install-N.N.N.tar.gz командой:

```
1  tar -xzvf bam-install-N.N.N.tar.gz
```

Меню установки представлено на рисунке 1.

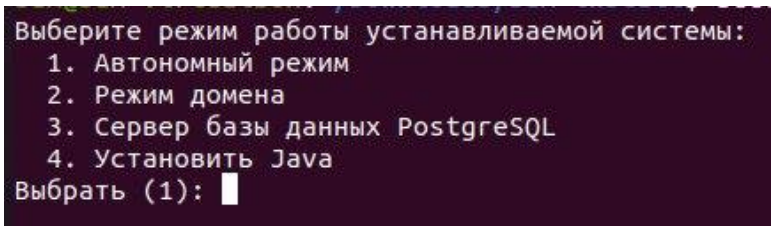

Рисунок 1 – Меню установки

Для установки Java - запустить скрипт install.sh и выбрать пункт «4. Установить Java».

Для установки БД - запустить скрипт install.sh и выбрать пункт «3. Сервер базы данных PostgreSQL». На рисунке 2 изображен скриншот из процесса установки БД.

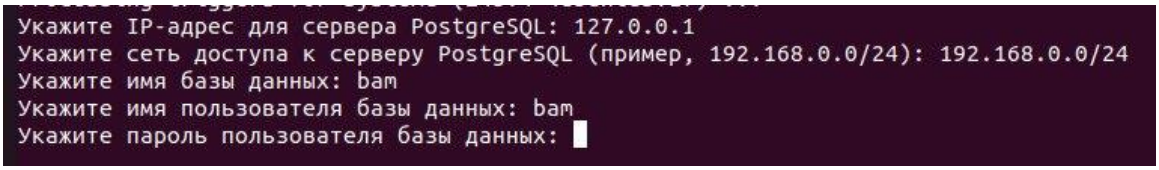

Рисунок 2 — Установка базы данных

2.3.3 Установка Wildfly и Изделия

Для установки Wildfly и Изделия - запустить скрипт «install.sh» и выбрать пункт «1. Автономный режим». На рисунке 3 изображен скриншот из процесса установки АМ в автономном режиме.

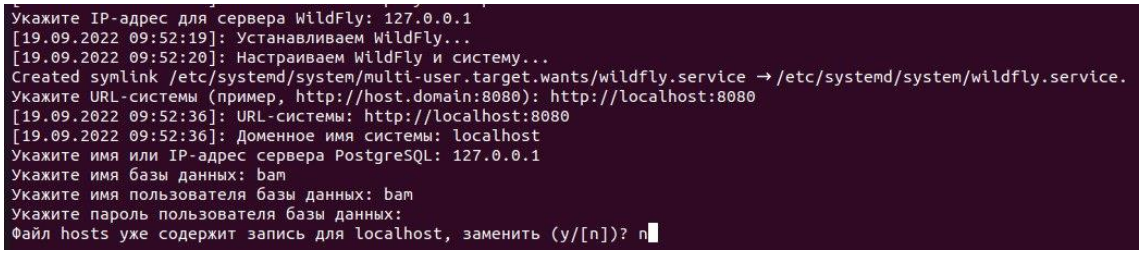

Рисунок 3 — Установка АМ в автономном режиме

2.3.4 Настройка после установки

Далее необходимо открыть порт 8080. Для это необходимо выполнить команду:

```
1 firewall-cmd --zone=public --add-port=8080/tcp --permanentfirewall-cmd --reload
```

По завершению установки приложение имеет необходимые базовые настройки, в т.ч. учетную запись для администрирования:

- логин: admin
- пароль: 5511566

Консоль администрирования доступна по адресу:

- **Ошибка! Недопустимый объект гиперссылки.**.

Для установки рекомендуется использовать доменное имя (DNS - адрес) например: am.bars.group.

Для работы доменное имя системы с IP-адресом сервера автономной установки должно быть прописано в DNS-сервере или в файле hosts клиента.

Для работы системы по доменному имени рекомендуется установить nginx.

Возможна работа приложения по ip адресу, тогда установка nginx не требуется.

Сервера WildFly запускаются на порту 8080, поэтому, если на сервере автономной установки не прописан редирект с другого порта (например, 80), то URL-системы должен включать :8080.

Если предполагается использование Nginx, указать в качестве URL-системы: **Ошибка! Недопустимый объект гиперссылки.**>. В jbos-cli.sh выполнить:

1	/subsystem=undertow/server=default-server/http-listener=default:write-attribute(name=proxy-address-forwarding,value=true) изменить https на http в файле /etc/wildfly/security.json systemctl restart wildfly iptable -t nat -A OUTPUT -p tcp -d 127.0.0.1 --dport 80 -j DNAT --to-destination 127.0.0.1:8080.

Если предполагается установка Nginx на отдельном сервере, на сервере автономной установки применить дополнительно правило:

iptable -t nat -A OUTPUT -p tcp -d $IP_ADDR_WF --dport 80 -j DNAT --to-destination $IP_ADDR_WF:8080

где: IP_ADDR_WF - адрес установки wildfly.

На сервере с Nginx никаких настроек кроме установки и настройки nginx производить не нужно.

2.4 Развертывание узлов домена

Для запуска системы в режиме домена (для режима домена требуется, чтобы в сети домена работал multicas) следует развернуть узлы домена в следующем порядке:

1. Узел мастера домена;
2. Узел балансера;
3. Узел ядра (если требуется дополнительный узел ядра, один экземпляр ядра запускается на мастере);
4. Узел консоли администрирования.

Сервера WildFly запускаются на порту 8080, поэтому, если на узле балансера не прописан редирект с другого порта (например, 80), то URL-системы должен включать :8080.

Если предполагается использование Nginx (балансер), указать в качестве URL-системы: **Ошибка! Недопустимый объект гиперссылки.**>.

Предустановки для всех узлов:

```
1 echo "net.core.wmem_max = 1048576" >> /etc/sysctl.conf
2 echo "net.core.rmem_max = 26214400" >> /etc/sysctl.conf
3 reboot
```

На всех узлах добавить записи в /etc/hosts с именами узлов, например:

```
1 192.168.x.2 am-wlb-web-01
2 192.168.x.3 am-web-01
3 192.168.x.4 am-web-02
4 192.168.x.5 am-core-01
5 192.168.x.6 am-core-02
6 192.168.x.7 am-db-01
```

2.4.1 Установка и настройка узла мастера домена

Запустить скрипт установки:

```
1 cd bam-install
2 ./install.sh
```

В появившемся меню выбрать пункт 2, затем пункт 1, пункт 1 и следовать указаниям установщика.

После установки узла мастера домена требуется добавить учетные записи остальных узлов, для этого запустите скрипт установки и выберите пункт 2, затем пункт 1, пункт 2. Данные добавленных учетных записей узлов потребуются для дальнейших инициализаций узлов.

2.4.2 Установка узла балансера

Для работы доменное имя системы с IP-адресом узла балансера должно быть прописано в DNS-сервере или в файле hosts клиента.

Сервера WildFly запускаются на порту 8080, поэтому, если на узле балансера не прописан редирект с другого порта (например, 80), то URL-системы должен включать :8080.

Запустить скрипт установки:

```
1 cd bam-install
2 ./install.sh
```

В появившемся меню выбрать пункт 2, затем пункт 2 и следовать указаниям установщика.

2.4.3 Установка узла ядра

Запустить скрипт установки:

```
1 cd bam-install
2 ./install.sh
```

В появившемся меню выбрать пункт 2, затем пункт 3 и следовать указаниям установщика.

2.4.4 Установка узла консоли администрирования

Запустить скрипт установки:

```
cd bam-install
./install.sh
```

В появившемся меню выбрать пункт 2, затем пункт 4 и следовать указаниям установщика.

Если предполагается использование Nginx - указать в качестве URL-системы: **Ошибка! Недопустимый объект гиперссылки.**>.

2.4.5 Установка Nginx

Скачать требуемую версию Nginx (не ниже 1.19.6) по адресу:

https://nginx.org/en/download.html

Для установки запустить команду:

```
apt install nginx
systemctl stop nginx
systemctl enable nginx
```

Удалить символьную ссылку /etc/nginx/sites-available/default.

Создать файл /etc/nginx/sites-available/bam_realms.conf следующего содержания:

```
server {
  listen 80;
  return 301 https://$host$request_uri;
}
server {
  listen 443;
  server_name ia.rt-eu.ru;
  # Файлы с сертификатом и закрытым ключом должны быть заранее
подготовлены, например с помощью https://letsencrypt.org/
  ssl_certificate /etc/nginx/cert.pem;
  ssl_certificate_key /etc/nginx/cert.key;
  ssl_session_cache builtin:1000 shared:SSL:10m;
  ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
  ssl_ciphers
HIGH:!aNULL:!eNULL:!EXPORT:!CAMELLIA:!DES:!MD5:!PSK:!RC4;
  ssl_prefer_server_ciphers on;
   location /admin/ {
    deny all;
  }
   location / {
    proxy_set_header Host $host;
    proxy_set_header X-Real-IP $remote_addr;
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header X-Forwarded-Proto $scheme;
    proxy_set_header X-Forwarded-Port 443;
    proxy_pass http://<IP-АДРЕС_УЗЛА_БАЛАНСЕРА>:8080;
    proxy_redirect http://<ДОМЕННОЕ_ИМЯ_СИСТЕМЫ>:8080/ /;
  }
}
```

Запустить Nginx:

```
1 systemctl start nginx
```

На узле балансера открыть порты 80 и 443, а также добавить правило:

```
1 iptables -t nat -A PREROUTING -p tcp -m tcp -s 192.168.x.0/24 --dport 80 -j REDIRECT --to-ports 8080
```