ENERGY CONSULTING
компания цифровых решений

Программный Комплекс «СОЮЗ-ЕАМ» (ПК «СОЮЗ-ЕАМ»)

Технологическая инструкция по инсталляции

Москва 2022 г.

Оглавление

1 Общие положения

1.1 Обозначение системы

Программный Комплекс «СОЮЗ-EAM».

Сокращенное фирменное обозначение на русском языке: «ПК «СОЮЗ-EAM».

1.2 Назначение, цели и задачи

ПК «СОЮЗ-EAM» (далее – система) предназначен для управления активами предприятия, в том числе мониторинга текущего состояния активов, планирования технического обслуживания и ремонта оборудования согласно регламентам ТОиР, оформления заказов на проведение работ по обслуживанию оборудования, учета и контроля выполнения данных работ. ПК «СОЮЗ-EAM» включает базу данных оборудования предприятия, поддерживающую иерархическую структуру и позволяющую вести учет основного и вспомогательного оборудования, в том числе его технических или иных параметров.

ПК «СОЮЗ-EAM» служит для обеспечения согласованного и координированного управления производственными активами предприятия.

ПК «СОЮЗ-EAM» представляет собой полностью отечественный программный комплекс, разработанный с учётом санкционных рисков на основе программного обеспечения «Визари».

ПК «СОЮЗ-EAM» устанавливается в одном, а при необходимости резервирования (повышения отказоустойчивости) и распределения нагрузки в нескольких территориально распределённых центрах обработки данных, в которых осуществляется хранение и обработка информации предприятия (организации).

2 Установка и подготовка системного окружения

1. На целевые серверы и управляющий хост установить CentOS 7.9

2. На целевых серверах и управляющем хосте на время установки должен быть доступ к сети интернет.

2.1 Подготовка управляющего хоста

1. Установить необходимые библиотеки apt

sudo apt-get install python3 python3-module-pip rsync unzip openssh openssl sshpass

2. yum

sudo yum install python3 python3-pip rsync unzip openssh openssl sshpass libselinux-python3

3. Обновить pip

sudo pip3 install --upgrade pip

4. Создать учетную запись оператора

sudo useradd -c "Ansible operator" -m ansible

5. задать пароль

sudo passwd ansible

6. Войти в систему на управляющем хосте под именем `ansible`

7. Сгенерировать ключ для доступа к управляемым серверам

ssh-keygen -t rsa -b 4096 -C "ansible@control.host"

8. Установить необходимые библиотеки python

pip3 install --upgrade ansible==2.10. jinja2 pexpect*

9. Установить необходимые библиотеки Ansible

ansible-galaxy collection install community.general community.rabbitmq community.postgresql

2.2 Подготовка к установке

Целевые серверы должны поддерживать авторизацию с публичным ключом.

Все операции производятся на управляющем хосте с установленным `ansible` версии 2.10 и последней доступной версии `jinja2` от пользователя `ansible`.

В случае если имя пользователя не совпадает, может потребоваться дополнительная настройка инвентарных переменных.

Для межсерверного обмена будет использован ip адрес первого сетевого интерфейса системы, если требуется другой адрес - указать в инвентаре или внести изменения в файл `etc/hosts` на целевых хостах после установки.

1. Создать инвентарь целевого ландшафта, скопировав папку `cmms` в соседнюю с именем ландшафта, например `test`

2. Внести целевые сервера в файл `test/inventory.yaml`

> Для правильной настройки системы, все группы, за исключением `kibana`, должны иметь в составе хост или другую группу с ними.

> ***Не следует указывать одинаковые ip для хостов с разными именами***, это приведет к ошибкам вроде блокировки файлов при установке пакетов. Для размещения нескольких приложений на одном сервере используйте группы, поместив в состав групп приложений имя этого сервера, параметры подключения указать один раз, где удобно.

3. Установить python3 на целевые машины:

- *ansible-playbook -i test preinstall-python3.yml -k -K -u %username_with_sudo_access%*

4. Создать управляющего пользователя на целевых серверах выполнив команду:

- *ansible-playbook -i test create-ansible-user.yml -k -K -u %username_with_sudo_access%*

5. Внести необходимые параметры конфигурации в переменные инвентаря в директории `test/group_vars`

- visary_id_host - доменное имя сервера авторизации

- visary_home_host - доменное имя сервера приложения

6. Разместить tls сертификаты и ключи для доменов в директории `files/test/ssl` с именами `{{ visary_common_ssl_crt_name }}.crt` и `{{ visary_common_ssl_crt_name }}.key` (см. `group_vars/nginx.yml`) для имеющихся доменов или сгенерировать самоподписанные сертификаты командой:

- *ansible-playbook -i test generate-certificates.yml --skip-tags openssl*

3 Развертывание ПК «СОЮЗ-ЕАМ»

1. Сгенерировать сертификаты OpenID командой:

   - *ansible-playbook -i test generate-identity-certificate.yml --skip-tags openssl*

2. Сгенерировать статические файлы конфигурации

   - *ansible-playbook -i test generate-config.yml*

3. Установить окружение выполнив комманду:

   - *ansible-playbook -i test install-app-environment.yml*

4. Установить приложения выполнив команду:

   - *ansible-playbook -i test install-visary.yml*

5. Открыть порты приложений:

   - *ansible-playbook -i test firewall.yml*

4 Порядок проверки работоспособности

Настроить днс сервер или добавить записи в файл `etc/hosts`.

Для проверки работоспособности Системы необходимо с рабочего места администратора и клиента запустить интернет-браузер и ввести URL системы.

Для вызова Системы с рабочего места пользователя необходимо выполнить следующие действия:

— открыть веб-браузер;

— ввести URL-адрес Системы.

Открывается окно аутентификации пользователя (рисунок 1).

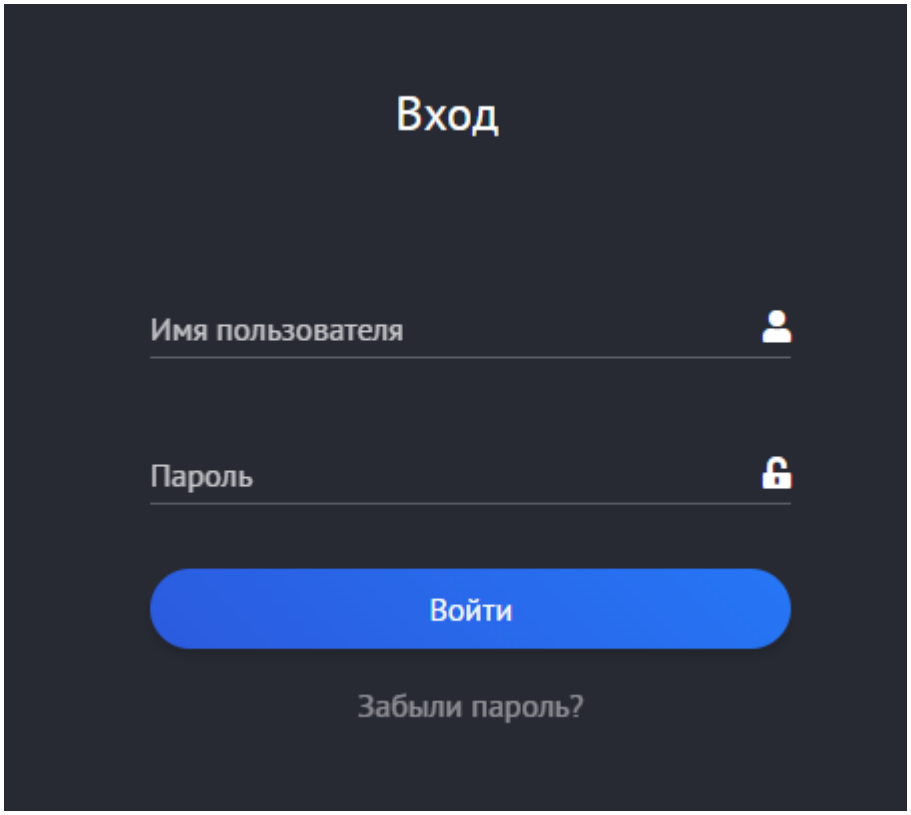

Рисунок 1 – Аутентификации администратора

В окне аутентификации, нужно ввести логин и пароль администратора, нажать кнопку «Войти». Логин администратора – admin, пароль по умолчанию прописан в инвентаре test\group_vars\all.yaml в переменной visary_default_admin_password.

5 Настройка Системы

Для настройки Системы администратор использует следующие разделы главного меню:

- Сервис:
  - Настройки;
  - Меню;
  - Мнемоники;
  - Бизнес-процессы;
  - Отчеты;
  - Шаблоны сообщений;
- Безопасность:
  - Панель администрирования;
  - Роли;
  - Доступ к объектам;

Система представляет собой перечень реестров, составляющих главное меню Системы.

Каждый реестр содержит перечень записей (карточек объектов).

Карточка объекта представляет собой форму (экран) с перечнем полей для ввода данных.

При необходимости данные отображаются на нескольких вкладках.

6 Аварийные ситуации

6.1 Действия в случае несоблюдения условий выполнения технологического процесса

В случае сбоя в работе Системы восстановление нормальной работы должно быть произведено после:

- перезагрузки ОС;
- перезапуска программного обеспечения.

При повторном возникновении сбоев или аварийных ситуаций необходимо сообщить о них разработчику Системы.

6.2 Действия по восстановлению программ и/или данных

Действия по восстановлению программ и/или данных при отказе магнитных носителей или обнаружении ошибок в данных осуществляются системным администратором.

6.3 Действия в случаях обнаружения несанкционированного вмешательства в данные

Если обнаружено, что кто-то воспользовался именем или паролем пользователя для доступа к данным, то следует изменить имеющийся пароль на новый пароль.

6.4 Действия в случаях отказа доступа к Системе

Если при авторизации логин и/или пароль были введены неверно, то выводится сообщение об ошибке. В этом случае следует заново ввести логин и пароль. Если пользователь уверен в правильности ввода имени и пароля, но, тем не менее, получил отказ в доступе, то следует обратиться к администратору Систему.

6.5 Действия в случаях ошибки сервера

Если сервер не может обработать запрос пользователя, то выдается соответствующее сообщение. Возможно, это связано с обновлением его программного обеспечения или работами по профилактике Системы. В этом случае следует очистить кэш браузера и перезагрузить страницу немного позже. Если проблема сохраняется, обратитесь к разработчику Системы.

6.6 Действия в других аварийных ситуациях

При невозможности исправить аварийную ситуацию, а также по любым другим вопросам администрирования следует обращаться к разработчику Системы.