Программное обеспечение «Базис.Digital Energy». Руководство по эксплуатации. Версия 1.2.0

RU.НРФЛ.00010-01.97.01

Москва

29/03/2024

Содержание

1 Аннотация

Настоящий документ предназначен для технического администратора ПО и содержит инструкции по выполнению работ, необходимых для эксплуатации ПО.

Руководство содержит инструкции по выполнению задач, связанных с:

- сопровождением и обслуживанием ПО;
- диагностикой, локализацией и устранением предусмотренных неисправностей.

2 Перечень эксплуатационных документов

Дополнительно к настоящему документу технические администраторы должны использовать следующие документы:

- ПО «Базис.Digital Energy». Руководство по установке RU.НРФЛ.00010-01 93 01;
- ПО «Базис.Digital Energy». Руководство администратора RU.НРФЛ.00010-01 95 01.

3 Идентификационные данные документа

Идентификационные данные ПО	**Программное обеспечение «Базис.Digital Energy»**
Название документа	ПО «Базис.Digital Energy». Руководство по эксплуатации
Обозначение документа	RU.НРФЛ.00010-01 97 01
Автор документа	ООО «БАЗИС»

4 Требования к составу и квалификации обслуживающего персонала

Системный инженер – должностное лицо, служебная деятельность которого обеспечивает качественную и безопасную эксплуатацию оборудования ЦОД или виртуального ЦОД – облачной платформы – после внедрения (ввода в эксплуатацию).

Администратор ОП – должностное лицо, служебная деятельность которого связана с эксплуатацией программных продуктов и стороннего ПО, используемого при создании среды функционирования:

- Kubernetes – проект с открытым исходным кодом, предназначенным для управления кластером контейнеров Linux как единой системой. Kubernetes управляет и запускает контейнеры Docker на большом количестве хостов, а так же обеспечивает совместное размещение и репликацию большого количества контейнеров.

Системный инженер должен иметь навыки проектирования или настройки аппаратных и программных конфигураций компьютерных сетей, обслуживания локальных вычислительных сетей. Кроме того, он может быть ответственен за организацию защиты информации и производить установку антивирусов и другого программного обеспечения, обновление ПО. Полезным будет также навык анализа затрат на системное обслуживание, составление отчетов и поиск способов оптимизации расходов.

Оперативный персонал (системный инженер), осуществляющий манипуляции с оборудованием на площадке, должен иметь допуск к эксплуатации электроустановок до 1000В. Категория допуска должна быть согласована со службами эксплуатации ЦОД.

Обычными задачами системного администратора, в зависимости от инфраструктуры, являются контроль работы компьютерных программ и устранение ошибок в их работе, разовая диагностика/ремонт ПК и другой офисной техники.

Системный администратор должен уметь использовать множество утилит и инструментов администрирования системой с целью:

- контроля работоспособности системы (проверки основного функционала);
- проверки работоспособности отдельных системных служб;
- конфигурирования виртуальных сервисов системы;
- резервного копирования и восстановления виртуальных машин.

Для выполнения задач по сопровождению ПО «Базис.Digital Energy», необходимо иметь опыт работы, связанный с системным администрированием серверного оборудования, а также понимать основные принципы создания и настройки кластера Kubernetes.

Деятельность системного инженера регулируется и контролируется отделом информационной безопасности, а также внутренними регламентами предприятия, нацеленными на обеспечение безопасности данных и соблюдение конфиденциальности.

5 Описание продукта

5.1 Назначение

ПО «Базис.Digital Energy» (далее Базис.Digital Energy, ПО, система) основано на концепции DevSecOps. Концепция DevSecOps реализует внедрение автоматизированных проверок безопасности в процессе DevOps, то есть в процесс разработки программного обеспечения на протяжении всего жизненного цикла, начиная от разработки, тестирования до его доставки и развертывания. Базис.Digital Energy предоставляет DevSecOps как услугу, что позволяет решить следующие задачи:

- применение разнообразных инструментов;
- автоматизация развертывания и обновления инструментов;
- минимизировать количество конфигурационных файлов инструментов;
- связанность инструментов;
- поддержка и эксплуатация инструментов.

Функциональные возможности

Продукт выполняет функции создания кластера Kubernetes, его настройки, установки и настройки необходимых инструментов DevOps и DevSecOps и предоставляется в виде услуги, как один из платформенных сервисов «Базис.DynamiX».

ПО «Базис.Digital Energy» предоставляет пользователю следующие функциональные возможности:

- полнофункциональный графический интерфейс, позволяющий осуществлять настройку, установку инструментов, обеспечивающий удобное взаимодействие с инструментами;
- набор готовых инструментов для развертывания;
- обеспечение связанности инструментов;
- предоставление обновляемого хранилища образов для своевременного обновления инструментов;
- предоставление системы мониторинга установленных приложений;
- возможность интеграции с другими продуктами ООО "БАЗИС".

5.2 Структура ПО

- backend (написан на Golang);
- decort-go-sdk - компонент, представляющий библиотеку, написанную на языке GO, позволяющую взаимодействовать с API облачной платформы DECORT. Библиотека содержит в себе структуры и методы, необходимые для отправки запросов. Decort SDK имеет встроенный http-клиент и поддерживает разные способы авторизации на платформе. Библиотека так же содержит в себе модели ответов от платформы;
- monitagent (написан на Golang) - размещаемый в k8s кластере сервис, предназначенный для контроля и мониторинга инструментов;
- integagent (написан на Golang) - также размещаемый в k8s кластере сервис, предназначенный для настройки и интеграции инструментов;
- frontend (написан с использованием Vue.js фреймворка) компонент, представляющий собой javascript приложение, исполняемое в браузере пользователя, и предназначенное для создания графического интерфейса к ПО «Базис.Digital Energy» .

На рисунке 1 отображена обобщенная схема взаимодействия сервисов ПО «Базис.Digital Energy», сервисов инструментов (инсталлируемых продуктов) и иных сервисов:

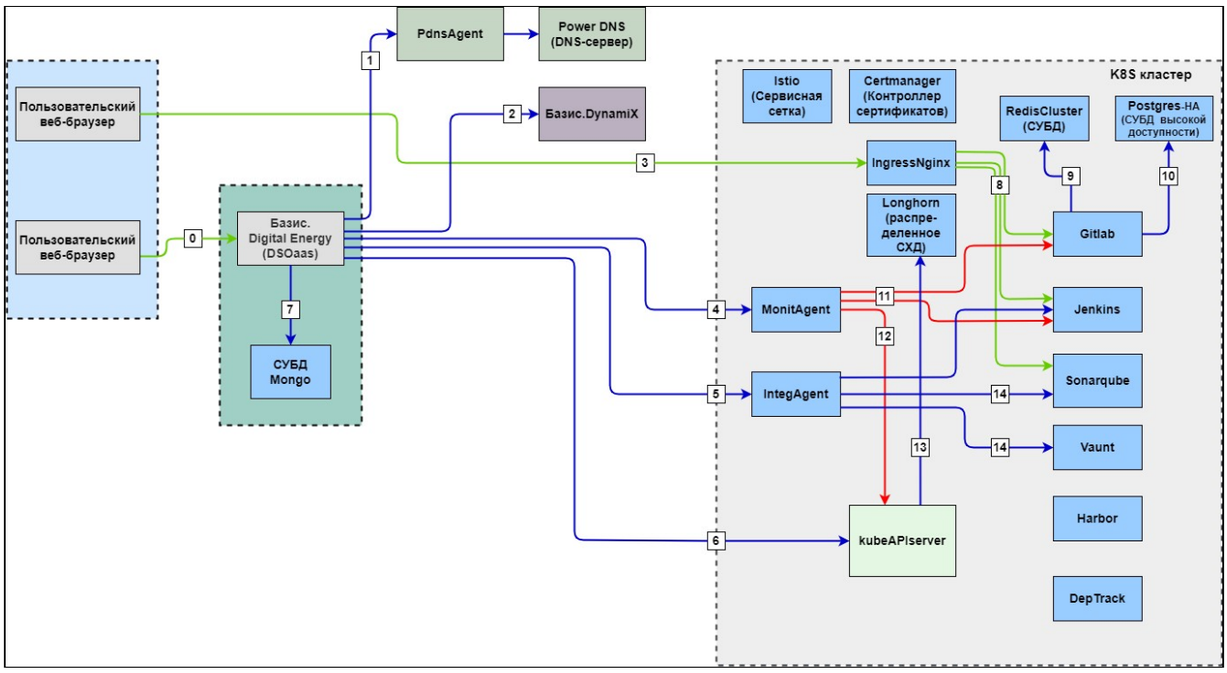

Рисунок 1 - Схема взаимодействия сервисов ПО «Базис.Digital Energy», сервисов инструментов (инсталлируемых продуктов) и иных сервисов

где,

- Ingress nginx - Контроллер Ingress-NGINX для Kubernetes;
- IntegAgent - Интеграционный сервис, Сервис комплексного управления инсталлированными продуктами;
- KubeAPIServer - сервисы Kubernetes;
- MonitAgent - Сервис мониторинга, Сервис мониторинга состояния продуктов;
- PdnsAgent - DNS сервис, Сервис управления DNS записями.

Назначение коммуникации на схеме:

- 0 - Получение JS фронтэнда приложения, RPC запросы для развертывания K8S кластера, запросы для инсталляции, деинсталляции, мониторинга приложений, запросы для аутентификации и авторизации, запросы для управления пользователями DSOaaS;
- 1 - RPC запросы на создание/удаление DNS зон и DNS записей сервисов;
- 2 - RPC запросы на создание/удаление K8S кластера и вспомогательной информации;
- 3 - HTTP запросы для получения JS фронтэндов продуктов и взаимодействия с продуктами, развернутыми в кластере;
- 4 - RPC запросы для мониторинга состояний кластера, компонентов продуктов и самих продуктов;
- 5 - RPC запросы для интеграционного управления продуктами, развернутых в кластере;
- 6 - RPC запросы для управления K8S кластера и его объектами, в частности развертывания продуктов;
- 7 - Запросы к Mongo DBMS для получения/хранения информации о развернутых кластерах, продуктах, пользователях/группах, сессиях и иной информации;
- 8 - HTTP запросы к продуктам внутри кластера, переданные извне него посредством reverse proxy;
- 9 - Запросы к Redis key-value DBMS, для хранения промежуточных/кэшируемых данных;
- 10 - SQL запросы к PostgreSQL DBMS для хранения основных данных приложений-продуктов;
- 11 - Запросы к приложениям-продуктам для мониторинга их состояния;
- 12 - Запросы к K8S API для мониторинга/контроля состояний объектов кластера и интегрированных в кластер продуктов, таких как certmanager, longhorn, istio;
- 13 - Event запросы к интегрированным в кластер сервисам;
- 14 - Запросы к приложениям-продуктам для реализации/развертывания типовых схем взаимодействия.

Типы коммуникаций на схеме:

- 0 - HTTPS REST;
- 1 - GRPC;
- 2 - HTTPS REST;
- 3 - HTTPS REST;
- 4 - GRPC;
- 5 - GRPC;
- 6 - HTTPS REST;

- 7 - MONGO;
- 8 - HTTPS, HTTPS REST;
- 9 - Redis;
- 10 - PostgreSQL;
- 11 - HTTP/HTTPS REST;
- 12 - HTTPS REST;
- 13 - HTTPS REST;
- 14 - HTTP REST.

Инструменты (инсталлируемые продукты с их сервисами) на схеме можно условно разделить на две группы по назначению:

Инфраструктурный уровень:

- Certmanager;
- Istio;
- Ingress-nginx;
- IntegAgent;
- Longhorn;
- MonitAgent;
- Redis cluster;
- Postgresql-HA.

GUI инструменты (продукты) непосредственно для использования в разработке:

- Deptrack;
- Gitlab;
- Harbor;
- Jenkins;
- Sonarqube
- Vault;
- Nexus.

5.3 Паспорта инсталлируемых сервисов

Название сервиса	**Описание**
Certmanager	Язык программирования - golang Есть возможность использовать prometheus, настройка в values
Dependency track	Язык программирования - java Есть возможность использовать prometheus(https://docs.dependencytrack.org/getting-started/monitoring), настройки в values нет. Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn; • Postagent; • Postgresql
Gitlab	Язык программирования - ruby, golang, js Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn; • Postagent; • Postgresql

Название сервиса	Описание
Harbor	Язык программирования - golang, ts, python Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn; • Postagent; • Postgresql; • Redis
IngressNginx	Язык программирования - golang Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливается сервис: Certmanager
IntegAgent;	Язык программирования - golang Интеграционный сервис и сервис комплексного управления инсталлированными продуктами. Разработка ООО "БАЗИС"
Istio	Язык программирования - golang Есть возможность использовать prometheus, настройка в values
Jenkins	Язык программирования - java Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn
Longhorn	Язык программирования - shell, python Возможности настройки prometheus в values нет Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx
MonitAgent	Язык программирования - golang Сервис мониторинга, сервис мониторинга состояния продуктов. Разработка ООО "БАЗИС"
Postgress-HA	Язык программирования - c Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager: • Ingress-Nginx: • Longhorn: • Postagent

Название сервиса	Описание
RedisCluster	Язык программирования - C Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Ingress-Nginx; • Postgresql; • Postagent
Sonarqube	Язык программирования - java Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn; • Postagent; • Postgresql
Vaunt	Язык программирования - golang Есть возможность использовать prometheus, настройка в values Для обеспечения работы устанавливаются сервисы: • Certmanager; • Ingress-Nginx; • Longhorn

6 Условия применения

ПО «Базис.Digital Energy» эксплуатируется в вычислительной среде центра обработки данных (дата-центра), который может быть как централизованным, так и территориально-распределенным.

Основные компоненты составляющие типовой информационно-вычислительный центр (далее – дата-центр или ЦОД):

1. Приложение: компьютерная программа, задающая логику вычислительных операций.
2. Система управления базами данных (СУБД): ПО, обеспечивающее структурированный способ хранения банков (баз) данных.
3. Хост-система (главный компьютер): вычислительная платформа, состоящая из оборудования, программно-аппаратных средств и программного обеспечения, обеспечивающая работу управляющих приложений и СУБД.
4. Сеть: физические каналы обмена данными, обеспечение связи между различными устройствами, подключенными к сети.
5. Хранилище: устройство накопления и постоянного (длительного) хранения данных.

Приложения, наделенные бизнес-логикой, функционируют, как правило, в границах IaaS – изолированной от прямого вмешательства среде.

СУБД используются как для поддержания целостности модели инфраструктуры, так и для накопления и/или выборки данных. В зависимости от архитектуры применения приложений, использующих определенные СУБД, выбираются узлы, обеспечивающие наиболее благоприятные условия эксплуатации. Могут быть выбраны как серверные компьютеры, так и виртуальные машины, работающие под управлением ОС, обеспечивающей максимальную совместимость с оборудованием – подсистемами передачи и хранения информации, а также наиболее подходящие для выбора в качестве среды функционирования СУБД.

Качество электропитания, подводимого к хост-системе, сетевому оборудованию и системам хранения данных, равно как и прочим средствам ВТ, включенным в состав облачной инфраструктуры, должно соответствовать действующим нормам.

Обслуживающий персонал должен обладать общими знаниями электробезопасности, пройти необходимый инструктаж ОТ и ТБ, получить допуски к работе на электроприёмниках, в соответствии с Правилами Безопасной Эксплуатации Электроустановок и с учетом доступа в технические помещения.

Кроме того, оперативный персонал, эксплуатирующий оборудование ЦОД в той или иной степени, обязан соблюдать меры пожарной безопасности.

6.1 Инструменты администратора

Деятельность администратора ПО не ограничена использованием одного компьютера (АРМ). В зависимости от характера возникающих задач администратор может использовать различные виды СВТ: от персонального компьютера (ноутбука) с установленной операционной системой Linux до тонкого клиента, с помощью которого пользователь VDI осуществляет подключение к VDI машине.

На СВТ, используемом администратором, должен быть установлен веб-браузер, поддерживаемый операционной системой (Windows, Ubuntu, CentOS и др.). Кроме того, должно быть установлено ПО, позволяющее осуществлять безопасное подключение к управляющим/вычислительным узлам инфраструктуры, а также к вспомогательным виртуальным машинам, если таковые интегрированы в облачную платформу для определенных (сервисно-профилактических) нужд.

Веб-браузер позволяет использовать веб-интерфейс ПО.

Рекомендуемые к использованию веб-браузеры: не рекомендуется применение браузера **Internet Explorer.**

6.2 Удаленный доступ к информации

Удаленный доступ к информации должен обеспечивать безопасные технологии приёма и передачи данных. Например, если настраивается удаленный доступ к облаку, следует использовать SSH или организовывать дополнительные сетевые каналы, использующие VPN.

Необходимо соблюдать меры предосторожности и правила информационной безопасности, установленные в рамках отдела и/или организации. Администратор должен быть бдительным при выполнении авторизации с чужого рабочего места (ТК), так как некоторые веб-браузеры сохраняют вводимые пароли через куки или другими способами.

После того как администратор закончил работу в веб-браузере любого из СВТ, не закрепленного лично за ним, он обязан принять меры по устранению любых сохраненных учетных данных, связанных с доступом к средствам управления или отдельным компонентам облака (имена учетных записей, пароли к

ним и т.п.). Записные или электронные книги, равно как и данный документ, не должны находиться без присмотра в помещениях общего пользования.

> ⚠ **Не допускается случайная или основанная на личном доверии передача третьим лицам учетных данных, смарт-карт, электронных ключей и т.п. средств, позволяющих получить полный или частичный доступ к информации об инфраструктуре.**

В конце рабочей смены все персональные компьютеры и СВТ, закрепленные за администратором, должны быть переданы по смене, с соответствующей отметкой в журнале технической эксплуатации, или заблокированы и заперты в специальном помещении, в зависимости от принятых на предприятии организационных мероприятий и политик безопасности.

Если используются АМДЗ, то электронные ключи должны храниться в сейфе или сдаваться под охрану, в с соответствии с действующими на предприятии должностными инструкциями по информационной безопасности.

6.3 Техническое обслуживание, ремонт

Техническое обслуживание и ремонт средств вычислительной техники, коммутационного оборудования и систем хранения данных, а также источников бесперебойного питания осуществляются на основе паспортов и руководств по (сервисному) обслуживанию, соответствующих моделям и предоставленных предприятиями-изготовителями.

Персонал, осуществляющий техобслуживание/ремонт, должен пройти инструктаж по технике безопасности и обязан слаженно взаимодействовать с администратором, ответственным за эксплуатацию облачной инфраструктуры.

Администратор обязан вести журнал эксплуатации облачной инфраструктуры, оформлять все существенные события, начиная с момента завершения ПНР и приема-сдачи платформы в эксплуатацию.

Планово-профилактические работы должны быть тщательно спланированы вместе с оценкой рисков для эксплуатации. Рекомендуется имитация и отработка вероятных ситуаций на тестовом стенде, чтобы аварийные ситуации, не влияли на качество услуг.

7 Проверка работоспособности ПО

После завершения развертывания ПО «Базис.Digital Energy» произвести создание тестового кластера и установку инструментов.

Успешность тестовой операции свидетельствует о работоспособности ПО.

Для того, чтобы в случае возникновения неопределенных обстоятельств в работе ПО было возможно эффективно взаимодействовать с Технической Поддержкой, предусмотрено логирование работы ПО.

8 Общие указания

Для реализации функций безопасности среды функционирования ПО «Базис.Digital Energy» должны выполняться следующие действия:

- необходимо регулярное обновление всех сред функционирования ПО «Базис.Digital Energy» до актуальных версий с применением всех необходимых патчей безопасности с официальных сайтов разработчиков сред функционирования;
- компоненты операционной системы и сред функционирования ПО «Базис.Digital Energy» должны быть максимально ограничены. Компоненты, которые не участвуют в функционировании ПО «Базис.Digital Energy», должны быть отключены;
- должно обеспечиваться предотвращение несанкционированного доступа к идентификаторам и паролям администраторов среды виртуализации, которые необходимы для управления и технической поддержки среды функционирования ПО «Базис.Digital Energy»;
- необходимо использовать на серверах, где развернута среда функционирования ПО «Базис.Digital Energy», в качестве средств защиты информации от несанкционированного доступа, сертифицированных ФСТЭК России версий операционных систем с установленными обновлениями или наложенных средств защиты информации, прошедших сертификацию по требованиям безопасности информации в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00;
- должна быть обеспечена физическая сохранность серверной платформы с установленным ПО «Базис.Digital Energy» и исключение возможности физического доступа к ней посторонних лиц.

9 Действия по безопасной установке и настройке

Подробное описание установки ПО приведено в документе «ПО «Базис.Digital Energy». Руководство по установке» RU.НРФЛ.00010-01.97.01.

10 Обновление ПО

Обновление ПО осуществляется в соответствии с алгоритмом, описанным в в документе «ПО «Базис.Digital Energy». Руководство по установке» RU.НРФЛ.00010-01.97.01.

11 Деинсталляция сервиса

Для деинсталляции ПО выполнить следующие команды:

```
$ helm uninstall -n dsoaas dsoaas-server

release "dsoaas-server" uninstalled
```

12 Аварийные ситуации

12.1 Действия в случаях обнаружения несанкционированного вмешательства в данные

Несанкционированное вмешательство обнаруживается при помощи протокола нарушений безопасности.

В случаях обнаружения несанкционированного вмешательства в данные, необходимо установить логин пользователя, под которым была произведена аутентификация, затем сменить пароль для этого пользователя и проинформировать пользователя о смене пароля.

12.2 Действия в других ситуациях

В других аварийных ситуациях необходимо обратиться в сервисную службу по электронному адресу: **support@basistech.ru**

13 Описание функционирования

Описание совместного функционирования технических средств и ПО, описание организации входных и выходных данных, используемых при обслуживании технических средств и описание взаимодействий устройств с ПО приведено в эксплуатационных документах:

- RU.НРФЛ.00010-01.97.01 ПО «Базис.Digital Energy». Руководство по установке;
- RU.НРФЛ.00010-01.95.01 ПО «Базис.Digital Energy». Руководство администратора.

14 Термины и определения

Термин	Определение
Golang	Компилируемый многопоточный язык программирования
Helm	Диспетчер пакетов, который упрощает настройку и развертывание приложений в кластерах Kubernetes (для разработчиков и операторов)
Kubernetes	Проект с открытым исходным кодом, предназначенным для управления кластером контейнеров Linux как единой системой. Kubernetes управляет и запускает контейнеры Docker на большом количестве хостов, а так же обеспечивает совместное размещение и репликацию большого количества контейнеров
DevSecOps	(от англ. development, security и operations) - интеграции тестирования безопасности в каждый этап процесса разработки программного обеспечения

15 Перечень сокращений

Сокращение	Определение
LDAP	(англ. Lightweight Directory Access Protocol) - протокол прикладного уровня для доступа к службе каталогов
USB	(англ. Universal Serial Bus) — «универсальная последовательная шина», последовательный интерфейс для подключения периферийных устройств к вычислительной технике
АМДЗ	Аппаратный модуль доверенной загрузки
ОТ	Охрана труда
ПО	Программное обеспечение
Пул	Логический объект СХД, объединяющий пространства нескольких физических накопителей в единое пространство хранения данных
СВТ	Средства вычислительной техники
СХД	Система хранения данных
ТБ	Техника безопасности
ЦОД	Центр обработки данных