Программное обеспечение «Базис.Virtual Protect». Руководство по установке. Версия 1.6.1

RU.НРФЛ.00009-01.96.01

Москва

29/02/2024

Содержание

1 Аннотация

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

2 Назначение руководства

Настоящее руководство по установке содержит инструкции по выполнению следующих работ:

- подготовка к установке ПО;
- установка и настройка ПО;
- проверка доступности интерфейса управления;
- первичная проверка работоспособности.

3 Перечень эксплуатационных документов

Дополнительно к настоящему документу технические администраторы должны использовать следующие документы:

- «ПО «Базис.Virtual Protect». Руководство по эксплуатации. RU.НРФЛ.00009-01 97 01;
- «ПО «Базис.Virtual Protect». Руководство администратора RU.НРФЛ.00009-01 95 01.

4 Идентификационные данные документа

Идентификационные данные ПО	**Программное обеспечение «Базис.Virtual Protect»**
Название документа	«ПО «Базис.Virtual Protect». Руководство по установке»
Обозначение документа	RU.НРФЛ.00009-01 96 01
Автор документа	ООО «БАЗИС»

ПО поставляется "упакованным" в контейнеры и в зависимости от архитектуры системы заказчика, на которую устанавливается ПО, развертывается одним из способов:

- единственный узел управления (УУ) - с помощью приложения docker-compose;
- кластер - с помощью диспетчера пакетов Helm для Kubernetes (helm чарт, helm чарт тоже может быть выгружен в репозиторий заказчика).

5 Системные требования

Установка, обновление и удаление ПО "Базис.Virtual Protect" выполняется инженером по внедрению или системным администратором ОП, имеющим необходимый уровень подготовки и определенную квалификацию.

Допускается комбинированное взаимодействие между инженером по внедрению и системным администратором, предполагающее ассистирование с передачей основных навыков, которые потребуются в дальнейшем – на этапе пробной эксплуатации и/или после перевода облачной инфраструктуры в непрерывную эксплуатацию (т.н. производство или продакшен).

Требования, предъявляемые к выбору (системного) администратора, подробно изложены в документе «ПО «Базис.Virtual Protect». Руководство администратора RU.НРФЛ.00009-01 95 01.

5.1 Аппаратные требования

Аппаратные средства размещаются в территориально-распределенном ЦОД.

5.2 Среда функционирования

Среда функционирования ПО «Базис.Virtual Protect» (далее – системное окружение) должна включать один из вариантов:

- развернутый кластер Kubernetes;
- Linux сервер с установленным приложением docker-compose.

5.3 Требования к стенду

5.3.1 Начальные условия

1. Версия Базис.DynamiX не ниже 3.8.8.
2. Организован доступ к cloudapi платформы Базис.DynamiX.
3. Организован доступ к registry с образами для Базис.Virtual Protect.
4. Организован root-доступ на узлы гипервизора Базис.DynamiX для установки модуля ядра.
5. Необходимо обеспечить сетевую доступность к Базис.DynamiX.
6. Необходимо обеспечить сетевую связанность с хранилищем и целевыми кластерами, которые необходимо резервировать.
7. Необходимо подключить NFS или любой другой с монтированием в локальную систему для резервирования дисков виртуальных машин.
8. Для организации хранения резервной копии кластеров необходимо S3-совместимое хранилище.

Допускается использование хранилища резервных копий vStorage.

> ⚠ Все сущности должны быть доступны друг другу.
> Все ресурсы должны иметь доступ во внешнюю сеть.

5.3.2 Виртуальная машина

Минимальные требования к виртуальной машине:

- 2 CPU;
- 4096 MB RAM;
- 50 GB disk.

5.3.3 Созданный кластер

Минимальные требования к созданному кластеру:

- 1 Master узел:
  - 2 CPU;
  - 2048 MB RAM;
  - 50 GB disk;
- 3 Worker узла:
  - 4 CPU;
  - 4096 MB RAM;
  - 100 GB disk.

5.3.4 Свободное пространство в ресурсной группе для min-IO

Минимальные требования к в ресурсной группе для min-IO:

- 2 CPU;
- 4096 MB RAM;
- 100 GB disk.

5.4 Хранилище резервных копий

Для хранения резервных копий используется объектное S3-совместимое хранилище (облачный сервис), обеспечивающее сохранение больших объёмов данных.
Кроме того, для такого хранилища свойственны безопасность, надежность и отказоустойчивость.

Альтернативно, может применяться высокопроизводительное хранилище объектов MinIO или другие системы, совместимые на уровне API с объектным хранилищем S3.
Основа API взаимодействия -- протокол HTTP.

5.5 Организационное обеспечение

Обеспечение физической сетевой инфраструктуры находится в зоне ответственности администратора сети и может включать в себя необходимость настройки и поддержания в исправном состоянии:

- физических коммутаторов;
- межсетевых экранов или маршрутизаторов;
- сетевых интерфейсов на серверных компьютерах (инфраструктурных узлах).

Следует провести определенные оргмероприятия по обеспечению безопасности доступа: к рабочему месту (АРМ) администратора; к инфраструктурным узлам; к инфраструктурному серверу.

При активной поддержке политики импортозамещения на выделенное СВТ (ПК или ТК) рекомендуется установить сертифицированную ОС, класс защищенности которой определяется специалистом по информационной безопасности эксплуатирующей организации (оператором облачной платформы).

6 Подготовка к установке

Предоставление доступа к публичным репозиториям образов на целевых кластерах.

Целевой кластер Kubernetes должен быть развёрнут предварительно.

Среда функционирования ПО «Базис.Virtual Protect» (далее – системное окружение) должна включать один из вариантов:

- развернутый кластер Kubernetes;
- выделенный сервер под управлением ОС Linux (docker-compose).

Веб-интерфейс средства управления (Dashboard), обеспечивающего операции администрирования (в подключаемых кластерах Kubernetes), обслуживается с помощью внутреннего механизма, встроенного в контейнер.
Собранный разработчиками ПО контейнер разворачивается с помощью утилиты **docker-compose**.

7 Установка ПО

ПО поставляется заказчику, упакованным в контейнеры и далее разворачивается на устройстве управления способом, соответствующим структуре УУ.

Структура УУ:

- кластер Kubernetes;
- вычислительный узел ВУ (развёртывание из контейнера).

7.1 Способы развёртывания

Если УУ представлен кластером, то ПО устанавливается с помощью Helm-чарта (из программного пакета), после чего дополнительно настраиваются параметры работы сервиса.

Если УУ представлен единичным вычислительным узлом, то ПО разворачивается с помощью docker-compose (из контейнера).

7.2 Развертывание ПО из контейнера

Ниже рассмотрен вариант развёртывания ПО «Базис.Virtual Protect», распространяемого в форме контейнеров. Для их получения потребуется доступ к сети Интернет и репозиторию (ресурсу Dokcer Registry).

Необходимо на выделенный сервер под управлением ОС Linux предварительно установить СПО Docker и Docker-compose, обеспечивающее поддержку *контейнеризации*, из стандартного репозитория операционной системы.

Фактически, образ упаковывается в файл архива (`virtualprotect.tar`), который принято называть *контейнером*.

Копирование загруженного образа – Docker-контейнера – на целевое устройство (выделенный сервер) осуществляется командой:

```
docker load < virtualprotect.tar
```

Логические связи между контейнерами сохраняются в конфигурационном файле `docker-compose.yml`. Ссылка на образ продукта указывается в секции — *services/api*, с помощью параметра "**image: <URL_образа>**". Например:

```
services:
    api:
    - image: hub.digitalenergy.online/virtualprotect/virtualprotect:1.6.1
```

Примечание

По умолчанию, для веб-интерфейса настроено использование порта 8080.

Запуск контейнера в работу осуществляется командой:

```
docker-compose up
```

или (в фоновом режиме)

```
docker-compose up -d
```

После успешного разворачивания контейнера станет доступным *веб-интерфейс*, доступ к которому осуществляется по ссылке: http://localhost:8080/

После выполнения входа в систему (авторизации) продукт готов к использованию.

7.3 Установка ПО (в кластере)

Установка ПО в кластере Kubernetes производится без хранилища бэкапов (по умолчанию). Это позволяет создать необходимое количество хранилищ и подключить их через Dashboard.

Выполните установку интерфейса управления (Dashboard) и настройку параметров, как изложено ниже.

Примечание

Установка инструмента в определённый кластер выполняется из интерфейса управления – операция выбирается из контекстного меню.

7.3.1 Установка Dashboard

Установка интерфейса управления – Dashboard – производится с помощью Helm-чарта. Helm – это *диспетчер пакетов*, который упрощает настройку и развертывание приложений в кластерах Kubernetes (для разработчиков и операторов). Чарт – это пакет для Helm, который содержит все определения ресурсов, необходимые для запуска приложения, инструмента или службы внутри кластера Kubernetes.

Необходимо в целевом кластере создать пространство имен:

```
kubectl create namespace dashboard
```

Развертывание релиза чарта выполняется командой:

```
helm install -n dashboard virtualprotect ./helm
```

В данном случае указывается вновь созданное пространство имён (`dashboard`) и непосредственно сам чарт – `virtualprotect`.

Внимание

Запускать развёртывание необходимо из корня репозитория, содержащего директорию `helm`.

При необходимости, можно создать файл с измененными значениями переменных `values.yaml` и запустить установку следующей командой:

```
helm install -n dashboard -f values.yaml virtualprotect ./helm
```

По завершении процесса установки будет выведена «заметка» (сообщение) о том, как запустить перенаправление (port-forward) до Dashboard.

Примечание

В параметрах по умолчанию установка контроллера ingress не производится.
Чтобы изменить это, необходимо создать файл `values.yaml` с измененными значениями переменных в разделе — *ingress:*.

7.4 Настройка параметров

Параметры работы сервиса настраиваются через переменные окружения, в разделе — *environment:* контейнера API (`docker-compose.yml`):

```
MONGO_URI=<DB host>
MONGO_DB_USERNAME=<DB username>
MONGO_DB_PASSWORD=<DB password>
MONGO_DATABASE=<DB name>
VP_PORT=<port>
JWT_SECRET=<string>
NOTIFY_SENDER=smtp
SMTP_HOST=<host>
SMTP_PORT=<port>
SMTP_USER=<user>
SMTP_PASSWORD=<smtppassword>
SMTP_ENCRYPT=ssl
```

Чтобы доставка почтовых сообщений была адресной, вместо test@yandex.ru укажите собственный адрес почтового ящика, зарегистрированный на E-mail сервисе (`Яндекс Почта`).

Кроме того, в Helm чарте требуется отредактировать раздел — *env:* (`values.yml`):

```
- name: "MONGO_DATABASE"
value: <DB name>
```

и т.д.

7.5 Проверка работоспособности ПО

Открывшийся интерфейс Dashboard означает успешную установку ПО.

Работоспособность ПО проверяется подключением к существующему кластеру Kubernetes (динамической инфраструктуре) и созданием тестовой резервной копии объекта,
а также обратной операцией (восстановлением объекта инфраструктуры из резервной копии).

8 Термины и определения

Термин	Определение
CRON	компьютерная программа в системах класса UNIX, использующаяся для периодического выполнения заданий в определённое время (автоматический запуск программ и скриптов на сервере в определённое время)
Docker	проект с открытым исходным кодом для автоматизации развертывания приложений в виде переносимых автономных контейнеров, выполняемых в облаке или локальной среде
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
MinIO	высокопроизводительное хранилище объектов MinIO. MinIO - высокопроизводительное решение для хранения объектов, которое предоставляет API, совместимый с S3, и поддерживает все основные функции S3
Чарт	пакет для Helm, который содержит все определения ресурсов, необходимые для запуска приложения, инструмента или службы внутри кластера Kubernetes

9 Перечень сокращений

В документе использованы следующие сокращения:

Сокращение	**Определение**
Kubernetes	K8S
ОП	Облачная платформа
ОС	Операционная система
ПАК ПК	Программно-аппаратный комплекс Программный комплекс
ПО	Программное обеспечение
СВТ	Средства вычислительной техники
СПО	Специальное программное обеспечение
ТК	Тонкий клиент
УУ	Узел управления
ЦОД	Центр обработки данных