Информация, необходимая для установки программного обеспечения

«Платформа Боцман Клик»

Москва 2023

Информация, необходимая для установки программного обеспечения

История изменений

Версия	Дата	Комментарий	Автор
1.0.0	13.03.2023	Создание документа	Повалкин Дмитрий

Оглавление

ГЛОССАРИЙ

Термин/сокращение	Определение
AlertManager	Компонент Prometheus, служит для запуска оповещений через Email, Slack или другие клиентские уведомления
Ansible	Продукт с открытым кодом, который автоматизирует подготовку облачных решений, управление конфигурацией и развертывание приложений
Cilium	Программное обеспечение с открытым исходным кодом для обеспечения, защиты и наблюдения за сетевым подключением между рабочими нагрузками контейнеров, созданное в облаке и основанное на технологии ядра eBPF
CIS Benchmarks	Набор рекомендаций по настройке широкого спектра ПО (серверное, операционные системы, облачное ПО, десктопное ПО)
Docker	Проект с открытым исходным кодом для автоматизации развертывания приложений в виде переносимых автономных контейнеров, выполняемых в облаке или локальной среде
Hubble	Передовая доступная система управления безопасностью разработки, созданная для достижения наилучших результатов в области безопасности разработки
Hashicorp Terraform	Средство IaC с открытым кодом для подготовки и управления облачной инфраструктуры
Grafana	Аналитическая платформа с открытым исходным кодом, которая позволяет опрашивать и визуализировать данные, отправлять предупреждения и разбираться в метриках независимо от того, где они хранятся
Loki	Набор компонентов для полноценной системы работы с логами
Longhorn	Распределенное блочное хранилище для K8s
Prometheus	Бесплатное программное приложение, используемое для мониторинга событий и оповещения
Yandex CSI	Технология позволяет динамически резервировать бакеты S3-совместимых хранилищ и монтировать их к подам кластера в виде постоянных томов Kubernetes (PersistentVolume)
CD	Непрерывное развертывание
CI	Непрерывная интеграция
CIS	Center for Internet Security – Центр Интернет Безопасности, некоммерческая организация, продвигающая передовые решения в области информационной безопасности
Configuration as Code (CaC), Infrastructure as Code (IaC)	Конфигурация в виде кода/ Инфраструктура в виде кода Определяет параметры конфигурации и инфраструктуры в удобочитаемом YAML-файле, который может храниться в виде исходного кода
cypher_key	Ключ шифрования
DNS	Система доменных имен
Docker	Программное обеспечение с открытым исходным кодом для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации
Helm	Менеджер пакетов для Kubernetes
Hubble UI	Расширение Cillium, позволяющее схематично визуализировать потоки данных сетевого уровня
Ingress	Модуль управления внешними подключениями к кластеру

Kubernetes, k8s	Платформа с открытым исходным кодом для управления кластером контейнерных приложений и сервисов
kubectl	Инструмент командной строки для управления кластером Kubernetes
Pod	Термин нотификации Kubernetes, объединяющий в себе перечень контейнеров приложения с общими ресурсами хранения и сетевыми ресурсами
RBAC	Метод регулирования доступа к компьютерным или сетевым ресурсам на основе ролей отдельных пользователей
S3	Simple Storage Service. Протокол передачи данных
S3-хранилище	Объектное хранилище. Позволяет хранить большие объемы данных в исходном формате без иерархии и разбивки на отдельные каталоги. Не имеет ограничений по масштабированию
ssh_key	Учетные данные для доступа по протоколу ssh
Stateless	Сервис без сохранения состояния
Terraform	Инструмент декларативного управления инфраструктурой
VMware	Технология виртуализации сервера
VShpere	Платформа виртуализации облачных вычислений от VMware
YAML	Формат предствления данных, доступный для восприятия конечным пользователем
АРМ	Автоматизированное рабочее место - место работы оператора ПК
Кластер	Набор из нескольких серверов (узлов), на которых установлены компоненты среды контейнерной оркестрации
Контейнер	Экземпляр исполняемого программного обеспечения, объединяющий двоичный код приложения со связанными файлами конфигурации, библиотеками, зависимостями и средой выполнения
Контейнеризация	Технология изоляции процессов на основании пространства имен и групп пользователей операционной системы
Оркестрация контейнеров	Автоматизация и управление жизненным циклом контейнеров и услуг: автоматизация планирования, развертывания, масштабируемости, балансировки нагрузки, доступности и организации сетей контейнеров
ОС	Операционная система
Пространство имен	Множество, объединяющее модель, абстрактное хранилище или окружение, созданное для логической группировки уникальных идентификаторов (имен)
Платформа	Платформа Боцман Клик
ПО	Программное обеспечение
Репозиторий	Место хранения и поддержки структурированных данных
Секрет	Любая конфиденциальная информация. Например: логин, пароль, ключ и пр.
ЯндексОблако, YandexCloud, ЯО	Публичная облачная платформа

1. АННОТАЦИЯ

Настоящая инструкция содержит информацию по установке комплексной автоматизированной «Платформы Боцман Клик».

Платформа — это совокупность программных средств, обеспечивающих комплексное управление кластеров kubernetes с набором готовых инструментов для развертывания, мониторинга, балансировки нагрузок, автомасштабирования, строгих политик безопасности и резервного копирования.

Платформа предназначена для создания и управления виртуальным частным облаком и может применяться во всех индустриях.

2. ОБЩАЯ ИНФОРМАЦИЯ

1.1 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ ДЛЯ ЗАПУСКА УСТАНОВЩИКА

- На АРМ оператора должен быть установлен docker
- Сетевой доступ АРМ оператора до целевой площадки
- Подготовленное S3 хранилище для состояний кластера
- Подготовка Яндекс облака или vSphere
- Компоненты установщика

1.2 КОМПОНЕНТЫ УСТАНОВЩИКА

- Приложение Bootsman
  С его помощью производятся все манипуляции с кластером
- Файл конфигурации config.yml
  Хранение настроек для инсталятора
- Ключ шифрования cypher_key
- Ключ шифрования файла-состояния в S3.
  Должен быть сохранен, при утрате дальнейшее управление кластером с помощью приложения - невозможно.
  Ключ должен быть 32х символьным
- Приватный ssh-ключ
  Ключ для подключения к компонентам кластера
- Образ подготовленной виртуальной машины (Для VMware)
  Используется как шаблон для создания всех узлов

1.3 ТРЕБОВАНИЯ К СРЕДЕ УСТАНОВКИ И ФУНКЦИОНИРОВАНИЯ ПЛАТФОРМЫ

Платформа работает под управлением следующих операционных систем:

Операционная система	**Версия системы**	**Версия ядра**
RedOS	MUROM (7.3.2)	5.15
Ubuntu	Focal/Jellyfish	5.4/5.15

В качестве аппаратного обеспечения Платформы используются:

- VMware vSphere версии гипервизора не ниже 7.0.3
- Yandex Cloud

Каждая инсталляция включает в себя создание следующих типов узлов:

- Bastion
  Точка входа в кластер. Обеспечивает защиту и используется как прокси для ssh подключений. Обладает инструментами для управления кластера
- Master
  Узлы обеспечивающие работоспособность кластера
- Worker
  Узел обслуживающие полезную нагрузку

Для обеспечения отказоустойчивости минимальная конфигурация состоит из: Bastion, трех Master- и двух Worker-узлов

Количество узлов в кластере оркестрации контейнеров для приложений определяется требованиями к вычислительным ресурсам прикладного ПО с учетом факторов резервирования и механизмов обновления.

1.4 ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К УЗЛАМ

Число узлов, а также их конфигурация определяется требованиями прикладного ПО с учетом факторов резервирования и обновления.
Ниже представлены минимальные требования к узлам для их функционирования.

Master

Параметр	**Минимальная конфигурация**
CPU (vCPU)	4
RAM (GB)	8
Storage (GB)	32

Worker

Параметр	**Минимальная конфигурация**
CPU (vCPU)	4
RAM (GB)	8
Storage (GB)	60

Bastion

Параметр	Минимальная конфигурация
CPU (vCPU)	2
RAM (GB)	4
Storage (GB)	30

1.5 ТРЕБОВАНИЯ К ТОПОЛОГИИ СЕТИ

1. Узлы должны принадлежать одной сети
2. Узлы должны иметь доступ к ресурсам в сети интернет, указанным далее по тексту

1.6 ТРЕБОВАНИЯ ДОСТУПНОСТИ РЕСУРСОВ

В процессе установки потребуются дополнительные компоненты, доступность которых определяется в зависимости от выбора Операционной системы:

Ubuntu 20.04

Ресурс	Описание
http://archive.ubuntu.com/ubuntu	Основной репозиторий для ubuntu 20.04
http://security.ubuntu.com/ubuntu	Репозиторий с обновлениями безопасности
https://download.docker.com	Репозиторий с docker
https://get.helm.sh	Инструмент Helm
https://storage.googleapis.com	Инструмент kubectl
https://docker.io	Репозиторий Docker контейнеров
https://github.com/rancher/rke/releases/download	Инструмент rke
https://git.stsoft.team	git&helm репозиторий stsoft
https://charts.rancher.io/	Helm репозиторий rancher
registry.terraform.io	Репозиторий операторов terraform

Ubuntu 22.04

Ресурс	Описание
http://mirror.yandex.ru/ubuntu	Основной репозиторий для ubuntu 22.04
http://security.ubuntu.com/ubuntu	Репозиторий с обновлениями безопасности
https://download.docker.com	Репозиторий с docker
https://get.helm.sh	Инструмент Helm
https://storage.googleapis.com	Инструмент kubectl
https://docker.io	Репозиторий Docker контейнеров
https://github.com/rancher/rke/releases/download	Инструмент rke
https://git.stsoft.team	git&helm репозиторий stsoft
https://charts.rancher.io/	Helm репозиторий rancher
registry.terraform.io	Репозиторий операторов terraform

RedOS

Ресурс	Описание
https://repo1.red-soft.ru	Репозиторий RedOS
https://get.helm.sh	Инструмент Helm
https://storage.googleapis.com	Инструмент kubectl
https://docker.io	Репозиторий Docker контейнеров
https://github.com/rancher/rke/releases/download	Инструмент rke
https://git.stsoft.team	git&helm репозиторий stsoft
https://charts.rancher.io/	Helm репозиторий rancher
registry.terraform.io	Репозиторий операторов terraform

1.7 УСТАНАВЛИВАЕМОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ НА УЗЛЫ КЛАСТЕРА

В процессе установки на узлы кластера устанавливается следующее базовое ПО:

Ubuntu	Redos
cloud-init	cloud-init
openssh-server	openssh-server
nfs-common	nfs-utils
python3-pip	python3-pip
lvm2	lvm2
open-iscsi	iscsi-initiator-utils
net-tools	net-tools
htop	htop
vim	vim
tmux	tmux
ncdu	ncdu
tcpdump	tcpdump
strace	strace
tree	tree
iftop	iftop
nano	nano
traceroute	traceroute
nmon	nmon
mtr	mtr
iotop	iotop
mc	mc
snapd	snapd
wget	wget
curl	curl
lsof	lsof

Ubuntu	Redos
rsync	rsync
python3-setuptools	python3-setuptools
zsh	zsh
apt-transport-https	
ca-certificate	ca-certificates
software-properties-common	
virtualenv	python3-virtualenv

1.8 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ УСТАНАВЛИВАЕМОЕ НА УЗЛЫ ПО РОЛЯМ

Master- и Worker-узлы

Ubuntu	RedOS
docker-ce 5:20.10.23~3-0~ubuntu-bionic	docker-ce 3:20.10.10-1.el7
docker-ce-cli 5:20.10.23~3-0~ubuntu-bionic	docker-ce-cli 1:20.10.10-1.el7
containerd.io 1.6.16-1	containerd.io 1.5.8-2.el7

Bastion

Ubuntu/RedOS
Helm
kubectl

2 УСТАНОВКА ПЛАТФОРМЫ

2.1 ПОДГОТОВКА ПЛОЩАДОК ДЛЯ УСТАНОВКИ ПЛАТФОРМЫ*

vSphere	Yandex Cloud
Загрузить базовый образ (.iso) ubuntu или redos в кластер	Подготовить Cloud и Fodler для инсталяции
Создать ResourcePool для инсталяции	Создать сервис-аккаунт с правами editor, и создать авторизационный ключ
	Получить свой OAuth токен

*В контексте настоящего руководства предварительная настройка vSphere и Yandex Cloud не рассматривается.

2.2 КОНФИГУРАЦИОННЫЙ ФАЙЛ

```
# Тип провайдера, yc - ЯО, vsp - vSphere
cloudId: yc
# Абсолютный путь до приватного ssh-ключа
privateKeyPath: /id/rsa/path
# Настройки для подключения к s3 хранилищу
s3:
  # Адрес к хранилищу
  endpoint: localhost.localdomain
  # Включить SSL
  secure: true
  # Имя ключа для подключения
  accessKeyId: 2345defgh
  # Секрет для подключения
  secretAccessKey: 12345678
  # Имя бакета
  bucketName: "bucket-name"
  # Директория для хранения state-файла внутри s3-бакета. Должен быть
уникальным для каждого кластера.
  prefixFolder: "bootsman-1"
cloudConfig:
  # Путь до kubecofig
  k8sKubeConfig: "~/.kube/config"
  # Базовое доменное имя
  domainSuffix: soft-s.tech
  # Доменное имя для Rancher. Без указание протокола (http/https)
  rancherWebHostname: bootsman-test.soft-s.tech
  # Системный пользователь
  rkeUser: bootsman
  # Registry proxy
  registryProxy: "https://registry.bootsman.local"
infrastructure:
  # Используемая операционная система. "redos" или "ubuntu"
  os: ubuntu
  # Название сети, в которой будет работать кластер. В ЯО - сеть будет
создана, в vSphere сеть должна существовать
  resVpcNetworkName:
```

```
  # Настройка Узлов
  instances:
    # Тип хранилища. Только для ЯО
    diskType: network-ssd
    bastion:
      # Число vCPU
      cores: 2
      # Объем оперативной памяти, GB
      memory: 4
      # Объем дискового пространства, GB
      diskSize: 30
    master:
      # Число Master-узлов. Должно быть 3 и более, причем должно быть
нечетным
      count: 3
      # Число vCPU
      cores: 4
      # Объем оперативной памяти, GB
      memory: 8
      # Объем дискового пространства, GB
      diskSize: 32
    worker:
      # Число Worker-узлов. Возможный минимум - 1. Рекомендуемый минимум - 2,
для обеспечения отказоустойчивости.
      count: 2
      # Число vCPU
      cores: 4
      # Объем оперативной памяти, GB
      memory: 8
      # Объем дискового пространства, GB
      diskSize: 60
    # Дополнительный узел для ЯО
    frontend:
      # Число vCPU
      cores: 2
      # Объем оперативной памяти, GB
      memory: 6
      # Объем дискового пространства, GB
      diskSize: 40

# Настройки для подключения к ЯО
yandex:
  # Авторизационный ключ ЯО (Создать в web-интерфейсе яндекс облака и скачать
в виде json)
  keysData: '{}'
  # id folder в ЯО
  folderId:
  # Зона доступности ЯО. Варианты: ru-central1-a, ru-central1-b, ru-central1-
c
  providerZone:
  # Токен для авторизации в ЯО
  oAuthToken:
  # id целевого клауда в ЯО
  cloudId:
  # Идентификатор образа
  img:

# Настройки для подключения в vSphere
vsphere:
  # Имя пользователя vSphere
  login:
```

```
  # Пароль пользователя
  password:
  # Web-адрес vSphere
  baseUrl: http://10.0.1.10
  # Имя датацентра
  datacenter: "vSAN Datacenter"
  # Используемый Resource Pool. Он должен быть преднастроен
  resourcePool: "bootsman_ts"
```

2.3 ЗАПУСК И ПРОЦЕСС УСТАНОВКИ

Запуск процесса установки осуществляется посредством интерфейса командной строки.

Все операции, связанные с установкой и базовым обслуживанием, выполняются на АРМ Оператора, в директории расположения файла bootsman.

Перед запуском следует отредактировать config.yml

```
Перед запуском следует отредактировать config.yml
Подготовить ключ шифрования вручную или командой:

echo $RANDOM | md5sum | head -c 32 > cypher_key

Запустить инсталяцию

./bootsman up

Вывод успешного выполнения инсталяции

# Инициализация провайдеров terraform
2023/02/16 14:06:50 Initialization infrastructure
# Генерация промежуточного файла конфигурации hosts.cfg
2023/02/16 14:06:59 Generate hosts
# Проверка terraform-инструкций
2023/02/16 14:06:59 Initialization infrastructure.
# Подготовка конфигурации
2023/02/16 14:07:00 Initialization infrastructure..
# Применение terrform-инструкций
2023/02/16 14:07:00 Building infrastructure
# Запуск проверки состояния созданных виртуальных машин
2023/02/16 14:07:44 Building infrastructure.
# Успешное создание виртуальных машин
2023/02/16 14:08:26 Successfully created bastion at 158.160.8.2
2023/02/16 14:08:28 Successfully created master-0 at 192.168.142.20
2023/02/16 14:08:31 Successfully created master-1 at 192.168.142.14
2023/02/16 14:08:33 Successfully created master-2 at 192.168.142.31
2023/02/16 14:08:36 Successfully created worker-0 at 192.168.142.5
2023/02/16 14:08:42 Successfully created worker-1 at 192.168.142.38
2023/02/16 14:08:43 Successfully created worker-2 at 192.168.142.30
# Установка требуемых пакетов на Master и Worker узлы
2023/02/16 14:08:43 Configurating servers
2023/02/16 14:11:21 Configurating servers.
# Установка docker на Master и Worker узлы
2023/02/16 14:11:21 Configurating docker
# Установка пакетов и инструментов на bastion
2023/02/16 14:13:55 Configurating bastion
# Загрузка контейнеров для кластера
2023/02/16 14:16:24 Preloading components
```

```
# Генерация cluster.yml для приложения rke
2023/02/16 14:25:36 Generating k8s cluster config
# Создание rke кластера
2023/02/16 14:25:57 Building k8s cluster
# Генерация kubeconfig и перенос на bastion
2023/02/16 14:36:16 Generating kubeconfig
# Установка CNI плагин cilium
2023/02/16 14:36:33 Install k8s network
# Установка драйвера хранилища
2023/02/16 14:39:31 Install storage driver
# Установка Rancher
2023/02/16 14:41:13 Install k8s components
# Установка мониторинга
2023/02/16 14:43:51 Install monitoring system
# Установка системы логирования
2023/02/16 14:47:15 Install logging system
# Установка и активация плагинов
2023/02/16 14:49:05 Install UI extention
# Сообщение об окончании установки
2023/02/16 14:52:18 Bootsman finished your infrastructure.
# Сообщение с сгенерированным паролем для входа
2023/02/16 14:52:18 Your bootstrap password is
MYss8YxsxgXZNIItjRZ661VayzAFDvgb
```

Платформа готова к работе.

Расширенный журнал установки "bootsman.log" создается и дополняется на ПК Оператора, в той же директории, где расположен установочный файл.