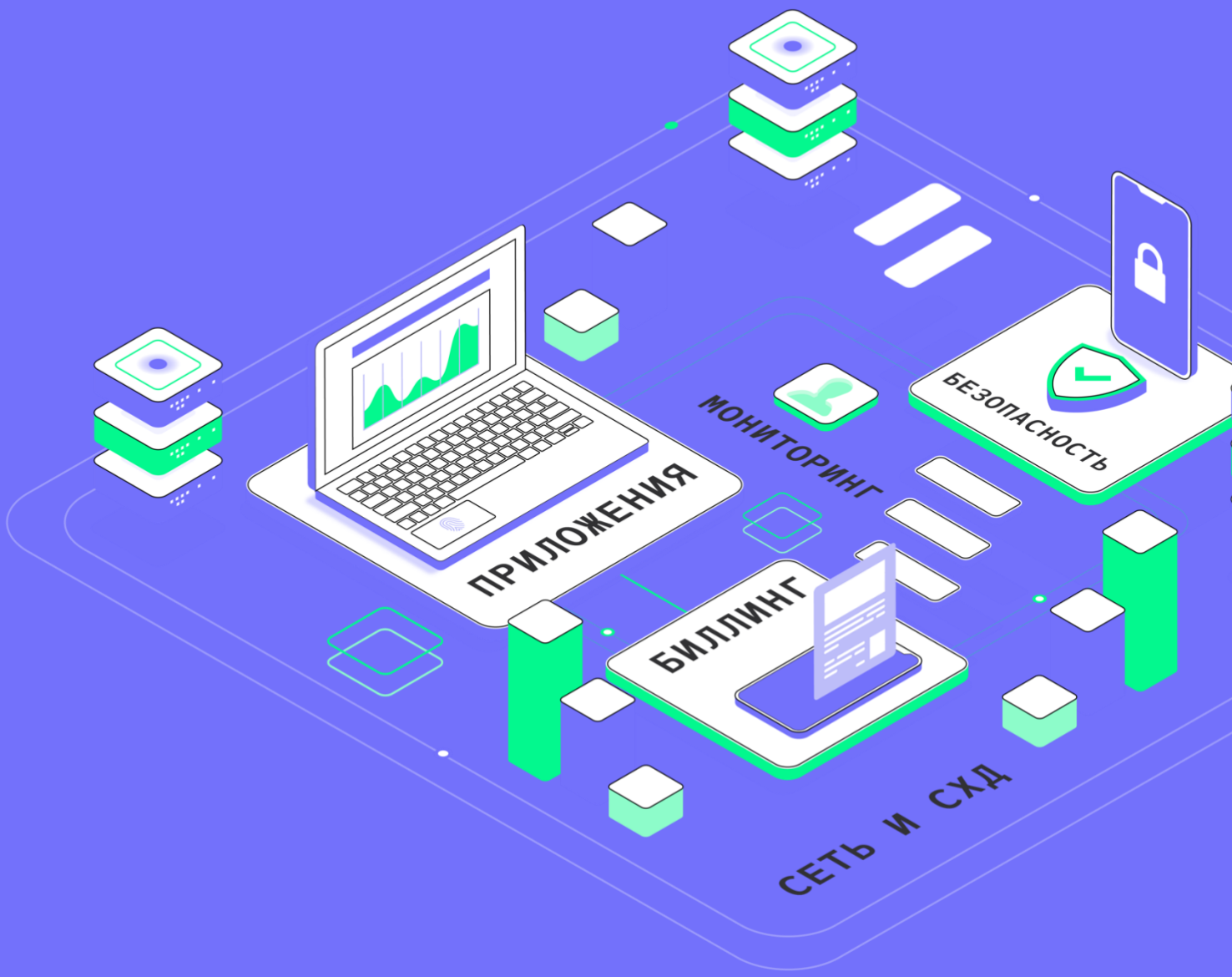
Боцман

bootsman.tech



White paper

Платформа «Боцман»

Предпосылки создания платформы «Боцман»

В недавнем отчете Forrester Wave говорится, что облачные технологии становятся предпочтительным способом для организаций создавать и модернизировать свои приложения и сервисы. Популярность контейнеров и Kubernetes продолжает расти, и, по прогнозам Gartner, к 2023 году более 75 % организаций по всему миру будут запускать контейнерные приложения в продуктивной среде. Этот прогнозируемый рост демонстрирует ценность облачных технологий, таких как Kubernetes, для корпоративных разработчиков и ИТ-операторов, использовать решения, которые помогут быстрее создавать приложения и управлять средами без ущерба для надежности, гибкости и безопасности.

Объединив свои ИТ-операции с Kubernetes, компании могут получить значительные преимущества, в том числе:

- обеспечивать высокий уровень надежности в любой инфраструктуре;
- повышение эффективности DevOps с помощью стандартизированной автоматизации;
- обеспечить применение политик безопасности в любой инфраструктуре.

Однако использование только одного Kubernetes может привести к накладным расходам и риску, с которым может столкнуться каждый заказчик:

- ручная настройка конвейера CI/CD – время и специалисты;
- отсутствие готовых сценариев YAML для масштабирования;
- необходимость интеграции удобной панели управления кластерами;
- нет расширенных политик безопасности;
- отсутствие вендорской поддержки с фиксированным SLA.

Инструменты платформы для управления виртуальным частным облаком должны покрывать:

- упрощенные кластерные операции: повышение эффективности DevOps за счет упрощенных кластерных операций;
- согласованную политику безопасности и управление пользователями;
- высокий уровень надежности при простом и последовательном доступе к общим инструментам и службам.

“The Forrester Wave™: Multicloud Container Development Platforms, Q3 2020” by Dave Bartoletti, Charlie Dai with Lauren Nelson, Duncan Dietz, Han Bao, Bill Nagel, Forrester

"Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024” by Susan Moore, Gartner.

Описание платформы «Боцман»

Платформа «Боцман»— это платформа для создания и управления мульти кластерами Kubernetes, которая предоставляет следующие ключевые функции:

- настроенный конвейер CI/CD;
- удобная панель управления на базе Prometheus и Grafana;
- политика безопасности и управление пользователями — расширенный RBAC, CIS Benchmark и Alertmanager;
- каталог приложений и набор инструментов для разработчиков;
- вендорская поддержка в соответствии с SLA.

Платформа «Боцман» позволяет управлять мульти кластерами kubernetes с набором готовых инструментов для:

- развертывания;
- мониторинга;
- балансировки нагрузок;
- автомасштабирования;
- строгих политик безопасности;
- резервного копирования.

Одно из ключевых преимуществ решения — это поддержка от разработчика программного обеспечения, что позволит заказчикам иметь решение с согласованным SLA на решение инцидентов.

Разворачивание платформы «Боцман» в части архитектуры — возможно как в:

- Яндекс Облаке;
- на инфраструктуре Заказчика (Bare Metal);
- программно-аппаратный комплекс на базе инфраструктуры Аквариус.

В составе решения платформы «Боцман» используются инструменты открытого программного обеспечения, позволяющие выполнять такие операции по управлению мульти кластерами Kubernetes, как:

- Provisioning;
- Обновления;
- Бэкап;
- Тестирование;
- RBAC.

При этом, пользовательский интерфейс позволит использовать:

- каталог приложений;
- Kubectl;
- API;
- CLI.

Сравнение платформ

В этом анализе мы используем «шар», чтобы проиллюстрировать, как сравниваются решения от разных вендоров по категориям:

- ● — «полный шар» отражает лучшие показатели в своем классе в этой категории;
- ◕ — «шар в три четверти» присуждается второму месту в этой категории;
- ◑ — «полушар» иллюстрирует приемлемые возможности в этой категории;
- ◔ — «четверть шара» отражает слабые возможности в этой категории;
- ○ — «пустой шар» указывает на то, что платформа не обладает технологиями в данной категории.

1. Операции с кластером

Операция	«Боцман»	Openshift	Tanzu
Простота установки, настройки и обслуживания	●	◕	◕
Интуитивно понятный пользовательский интерфейс	●	●	◕
Мультиоблачность	●	◕	◕
Мультикластеры	●	◑	◕
Edge Поддержка	●	◔	◔
Поддержка Hosted Kubernetes	●	◔	◑
Bare Metal, OpenStack & vSphere	●	◕	◑
Импорт существующих кластеров	●	◕	◕
Высокая доступность	●	●	◕
Балансировка нагрузки	●	◑	◑
Централизованный аудит	●	◕	◑
Самообслуживание Provisioning	●	◑	◑
Личный реестр и управление изображениями	●	●	●
Обновления кластера и управление версиями	●	●	◑
Поддержка хранения	●	◕	●
Поддержка архитектуры ARM	●	○	○
Поддержка Airgap	●	◕	◕
ETCD Резервное копирование и восстановление	●	◑	◕

2. Политика безопасности и управление пользователями

Операция	«Боцман»	Openshift	Tanzu
Активная директория и поддержка LDAP	●	●	●
Политики безопасности сети и подов	●	◕	◑
Соблюдение и отслеживание CIS Benchmark	●	◕	◑
Глобальные RBAC политики	●	◑	◕

3. Инструменты и сервисы

Операция	«Боцман»	Openshift	Tanzu
Каталог приложений	●	●	◑
Provision с конфигуратором	●	◑	◑
Интеграция с решениями CI/CD	●	●	◑
Расширенный мониторинг	●	●	◑
Оповещения и уведомления	●	●	◔
Отправление внешних логов	●	●	◑
Поддержка интегрированного Service Mesh	●	◕	◔
SLA Enterprise уровня	●	◑	◑

3.1 Операции с Кластером

3.1.1 Простота установки, конфигурирования и обслуживания:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 3**

«Боцман»

«Боцман» работает в любом сертифицированном дистрибутиве Kubernetes — от облака до ядра и на периферии. Для пограничных развертываний «Боцман» не нужны контейнеры Docker при использовании с такими дистрибутивами, как K3s и Cluster API. Боцман может использовать операционную систему, такую как Ubuntu, RedOS, Astra чтобы помочь запустить Kubernetes наиболее эффективным из возможных способов. Kubernetes Cluster API использует синтаксис конфигурации, разработанный для обеспечения прозрачности и динамической реконфигурации кластера без простоев.

OpenShift

OpenShift Container Platform (OCP) состоит из установочного бинарного файла, который работает с Terraform и набором скриптов для развертывания OCP4. Руководство по установке предоставляется для поставщиков общедоступных и частных облачных сервисов, наряду с руководствами для bare metal и «любого другого поставщика». Установщикам облачных провайдеров требуется доступ администратора к среде для создания ресурсов, но после завершения установки они могут работать без доступа администратора. Простой запуск бинарного файла, поскольку во время запуска доступно минимальное количество опций для настройки кластера. Вся настройка происходит из OCP4 после того, как кластер подключен к сети. OCP4 требует минимум три ноды управления и две или более рабочие ноды, плюс загрузочную ноду для установки, которая может быть удалена после подключения кластера к сети. Ноды bootstrap и control plane должны работать под управлением Red Hat Enterprise Linux CoreOS.

Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) поставляется с инсталлятором, который запускается с локального компьютера. Установка кластера управления TKG и кластеров приложений происходит через графический интерфейс установщика или с помощью директив командной строки, которые используют файл конфигурации YAML. Кластеры могут запускаться только на нодах vSphere, Amazon EC2 или Microsoft Azure. Нижестоящие кластеры Kubernetes устанавливаются только через CLI. Обновления привязаны к версии TKGI CLI и требуют, чтобы пользователи загружали и устанавливали виртуальные машины и шаблоны базовых образов перед выполнением обновлением кластера . Исключением из этих правил является случай, когда в среде используется Tanzu Mission Control (TMC), SaaS-предложение VMware для управления кластерами. Если это так, то TMC действует как кластер управления и может предоставлять нижестоящие кластеры TKG и управлять ими.

3.1.2 Intuitive UI — интуитивно понятный пользовательский интерфейс:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 3**

«Боцман»

Обновленный интерфейс «Боцмана» позволяет пользователям быстро развертывать кластеры Kubernetes и начинать управлять ими практически без необходимости обучения. Он был разработан с использованием подхода, основанного на логике, для смягчения и оптимизации сложных концепций и рабочих процессов Kubernetes, что позволяет использовать Kubernetes в организации без предварительной подготовки.

OpenShift

Пользовательский интерфейс OpenShift простой и понятный. Общие рабочие процессы находятся в верхней части меню, и легко доступен доступ как к стандартным рабочим процессам Kubernetes, так и к тем, которые уникальны для OpenShift.

Tanzu

KGI не поставляется с интерфейсом управления. Вместо этого VMware предлагает визуальное управление кластером с помощью SaaS-продукта под названием Tanzu Mission Control (TMC). TMC является частью облачных сервисов VMware. TMC имеет хорошо продуманный пользовательский интерфейс, который поставляется в двух версиях: стандартной и расширенной. Стандарт TMC содержит сокращенный набор функций для управления безопасностью и политиками для управления доступом на основе ролей (RBAC), квот, CIS Benchmark и других важных областей.

3.1.3 Intuitive UI — интуитивно понятный пользовательский интерфейс:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 3**

«Боцман»

«Боцман» представляет наибольшее количество вариантов развертывания Kubernetes. Он может предоставлять размещенные решения в основных облачных провайдерах. Он может предоставлять вычислительные ресурсы любого провайдера, для которого существуют драйверы для рантайма containerd, а затем устанавливать Kubernetes в эту среду. Он может импортировать существующие кластеры Kubernetes, работающие на любом провайдере. «Боцман» также предлагает опцию bare-metal для установки Kubernetes на любую систему, созданную с помощью других средств, таких как Ansible, Terraform, Puppet, Chef и др.

OpenShift

OpenShift предоставляет руководства по установке для AWS, GCP, Azure, IBM Cloud и VMware Cloud. Каждый кластер должен быть установлен независимо от других и существовать автономно.
Нет возможности развертывания рабочих нод в нескольких облаках для одного кластера. Все ноды управления должны работать под управлением Red Had Enterprise Linux CoreOS. Единственное опубликованное решение для соединения рабочих нагрузок в разных кластерах использует Submariner, проект, совместно разработанный инженерами SUSE и Red Hat. Отсутствие Kubernetes и агностицизм дистрибутива ОС в OpenShift продолжает представлять угрозу блокировки для клиентов.

Tanzu

Tanzu — это многокластерное и многооблачное решение, обеспечивающее согласованную работу. Однако его самые сильные функции, такие как Tanzu Mission Control (TMC), предоставляются только через опции SaaS. Это повышает риск lock-in и затрудняет смену платформы в будущем. Кроме того, поддерживается только часть провайдеров публичного облака, что ограничивает выбор Заказчика.

3.1.4 Multi-cluster:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 3**

«Боцман»

«Боцман» предоставляет функциональность Kubernetes через пользовательский интерфейс и API. Это, в свою очередь, позволяет пользователям взаимодействовать с Kubernetes, не зная, где он находится и как он настроен. Кроме того, «Боцман» абстрагирует ресурсы, специфичные для облака, такие как управление идентификацией и доступом, и уменьшает блокировку, позволяя операторам применять стандартные политики безопасности для кластеров, работающих в разных облаках. «Боцман» также использует Longhorn для хранилища данных и обеспечения переноса приложений между облаками путем предоставления стандартного интерфейса к базовым элементам Kubernetes.

OpenShift

Клиенты Red Hat могут управлять несколькими кластерами Kubernetes только с помощью Red Hat Advanced Cluster Management for Kubernetes, дополнительной платной услуги подписки.

Tanzu

Tanzu Kubernetes grid может развертывать и поддерживать несколько кластеров с помощью Cluster API с открытым исходным кодом. Это включает локальные кластеры, работающие в vSphere, и кластеры, работающие в облачной инфраструктуре Amazon EC2 или Microsoft Azure. Кроме того, Tanju Mission Control может импортировать существующие кластеры, что является единственным способом поддержки популярных размещенных решений Kubernetes, таких как Amazon EKS, Google GKE или Microsoft AKS.

3.1.5 Edge Support:

- **«Боцман» → 4**
- **OpenShift → 1**
- **Tanzu → 1**

«Боцман»

K3s — это облегченный дистрибутив Kubernetes, первоначально разработанный SUSE для работы в удаленных средах с ограниченными ресурсами. В августе 2020 года K3s был принят в качестве проекта CNCF Sandbox для дальнейшего продвижения его в качестве наиболее широко распространяемого дистрибутива Kubernetes в своем роде.

Continuous Delivery (CD) — Fleet и расширенные возможности наблюдения обеспечивают максимальную согласованность кластера и оперативное понимание от ядра до облака и пограничных областей. Кроме того, Fleet позволяет Боцман поддерживать до миллиона кластеров с одной консоли со встроенными возможностями безопасности, используя любой дистрибутив Kubernetes, сертифицированный CNCF. Возможна настройка ArgoCD или другой системы.

OpenShift

Подход RedHat к запуску Kubernetes соответствует ее техническим и коммерческим ограничениям. Поддержка нескольких кластеров из одной консоли — новая концепция для RedHat, а OpenShift продолжает привязывать своих пользователей к сертифицированному дистрибутиву Kubernetes. Идея Kubernetes на границе заключается в развертывании пограничных центров обработки данных под управлением OpenShift, который управляет «немыми» конечными точками.

Tanzu

История Tanzu edge построена на базе vSphere Remote Office Branch Office (ROBO), в котором центральное развертывание центра обработки данных vCenter управляет периферийными точками, работающими под управлением vSphere с двухузловым кластером vSAN. Эти среды, в свою очередь, работают под управлением Tanzu Kubernetes Grid и удаленно управляются SaaS-решениями Tanzu Mission Control и Tanzu Observability.

3.1.6 Hosted Kubernetes Support — поддержка Kubernetes на хостинге:

- **«Боцман» → 4**
- **OpenShift → 1**
- **Tanzu → 2**

«Боцман»

«Боцман» поддерживает развертывание в управляемые решения Kubernetes от Yandex. Если пользователь захочет развернуть кластер с новым провайдером, он может импортировать драйвер для этого провайдера непосредственно из пользовательского интерфейса. «Боцман» предоставляет операторам полное управление жизненным циклом кластеров из одного окна. «Боцман» теперь может импортировать, предоставлять, обновлять, конфигурировать и защищать кластеры во всех трех средах непосредственно с помощью обновленного унифицированного, интуитивно понятного пользовательского интерфейса «Боцман».

Кроме того, управляемые «Боцман» развертывания поддерживают шаблонизацию и сканирование эталонов CIS для поддержания высокого уровня безопасности.

OpenShift

Red Hat OpenShift — это однокластерное решение без поддержки размещенных решений Kubernetes от какого-либо поставщика. За дополнительную плату Red Hat Advanced Cluster Management for Kubernetes (ACM) может импортировать и управлять предварительно созданными кластерами на EKS, GKE, AKS и IBM Cloud. Однако он не может создавать, обновлять или удалять кластеры на этих платформах.

Tanzu

Tanzu Mission Control поддерживает управление размещенными кластерами Kubernetes, но не может их развертывать или удалять. Вместо этого кластеры должны быть созданы непосредственно у хостинг-провайдера, а затем импортированы.

3.1.7 Bare Metal, OpenStack & vSphere:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 2**

«Боцман»

«Боцман» поставляется с драйверами для развертывания в обычных облачных провайдерах, таких как Yandex, VK. «Боцман» также поддерживает любого облачного провайдера, для которого существует драйвер containerd. Он также поставляется с драйверами для vSphere, что позволяет пользователям этих технологий развертывать Kubernetes наряду со своими существующими виртуальными машинами. Движку «Боцман» Kubernetes требуется только драйвер containerd, что делает его подходящим для развертывания на «голом железе» любого дистрибутива Linux.

OpenShift

OpenShift поддерживает развертывание на bare metal и vSphere.

Tanzu

Tanzu развертывает кластеры Kubernetes на инфраструктуре vSphere. vSphere также может развертывать на управляемых vSphere хостах ESXi с помощью собственных расширений VMware, которые заменяют контейнерный движок и стандартный kubelet Kubernetes.

3.1.8 Импортирование существующих кластеров:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 3**

«Боцман»

«Боцман» импортирует существующие кластеры Kubernetes, делая их доступными для управления в пользовательском интерфейсе. Эти кластеры могут быть запущены в облаке, у размещенного провайдера, на «голом железе» или виртуальных машинах или на любой другой платформе. Если в кластере запущена обновленная версия Kubernetes, «Боцман» может импортировать ее без каких-либо дополнительных действий. Однако, если в кластере запущена нестандартная версия Kubernetes (OpenShift, Tanzu и т.д.), для управления «Боцману» потребуется некоторая дополнительная конфигурация.

OpenShift

Red Hat ACM (дополнительная платная услуга) может импортировать существующие кластеры OpenShift.

Tanzu

Tanzu Mission Control (TMC) может импортировать кластеры от внешних поставщиков. TMC — это только SaaS-решение.

3.1.9 High Availability:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 3**

«Боцман»

«Боцман» позволяет пользователю выбрать конфигурацию узлов для control plane, etcd and workers, позволяя выбрать конфигурацию высокой доступности, которая лучше всего соответствует роли кластера в организации. Платформа также позволяет пользователю выбрать, в какой зоне доступности будут работать ноды. Кластеры, развернутые с помощью Cluster API, могут быть динамически перенастроены на конфигурации из 3, 5 и 7 узлов по мере изменения потребностей организации.

Провайдер обеспечивает высокую доступность и восстановление нод на уровне виртуальных машин: control plane, etcd and workers.

OpenShift

Всегда развертывает высокодоступный кластер Kubernetes с тремя нодами для control plane и etcd, независимо от рабочих нод.

Tanzu

Развертывание Kubernetes в Tanzu имеет два варианта по умолчанию — разработка или продуктив. Кластер разработки имеет однонодную плоскость управления / single-node control plane, а продуктивный кластер имеет 3-хнодную плоскость управления. При работе в облачной среде продуктивный кластер по умолчанию размещает каждую ноду в отдельной зоне доступности.

3.1.10 Load Balancing / балансировка нагрузки:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 2**

«Боцман»

Кластеры, установленные «Боцманом» на вычислительных нодах, включают контроллер NGINX Ingress для балансировки нагрузки. Если «Боцман» развертывает кластер на хостинг-провайдере, который не устанавливает ingress controller / контроллер ингресса по умолчанию, каталог приложений «Боцман» и интеграция Helm позволяют установить ingress controller одним щелчком мыши. Также будет установлена служба Load Balancer Service для конкретного провайдера по необходимости. Все стандартные решения и балансировка нагрузки (включая шлюзы API и служебные сети) совместимы с кластерами, развернутыми в «Боцмане».

OpenShift

OpenShift использует собственный программный ресурс балансировки нагрузки, называемый Route. Он ведет себя как Ingress, но существует только в OpenShift и не переносится на другие кластеры Kubernetes. Контроллеры OpenShift Ingress управляются оператором Ingress. Он развертывает стандартный балансировщик нагрузки на основе HAProxy для обработки запросов Route и Ingress. OpenShift заполняет пространство API, размещая Route (ресурс, специфичный для OpenShift) под "v1", что создает впечатление, что это обычный ресурс Kubernetes. Когда пользователь создает Ingress (стандартный ресурс Kubernetes), OpenShift использует инструкцию для создания Route вместо него. Эта перекрестная связь усложняет использование тех же манифестов Kubernetes в кластере, отличном от OpenShift.

Tanzu

Установки Tanzu Kubernetes Grid Integrated Edition (TKGI) на vSphere или VMware Cloud на AWS по умолчанию получают NSX Advanced Load Balancer (ALB) Essentials Edition. Это решение для балансировки нагрузки четвертого уровня, которое включает в себя оператора Kubernetes для управления жизненным циклом балансировки нагрузки и входящих ресурсов в кластере Kubernetes. К сожалению, NSX ALB требует отдельного контроллера и конфигурации кластера, что создает дополнительную нагрузку на операционную команду. Версия Essentials Edition предлагает ограниченный набор функций. Тем не менее, если одна развернутая среда захочет использовать расширенные функции контроллера Avi (NSX ALB), каждая подключенная среда должна быть залицензирована для поддержки функций контроллера Advanced или Enterprise.

3.1.11 Централизованный аудит:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 2**

«Боцман»

«Боцман» обновил свои возможности ведения логов и теперь использует оператор Loki для ведения логов на всей платформе.

OpenShift

OpenShift может регистрировать все взаимодействия с OCP API, включая тело запроса, ответа и метаданные. Эта информация записывается в файлы и может быть запрошена с помощью команды OS. Для этого необходимо знать хост и logfile для запроса. OpenShift также поддерживает стандартное протоколирование API, доступное в Kubernetes.

Tanzu

TKG поставляется с Fluent Bit для сбора и пересылки логов. Логи могут отправляться в Elasticsearch, Kafka, Splunk, syslog или конечную точку HTTP. Он также передает некоторые метрики в Prometheus и Grafana. Развертывание и настройка Fluent Bit — это ручной процесс, который должен происходить на каждом кластере Kubernetes.

3.1.12 Self-service Provisioning:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 2**

«Боцман»

«Боцман» использует детализированную схему разрешений для предоставления или запрета доступа к ресурсам на глобальном уровне, уровне кластера и уровне пространства имен. Пользователи с доступом к серверу «Боцман» будут видеть только свои собственные кластеры или проекты, а дополнительная изоляция пространства имен гарантирует безопасность многопользовательских кластеров. Делегирование привилегий означает, что глобальный администратор может предоставить другому пользователю разрешение на создание кластеров, которые могут видеть только он или его команда. Такое делегирование ответственности, а также параметры того, как и где развертываются кластеры, обеспечивают разработчикам доступ к необходимым ресурсам, гарантируя при этом безопасность всей среды. Предоставление кластеров Kubernetes может осуществляться через пользовательский интерфейс, CLI или API.

Администратор «Боцман» также может использовать шаблоны для стандартизации конфигураций кластеров. «Боцман» гарантирует, что каждый кластер, который он создает на основе шаблона, будет единообразным и последовательным.

OpenShift

OpenShift — это однокластерное решение, которое должно быть развернуто с помощью программы установки. Он не содержит средств для запуска новых кластеров. Однако Red Hat ACM (дополнительная платная услуга) может развернуть кластеры OpenShift в нескольких средах.

Tanzu

Авторизованные пользователи могут развертывать, настраивать и взаимодействовать с кластерами TKG с помощью плагина vSphere для kubectl. Самостоятельное развертывание также доступно через Tanzu Mission Control (TMC).

3.1.13 Частный реестр (registry) и управление образами:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 4**

«Боцман»

«Боцман» содержит полную поддержку частных реестров. Он предоставляет вкладку в пользовательском интерфейсе, где пользователи могут ввести свои учетные данные реестра. Они сохраняются как Kubernetes Secrets и используются при извлечении из частных реестров.

OpenShift

OpenShift содержит полную поддержку частных реестров и включает локальный реестр, используемый для локально созданных образов. Доступ к локальному реестру использует учетные данные запрашивающего пользователя при определении разрешений. Доступ к внешним реестрам использует oc CLI для создания ImagePullSecrets и, по желанию, прикрепляет их к учетным записям служб.

Tanzu

В vSphere с Tanzu встроен центральный реестр Harbor, который может быть включен на управляющем кластере. После настройки все последующие кластеры могут использовать его для частных образов.

Tanzu использует функции, доступные в Kubernetes для доступа к частным и аутентифицированным реестрам. Пользователи должны вручную создавать объекты учетных данных реестра и привязывать их к рабочим нагрузкам, которые будут их использовать.

3.1.14 Обновление кластера и управление версиями:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 2**

«Боцман»

«Боцман» Kubernetes Engine запускает Kubernetes в контейнерах containerd. Обновления отдельных служб Kubernetes могут выполняться атомарно, с полной поддержкой отката к предыдущим версиям. Все обновления Kubernetes выполняются с нулевым временем простоя работающих рабочих нагрузок.

Полное обновление 3-хнодного кластера займет около 10 минут. «Боцман» выпускает обновления безопасности в течение двух недель после выпуска командой Kubernetes и несрочные обновления Kubernetes в течение четырех недель.

«Боцман» также позволяет проводить обновления в средах не имеющих доступ к публичному Internet (air-gapped).

OpenShift

OpenShift использует операторы Kubernetes для развертывания и обновления компонентов кластера Kubernetes. Все обновления Kubernetes выполняются с нулевым временем простоя работающих рабочих нагрузок. Полное обновление 3-хнодного кластера займет около 15 минут.

Tanzu

TKGI поддерживает обновление кластера с помощью CLI. Обновления привязаны к версии TKG CLI и требуют, чтобы пользователи загрузили и установили виртуальные машины и шаблоны базовых образов перед выполнением обновления кластера. Обновление кластера заменяет виртуальные машины и должно быть выполнено сначала на кластере управления. В документации на нескольких страницах перечислены предварительные условия и задачи по перерегистрации после обновления, что может сделать процесс обновления сложным для администраторов кластера. Однако зависимость от сервера управления и количество необходимых шагов подразумевает, что обновление не будет удобным для пользователя.

Кластеры, развернутые через Tanzu Mission Control, можно обновлять через этот интерфейс.

3.1.15 Storage Support / поддержка хранения данных:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 4**

«Боцман»

«Боцман» использует Longhorn (SDS с открытым исходным кодом, управляемый CNCF).

OpenShift

Red Hat поддерживает хранилища in-tree и CSI для Kubernetes. Они также поставляют ребрендированный дистрибутив Rook, проекта с открытым исходным кодом, который обеспечивает хранение контейнеров через Ceph, и NooBaa, многооблачного программно-определяемого уровня хранения, который Red Hat приобрела в 2018 году. Кроме того, Red Hat поддерживает NooBaa, Ceph и GlusterFS и поэтому может реализовать специфические для OpenShift расширения для этих решений.

Tanzu

Рабочие нагрузки VMware vSphere с Tanzu могут использовать хранилище из vSphere. Кластеры Tanzu Kubernetes Grid поставляются с классами хранения для Amazon EBS, Azure Disk или vSphere Cloud Native Storage (CNS), а также NFS и iSCSI. TKG.

3.1.16 Arm support / поддержка:

- **«Боцман» → 4**
- **OpenShift → 0**
- **Tanzu → 0**

«Боцман»

«Боцман» поддерживает установку на Arm64 и Arm7, и имеет партнерские отношения с производителями Arm серверов и тесно сотрудничает с их командами инженеров при создании новых релизов.

OpenShift

OpenShift не поддерживает развертывание на процессорах Arm.

Tanzu

Tanzu не поддерживает развертывание на процессорах Arm.

3.1.17 Airgap support:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 3**

«Боцман»

«Боцман» поддерживает установку airgap и включает исчерпывающую документацию о том, как создать частный сервер реестра и заполнить его всеми образами, необходимыми для установки.

OpenShift

OpenShift поддерживает установку airgap только на инфраструктуре, предоставляемой пользователем. Он не поддерживает установку air gap на автоматически развернутой облачной инфраструктуре.

Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) поддерживает установку airgap. Перед выполнением установки рабочая станция, подключенная к Интернету, должна запустить сценарий для получения образов из Интернета и заполнения частного сервера реестра в среде airgap. После завершения этого этапа оператор может отключить подключение к Интернету и развернуть кластер.

3.1.18 Etcd backup and restore / резервное копирование и восстановление:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 3**

«Боцман»

Все кластеры, развернутые в «Боцман», автоматически резервируются на локальное хранилище через регулярные промежутки времени. Оператор может изменить это на S3-совместимую конечную точку. Кластеры могут быть восстановлены до любого снимка из пользовательского интерфейса или CLI. HA-развертывания в «Боцмане» требуют ручной настройки кластера для выполнения резервного копирования. Они также могут записываться в локальное хранилище или S3-совместимую конечную точку. Восстановление HA-кластера требует развертывания нового кластера Kubernetes, восстановления резервной копии и выполнения новой установки «Боцмана». По завершении все удаленные кластеры Kubernetes переподключатся к новому кластеру.

OpenShift

Резервное копирование кластера OCP4 требует ручного входа в узел управления и выполнения сценария. Хотя это можно автоматизировать с помощью cron, в нем не предусмотрено сохранение на удаленную конечную точку. В результате эффективное решение по резервному копированию будет зависеть от оператора, который будет его разрабатывать, устанавливать и поддерживать.

Tanzu

Tanzu рекомендует Velero, решение для резервного копирования с открытым исходным кодом, поддерживаемое VMware. Операторы могут установить Velero и создавать резервные копии метаданных кластера, конфигурации рабочей нагрузки и данных рабочей нагрузки. Эти резервные копии могут быть восстановлены в новом кластере. Например, Velero может создавать резервные копии рабочих нагрузок и данных пользователей на кластере управления TKG, но не может создавать резервные копии состояния самого кластера.

3.2 Безопасность, управление политиками и пользователями

3.2.1 Active Directory и Поддержка LDAP:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 4**

«Боцман»

«Боцман» напрямую интегрируется с Active Directory, Azure AD, OpenLDAP, FreeIPA, OAuth-провайдерами, такими как GitHub, и SAML-провайдерами, такими как Keycloak и Okta. Конфигурация интеграции происходит на глобальном уровне, после чего пользователи становятся доступными для назначения на роли RBAC.

OpenShift

OpenShift запускает внутренний OAuth-сервер и проксирует связь с несколькими внутренними провайдерами. Он поддерживает совместимость с провайдерами на основе LDAP, Keystone, OpenID Connect и OAuth, а также предоставляет интерфейс для базовой аутентификации и внешних систем аутентификации.

Tanzu

Tanzu Kubernetes Grid включает проект с открытым исходным кодом Pinniped, который обеспечивает аутентификацию по отношению к провайдерам, поддерживающим LDAP и OIDC.

3.2.2 Политики безопасности сетей и подов:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 2**

«Боцман»

«Боцман» поддерживает конфигурацию Pod Security Admission (PSA) на глобальном уровне. Шаблоны PSA затем назначаются нижестоящим кластерам. Это обеспечивает соответствие и снижает риск человеческой ошибки при изменении политик. PSA можно создавать и редактировать через пользовательский интерфейс. «Боцман» также поставляется с kyverno — решением с открытым исходным кодом для управления на основе политик для кластеров Kubernetes.

OpenShift

OpenShift использует Security Context Constraints для выполнения функции объекта Pod Security Policy в Kubernetes. Он содержит надежную реализацию SCC для кластера. SCC можно редактировать только с помощью команды oc в CLI. OpenShift включает поддержку сетевых политик и нескольких сетей pod для изоляции трафика. Он также обеспечивает операторам соответствие требованиям (через проект с открытым исходным кодом OpenSCAP) и целостность файлов (через проект с открытым исходным кодом AIDE).

Tanzu

Tanzu Kubernetes Grid Integrated Edition (TKGI) требует использования собственных политик безопасности PodSecurityPolicies (PSP) для развертывания рабочих нагрузок в кластере Kubernetes. Однако это может негативно повлиять на развертывания из Helm или операторов, которые либо не имеют настроенных PSP, либо запрашивают более высокий уровень доступа, чем предоставляет PSP по умолчанию. Кроме того, Pods, запущенные в vSphere, описываются как «несоответствующие» и не поддерживают PodSecurityPolicies.

TKGI использует Antrea (по умолчанию) или Calico для работы с сетью. Оба поддерживают встроенные NetworkPolicies Kubernetes, и оба также имеют свои собственные расширения сетевой политики.

Tanzu Mission Control (TMC) поддерживает как PSP, так и политики безопасности, навязываемые Open Policy Agent (OPA). Несмотря на открытый исходный код, VMware включает OPA Gatekeeper только в Advanced и более поздние версии TMC.

3.2.3 Настраиваемое соблюдение контрольных показателей безопасности CIS Benchmark:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 2**

«Боцман»

«Боцман» поддерживает сканирование CIS на любом кластере Kubernetes, включая Yandex, VK, bare-metal. Инструмент сканирования CIS легко доступен в пользовательском интерфейсе «Боцман» и может быть развернут с помощью диаграммы Helm.

OpenShift

Контрольные показатели CIS доступны для OpenShift в разделе CIS Kubernetes Benchmarks.

Tanzu

Сканирование безопасности на соответствие эталонам CIS для Kubernetes доступно через Tanzu Mission Control (TMC) или с помощью Compliance Scanner для VMware Tanzu (бывший Pivotal Compliance Scanner).

3.2.4 RBAC политики:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 3**

«Боцман»

«Боцман» позволяет конфигурировать и поддерживать политики RBAC на глобальном уровне в пользовательском интерфейсе. Политики существуют для уровней Global, Cluster и Project, и в дополнение к шаблонам, которые предоставляет «Боцман», пользователи могут создавать бесконечное количество шаблонов для определения новых ролей. Более того, пользовательские шаблоны могут наследоваться от существующих шаблонов для создания иерархии легко поддерживаемых разрешений.

OpenShift

OpenShift использует встроенную RBAC Kubernetes, управление которой осуществляется с помощью команды oc. Он не включает управление RBAC через пользовательский интерфейс.

Tanzu

Tanzu Mission Control (TMC) содержит конфигурацию RBAC для организации, кластерной группы и объектов пространства имен, хотя они не переведены непосредственно на объекты Kubernetes RBAC. Кластеры, развернутые с помощью Tanzu (TKG), поддерживают стандартные объекты Kubernetes с расширениями, которые привязываются к пользователям vCenter Single Sign-On или настроенному коннектору OIDC для кластера.

3.3 Общие инструменты и сервисы

3.3.1 Каталог приложений:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 2**

«Боцман»

Каталог приложений «Боцман» расширяет Helm, чтобы предоставить пользователям легко понятный процесс установки приложений. Кроме того, он интегрируется с любым внешним репозиторием Helm, предоставляя пользователям возможность устанавливать приложения из любой системы. Для включения в каталог приложений «Боцман» требуется Helm 3.0.

OpenShift

OpenShift интегрируется с Red Hat's Operator Hub, курируемым списком приложений, которые отвечают требованиям Red Hat для включения. Пользователи могут устанавливать приложения из Developer Catalog, а администраторы могут добавлять новые репозитории Helm в Developer Catalog через CLI.

Tanzu

Tanzu Application Catalog (TAC) — это дополнительная платная услуга, с помощью которой операторы могут создать пакет приложений, который TAC отслеживает, обновляет, тестирует и развертывает в локальном реестре для использования локальными ресурсами. Эта услуга имеет базовую и расширенную версии, доступные по подписке.

3.3.2 Provision/ Terraform / Ansible:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 2**

«Боцман»

«Боцман» поддерживает провайдера Terraform, позволяя пользователям развертывать и управлять платформой, используя принципы Infrastructure as Code (IaC). Несмотря на отсутствие официальной интеграции с другими решениями, открытый API «Боцман» и использование контейнеров упрощают интеграцию с такими решениями, как Ansible, Puppet, Chef, группы автомасштабирования AWS, cloud-init или другие стратегии инициализации.

OpenShift

OpenShift использует Terraform для установки, но делает это путем включения программы установки Terraform и всех скриптов в бинарный файл программы установки. Они не видны пользователю и не доступны для включения в корпоративный рабочий процесс IaaS.

Tanzu

Невозможно развернуть кластер управления Tanzu Kubernetes Grid (TKG) через Terraform. Однако операторы могут развернуть гостевой кластер TKG и подключить его к vSphere с помощью K8s Provider для Terraform. Это отличается от развертывания кластера управления или назначения супервизорного кластера vSphere в качестве кластера управления TKG, и, хотя это возможно, такой метод развертывания не поддерживается.

3.3.3 CI/CD:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 2**

«Боцман»

«Боцман» интегрируется с любой системой CI/CD, которая работает с Kubernetes. Если у пользователя еще нет системы CI/CD, он может использовать «Боцман» Continuous Delivery («Боцман CD»), которая включает в себя использование «Боцман» project Fleet. «Боцман CD» — это подход на основе GitOps, который позволяет пользователям эффективно управлять рабочими процессами кластеров в масштабе. Любые изменения, вносимые в кластеры, проходят через централизованный контроллер Fleet, который имеет доступ к репозиторию Git, конфигурациям и назначениям кластеров. Это гарантирует, что правильный код будет применен к правильному приложению на нужном кластере. Fleet включен в «Боцман» и может быть установлен на любой кластер Kubernetes через Helm.

OpenShift

OpenShift работает с любой системой CI/CD, которая работает с Kubernetes. Кроме того, он поставляется с функциями для создания образов контейнеров внутри кластера, системой CI/CD, основанной на проекте с открытым исходным кодом Tekton, и рабочим процессом GitOps, основанным на проекте с открытым исходным кодом Argo CD.

Tanzu

Компания VMware объединила несколько решений с открытым исходным кодом в платную службу Tanzu Build Service, которая позволяет разработчикам использовать любой кластер Kubernetes (в том числе и не из Tanzu) для создания образов контейнеров. Они также объединили CI-движок Concourse с открытым исходным кодом в Concourse for VMware Tanzu. Кластеры Tanzu Kubernetes будут работать с любой системой CI/CD, которая работает с Kubernetes. Tanzu не предлагает интегрированного решения GitOps.

3.3.4 Расширенный мониторинг:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 2**

«Боцман»

«Боцман» поставляется с базовым мониторингом, активированным по умолчанию. Администраторы кластеров могут включить расширенный мониторинг одним щелчком мыши в пользовательском интерфейсе «Боцмана». Платформа развертывает Prometheus и Grafana на уровне проекта и кластера, и устанавливает предварительно настроенные информационные панели, которые сразу же обеспечивают видимость операций кластера. Пользователи могут получить доступ к Grafana и увидеть метрики для ресурсов, к которым они имеют доступ. Они также могут закомментировать свои рабочие нагрузки, чтобы Prometheus начал собирать с них пользовательские метрики.

OpenShift

OpenShift поставляется с Prometheus и Grafana, активированными по умолчанию, с предварительно настроенными оповещениями и информационными панелями. Начиная с версии 4.7, администраторы кластеров могут активировать мониторинг пользовательских рабочих нагрузок из того же стека.

Tanzu

Tanzu не включает мониторинг или визуализацию по умолчанию. Рекомендуемое компанией VMware решение для дополнительного мониторинга Tanzu — развертывание VMware Wavefront, дополнительная платная услуга.

3.3.5 Алерты и уведомления:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 1**

«Боцман»

«Боцман» поддерживает отправку оповещений в Slack, PagerDuty, WeChat, электронную почту или любой пункт назначения webhook. Уведомления могут быть настроены на уровне кластера и проекта, что позволяет делегировать ответственность за события приложения ответственным командам.

OpenShift

OpenShift позволяет администраторам и привилегированным пользователям создавать и управлять оповещениями для платформы и рабочих нагрузок пользователей. По умолчанию оповещения видны только в пользовательском интерфейсе, но OpenShift поддерживает отправку оповещений на адреса PagerDuty, Slack, Email или Webhook.

Tanzu

Оповещения и уведомления доступны через VMware Wavefront, отдельное платное решение для мониторинга, или через ручную настройку компонента Alert Manager в Prometheus.

3.3.6 Внешняя доставка логов:

- **«Боцман» → 4**
- **OpenShift → 4**
- **Tanzu → 2**

«Боцман»

«Боцман» для ведения логов использует собственный оператор для ведения логов на платформе. Fluent Bit используется для агрегации логов, а Fluentd — для фильтрации сообщений и маршрутизации. Установка протоколирования для управляемого кластера «Боцман» выполняется быстро и просто, для этого требуется всего один щелчок мыши в Cluster Explorer. Администраторы могут определить видимость журналов с помощью двух доступных ролей: logging-admin, которая дает полный доступ к потокам с именами и выходам, или logging-view, которая дает доступ только к потокам с именами.

OpenShift

Администраторы могут развернуть OpenShift Elasticsearch Operator и OpenShift Logging Operator. После установки журналы собираются, хранятся и визуализируются с помощью Fluentd, Elasticsearch и Kibana. Журналы также можно пересылать через Fluentd, syslog или собственный протокол Red Hat API. Видимость журналов соответствует разрешениям RBAC для программы просмотра.

Tanzu

Кластеры Tanzu Kubernetes Grid (TKG) поддерживают отправку журналов через Fluent Bit или как компонент VMware Wavefront (платное дополнение). Несмотря на открытый исходный код, VMware устанавливает Fluent Bit как собственное расширение TKG.

3.3.7 Windows container support / поддержка контейнера Windows:

- **«Боцман» → 0**
- **OpenShift → 4**
- **Tanzu → 0**

«Боцман»

«Боцман» не включает производственную поддержку для использования серверов Windows в кластерах Kubernetes и развертывания контейнеров Windows.

OpenShift

OpenShift (OCP4) включает производственную поддержку для использования серверов Windows в кластерах Kubernetes и развертывания контейнеров Windows.

Tanzu

Tanzu Kubernetes Grid (TKG) — это ребрендинговое название VMware Enterprise PKS (Pivotal Container Service). Хотя поддержка контейнеров Windows в PKS была бета-версией в декабре 2019 года, в документации TKG нет информации о развертывании рабочих Windows или контейнерных рабочих нагрузок Windows. Кроме того, ссылки на бета-версию поддержки в документации TKGI v1.8 были удалены из документации v1.11. Других ссылок или указаний на поддержку контейнеров Windows в документации v1.11 не обнаружено.

3.3.8 Поддержка Integrated Service Mesh:

- **«Боцман» → 4**
- **OpenShift → 3**
- **Tanzu → 1**

«Боцман»

«Боцман» поставляет cilium и Istio в виде компонента CNI, которые объединяют Pilot, Citadel, Galley и инжектор sidecar.

OpenShift

OpenShift предоставляет Istio, модифицированную Red Hat для работы в OpenShift. Хотя функционально она похожа на Istio, она не будет развиваться так же быстро, как темп выпуска Istio.

Tanzu

VMware продает Tanzu Service Mesh (TSM), собственную сетку, построенную поверх NSX и доступную через платформу VMware Cloud Services.

3.3.9 Enterprise SLA:

- **«Боцман» → 4**
- **OpenShift → 2**
- **Tanzu → 2**

«Боцман»

Предоставляется корпоративная подписка на «Боцман». Две опции поддержки от Вендора — «Стандарт» (9x5) и «Премиум» (24x7).

OpenShift

Red Hat обеспечивает поддержку OpenShift и стека программного обеспечения Red Hat. Однако многие компоненты OpenShift не могут быть изменены или использованы вне параметров Red Hat без отмены поддержки. Кроме того, модель поддержки Red Hat предусматривает стоимость виртуального ядра, поэтому каждое обновление среды клиента увеличивает стоимость поддержки.

Tanzu

VMware предлагает поддержку сообщества (неоплачиваемую), поддержку Premium Support (включенную в подписку или лицензию), а также более высокий уровень, включающий специального технического менеджера по работе с клиентами (TAM) для «более быстрого решения проблем и технического руководства». Премиум-поддержка включает круглосуточный доступ для решения проблем 1-й степени тяжести.