

**Платформа DevOps (ИС ТП)**

Программа и методика испытаний

Ответственный исполнитель:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / ФИО

|  |  |
| --- | --- |
| Дата: |  |
| Версия: |  |

Содержание

[1 Введение 4](#_Toc182824273)

[2 Объект испытаний 4](#_Toc182824274)

[3 Цель тестирования 4](#_Toc182824275)

[4 Объем тестирования 4](#_Toc182824276)

[5 Условия и порядок проведения 4](#_Toc182824277)

[5.1 Порядок проведения 4](#_Toc182824278)

[5.2 Место и продолжительность испытаний 5](#_Toc182824279)

[5.3 Отчетность 5](#_Toc182824280)

[5.4 Требования к техническим средствам 5](#_Toc182824281)

[6 Стратегия тестирования 6](#_Toc182824282)

[6.1 Функциональное тестирование 6](#_Toc182824283)

[6.1.1 Цель тестирования 6](#_Toc182824284)

[6.1.2 Проверяемые требования 6](#_Toc182824285)

[6.1.3 Методика тестирования 8](#_Toc182824286)

[6.1.4 Критерии завершения 12](#_Toc182824287)

[6.2 Тестирование безопасности 13](#_Toc182824288)

[6.2.1 Цель тестирования 13](#_Toc182824289)

[6.2.2 Проверяемые требования 13](#_Toc182824290)

[6.2.3 Методика тестирования 16](#_Toc182824292)

[6.2.4 Критерии завершения 23](#_Toc182824293)

[6.3 Мониторинг 24](#_Toc182824295)

[6.3.1 Цель тестирования 24](#_Toc182824296)

[6.3.2 Проверяемые требования 24](#_Toc182824297)

[6.3.3 Методика тестирования 25](#_Toc182824298)

[6.3.4 Критерий завершения 28](#_Toc182824299)

[6.4 Тестирование масштабируемости 29](#_Toc182824301)

[6.4.1 Цель тестирования 29](#_Toc182824302)

[6.4.2 Проверяемые требования 29](#_Toc182824303)

[6.4.3 Методика тестирования 31](#_Toc182824305)

[6.4.4 Критерий завершения 32](#_Toc182824306)

[6.5 Интеграционное тестирование 33](#_Toc182824308)

[6.6 Прочее тестирование 33](#_Toc182824309)

[6.6.1 Цель тестирования 33](#_Toc182824310)

[6.6.2 Проверяемые требования 33](#_Toc182824311)

[6.6.3 Методика тестирования 35](#_Toc182824313)

[6.6.4 Критерий завершения 36](#_Toc182824314)

# Введение

Настоящий документ представляет собой «Программу и методику испытаний», предназначенную для проведения испытаний ПО «Платформа DevOps (ИС ТП)» (далее – ИС "Платформа") для нужд Блока информационных технологий ПАО «Промсвязьбанк» (далее – Заказчик).

Испытания ИС "Платформа" проводит Заказчик с участием представителя Разработчика Платформы. Заказчик представляется группой экспертов, уполномоченных на подписание итогового «Протокола испытания».

Все компоненты ИС "Платформа" должны быть предварительно локально протестированы Разработчиком. Разработчик должен иметь документ, подтверждающий готовность ИС "Платформа" к тестированию.

Цель создания документа:

* Определить объекты испытания.
* Рекомендовать и описать стратегии тестирования, которые будут применены.
* Определить требуемые ресурсы и предоставить оценку трудозатрат на тестирование.
* Перечислить поставляемые Заказчику компоненты ИС "Платформа".
* Определить условия и порядок проведения испытаний.

# Объект испытаний

Объект испытаний: ИС «Платформа DevOps (ИС ТП)» , версия 1.0

Шифр системы: PSB.00x

Табл. 1. Комплектность ИС

|  |  |
| --- | --- |
| Подсистема/модуль | |
| ИС "Платформа" | 1.0 |
| Документация | |
| Приложение 2 к Договору №\_\_\_\_\_ от " " 2024 г | 1.0 |

# Цель тестирования

Целью тестирования ИС "Платформа" является:

* Проверка соответствие требований «Технического задания» и разработанного ПО.
* Обнаружение и устранения программных ошибок или (и), если это возможно, доказательство отсутствия последних в ПО.

# Объем тестирования

В рамках данных испытаний предполагается провести функциональное тестирование модулей ИС "Платформа" в соответствии с функциональными требованиями, описанными в документе «Техническое задание».

# Условия и порядок проведения

## Порядок проведения

* Сроки проведения испытаний за две недели согласуются Разработчиком с Заказчиком на основании предложений Разработчика.
* Испытания проводятся комиссией, формируемой Разработчиком совместно с Заказчиком.
* Испытания осуществляются на стенде Заказчика, согласно требованиям к техническому и программному обеспечению «Технического задания». Рекомендуется, чтобы тестовая система имитировала производственную среду, масштабированную в сторону уменьшения в тех случаях, когда это допустимо.
* Испытания производятся согласно настоящей «Программа и методика испытаний» в сроки согласованные с Заказчиком.
* Испытания заканчиваются оформлением документа «Протокол испытаний», который подписывается представителем Разработчиков, представителем Заказчика.
* Возникшие в ходе проведения испытаний замечания, устраняются в установленном порядке.

## Место и продолжительность испытаний

* Испытания проводятся на стенде с участием представителей Заказчика и Разработчика, уполномоченных на подписание «Протокол испытаний».
* Плановая дата начала испытаний: \_\_\_\_.\_\_\_\_\_.2024 г. в рабочее время (с 9 до 18). Плановая продолжительность испытаний – \_\_\_\_\_\_дней. Продолжительность испытаний может быть увеличена в случае необходимости проведения дополнительных тестов и проверок.

## Отчетность

* В процессе испытаний ведется «Протокол испытаний».
* По завершении испытаний составляется Акт, в котором излагаются общие результаты испытаний. К Акту прилагается «Протокол испытаний», который ведётся в процессе проведения испытаний.
* Акт составляется в двух экземплярах и подписывается представителями Заказчика и Разработчика.

## Требования к техническим средствам

Испытания должны проводиться на стенде, с минимальными техническими характеристиками, приведенными в таблице ниже.

|  |  |
| --- | --- |
| Сервер базы данных | |
| Процессор | 4 vCPU на каждый узел кластера |
| Жесткий диск | 100 GB SSD для каждого узла |
| Оперативная память | 16 GB RAM на каждый узел кластера |
| Сетевой адаптер | 1 Gbps Ethernet на каждый узел |
| Операционная система | Astra Linux SE 1.7 или совместимая операционная система на всех узлах. |
| Клиентские рабочие места | |
| Процессор | 2 vCPU |
| Оперативная память | 8 GB RAM |
| Жесткий диск | 50 GB SSD |
| Монитор | Разрешение не менее 1920x1080 (Full HD) |
| Сетевой адаптер | 1 Gbps Ethernet или Wi-Fi |
| Операционная система | Astra Linux SE 1.7 или совместимая операционная система |
| Системы, не входящие в состав ИС "Платформа" | |
| Платформа аппаратной виртуализации | |
| Система хранения данных | |
| LDAP-каталог | |
|  | |
| Почтовый сервер | |
| Система управления секретами | |
| AHRepo | |
| AHCode | |
| Luntry | |
| Система сбора журналов | |
| Система класса SIEM | |
| Средства защиты информации | |

# Стратегия тестирования

Для требований, предъявляемых к ИС "Платформа" установлены следующие категории:

* Решающее – требование, при невыполнении которого результат тестирования оценивается как неуспешный.
* Нерешающее – требование, несоответствие которому не является препятствием для оценки результата тестирования как успешного.

## Функциональное тестирование

### Цель тестирования

Убедиться в корректном функционировании объекта испытаний.

### Проверяемые требования

Таблица 1. Требования к функциональному тестированию



|  |  |  |  |
| --- | --- | --- | --- |
| Номер | Код требования в ТЗ | Краткое описание | Тестовые сценарии в ПМИ |
| 1 | П.3.1.12 | Наличие функционала сервисной сетки (Service Mesh) | Ф-12, Ф-16 |
| 2 | П.3.1.13 | Поддержка многоарендности с полной изоляцией арендаторов друг от друга | Ф-12 |
| 3 | П.3.1.2 | Возможность автоматической установки кластеров с заданной конфигурацией | Ф-8 |
| 4 | П.3.1.5 | Поддержка конфигурации высокой доступности и восстановления после аварий (Disaster Recovery) | Ф-14 |
| 5 | П.3.1.7 | Возможность управления распределением подов между узлами кластера | Ф-10 |
| 6 | П.3.1.8 | Механизм назначения меток на узлы кластера | Ф-8, Ф-10, Ф-12 |
| 7 | П.3.1.9 | Наличие подсистемы регистрации событий | Ф-12 |
| 8 | П.3.3.11 | Использование актуальной версии Kubernetes с задержкой не более 12 месяцев | Ф-5 |
| 9 | П.3.3.12 | Возможность использования предыдущей версии Kubernetes | Ф-5 |
| 10 | П.3.3.16 | Управление функциями Платформы через включение и отключение компонентов по функциональному признаку | Ф-12, Ф-13 |
| 11 | П.3.3.17 | Определение уровня доступности компонентов кластера с агрегацией по функциональности | Ф-7 |
| 12 | П.3.3.6 | Поддержка Hierarchical Namespaces | Ф-11 |
| 13 | П.3.3.8 | Возможность автоматического добавления аннотаций и меток к пространствам имен | Ф-11, Ф-15 |
| 14 | П.3.4.8 | Возможность интеграции с системой управления секретами | Ф-16 |
| 15 | П.3.5.1 | Возможность самостоятельной загрузки пакетов обновления для последующей установки | Ф-2, Ф-3 |
| 16 | П.3.5.2 | Обновление всех компонентов через единый инструмент управления | Ф-2 |
| 17 | П.3.5.4 | Поддержка хранения версий используемых компонентов | Ф-2, Ф-3 |
| 18 | П.4.1.2 | Отсутствие компонентов иностранного происхождения в контейнерных образах Платформы | Ф-4 |
| 19 | П.4.2.2 | Аутентификация через внешний провайдер OpenID Connect | Ф-11 |
| 20 | П.5.1.3 | Интеграция с хранилищем секретов с ограничением на хранение секретов в базе данных кластера | Ф-16 |
| 21 | П.5.2.8 | Проверка на наличие шифрования (TLS) соединений между подами и внешними соединениями | Ф-16 |
| 22 | П.6.1.10 | Хранение всех настроек системы с поддержкой резервирования и версионирования | Ф-9, Ф-8 |
| 23 | П.6.1.6 | Поддержка российских операционных систем из ЕРРП на пользовательских устройствах | Ф-4 |
| 24 | П.6.2.2 | Автономное восстановление после сбоев для высокой доступности системы | Ф-6, Ф-7 |
| 25 | П.6.2.3 | Отказоустойчивость и автоматическое переключение при сбоях (failover) | Ф-6 |
| 26 | П.6.3.1 | Поддержка автоматического горизонтального масштабирования без остановки работы | Ф-6, Ф-7 |
| 27 | П.6.5.2 | Возможность установки системы на оборудовании заказчика (on-premises) | Ф-1 |
| 28 | П.6.5.5 | Использование физических серверов для кластерных узлов системы | Ф-1 |
| 29 | П.6.5.6 | Возможность установки в изолированном контуре без доступа к Интернету | Ф-1 |

### Методика тестирования

Функциональное тестирование предполагает выполнение тестовых процедур, приведенных в таблице ниже.

Таблица 2. Порядок проведения функционального тестирования

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Код требования в ТЗ** | **Название Тестового сценария** | **Приоритет проверки** | **Шаги** | **Ожидаемый результат** | **Время прохождения** |
| 1 | П.3.1.12 | Ф-12, Установка / добавление элементов интерфейса / модулей (из поставки платформы) | Высокий | Установить платформу Deckhouse с предустановленным набором модулей default. Добавить или удалить необходимые модули, используя конфигурацию управления модулями Deckhouse. Проверить корректность работы новых модулей и убедиться, что состав модулей изменился в соответствии с настройками. | Платформа установлена с набором модулей default, после чего состав модулей был успешно изменен, а новые модули работают корректно. |  |
| П.3.1.13 |
| П.3.1.9 |
| П.3.3.16 |
| 2 | П.3.3.17 | Ф-7, Управление узлами кластера (добавление, удаление) | Высокий | Добавить новый узел в Kubernetes кластер, настроить его и убедиться, что он перешел в статус Ready. Освободить узел от рабочих нагрузок, удалить его из кластера и очистить конфигурацию. Проверить, что узел удален и больше не отображается в списке узлов кластера. | Узел был успешно добавлен в кластер и перешел в статус Ready, затем был освобожден от рабочих нагрузок, удален из кластера и перестал отображаться в списке узлов. |  |
| П.6.2.2 |
| П.6.3.1 |
| 3 | П.3.3.8 | Ф-15, Управление namespaces (добавление, удаление, редактирование) | Высокий | Создать новый namespace с помощью команды kubectl create namespace. Добавить или удалить labels на созданном namespace, используя команды kubectl label namespace. Убедиться, что изменения применились, и namespace отображает корректные labels. | Namespace успешно создан, labels были добавлены или удалены, и изменения отобразились корректно. |  |
| 4 | П.3.1.7 | Ф-10, Размещение компонентов Deckhouse Kubernetes Platform на выделенных узлах | Высокий | Добавить выделенный узел в кластер и настроить его для размещения компонентов мониторинга. Применить конфигурацию NodeSelector или Taints/Tolerations для ограничения размещения Prometheus только на выделенном узле. Проверить, что Prometheus успешно запустился на выделенном узле и функционирует корректно. | Выделенный узел был настроен для размещения компонентов мониторинга, Prometheus запустился на этом узле и работает корректно. |  |
| П.3.1.8 |
| 5 | П.4.1.2 | Ф-4, Поддержка РФ операционных систем (РЕДОС, ALT linux, Astra Linux) | Высокий | Установить узел Kubernetes под управлением одной из российских операционных систем (РЕДОС, ALT Linux, Astra Linux) и подготовить его для работы с Deckhouse Platform. Выполнить установку Deckhouse Platform на подготовленный узел, следуя документации по установке в выбранной ОС. Проверить, что все поды запускаются успешно и находятся в статусе Running. | Deckhouse Platform успешно установлена на узел с российской ОС, все поды работают корректно, и статус Running подтвержден для всех компонентов. |  |
| П.6.1.6 |
| 6 | П.3.1.5 | Ф-14, Отказоустойчивая конфигурация всех компонентов платформы | Низкий | Установить multi-master кластер Kubernetes и развернуть платформу Deckhouse. Проверить, что служебные компоненты (Prometheus, Grafana, Dex) имеют как минимум две реплики. Убедиться, что реплики распределены по различным узлам кластера для обеспечения отказоустойчивости. | Служебные компоненты Prometheus, Grafana и Dex развернуты в двух репликах и равномерно распределены между узлами кластера. |  |
| 7 | П.3.3.11 | Ф-5, Обновление версии Kubernetes | Высокий | Установить кластер Kubernetes с настройкой версии “Automatic”. Изменить версию Kubernetes на желаемую через конфигурацию кластера и применить изменения. Проверить, что на всех узлах кластера kubelet обновился до необходимой версии. | Версия Kubernetes была изменена на желаемую, и kubelet на всех узлах кластера обновился до необходимой версии. |  |
| П.3.3.12 |
| 8 | П.3.3.6 | Ф-11, Запуск модулей Deckhouse Enterprise версии | Высокий | Включить модуль user-authn с использованием команды управления модулями Deckhouse. Проверить, что в кластере появился namespace d8-user-authn. Убедиться, что в этом namespace запущен под с именем dex. | Модуль user-authn был включен, namespace d8-user-authn создан, а под dex успешно запущен. |  |
| П.3.3.8 |
| П.4.2.2 |
| 9 | П.6.5.2 | Ф-1, Возможность установки платформы в закрытом контуре | Высокий | Настроить локальные репозитории для Docker-образов и Helm-чартов, загрузив в них все необходимые компоненты. Выполнить установку с использованием локальных ресурсов и проверить корректную работу платформы. Подтвердить успешность установки, убедившись, что все компоненты функционируют автономно без доступа к интернету. | Установка прошла успешно, все компоненты Deckhouse Platform работают в закрытом контуре, все зависимости загружены из локальных репозиториев, и платформа готова к использованию. |  |
| П.6.5.5 |
| П.6.5.6 |
| 10 | П.6.2.2 | Ф-6, Возможность увеличения количества control-plane узлов | Высокий | Добавить два дополнительных узла в кластер и настроить их как master-узлы. Выполнить обновление конфигурации control-plane для включения новых узлов. Проверить состояние кластера и убедиться, что все узлы работают корректно, а кластер функционирует без ошибок. | В кластер были добавлены два новых master-узла, и кластер сохранил свою работоспособность. |  |
| П.6.2.3 |
| П.6.3.1 |
| 11 | П.3.5.1 | Ф-3, Возможность ручного обновления платформы Deckhouse | Высокий | Установить Deckhouse платформу, указав версию на единицу ниже текущего минорного релиза выбранного канала обновления, и настроить ручной режим обновления. Запустить обновление вручную, используя команду kubectl apply для нового релиза из репозитория канала обновлений на сайте releases.deckhouse.ru. Проверить логи обновления и убедиться, что статус ресурса deckhouserelease изменился на Deployed для новой версии. | Платформа Deckhouse успешно обновляется вручную до актуальной версии выбранного канала, а статус deckhouserelease отображается как Deployed. |  |
| П.3.5.4 |
| 12 | П.3.3.16 | Ф-13, Возможность отключения неиспользуемых модулей платформы | Средний | Отключить модуль upmeter, используя команду управления модулями Deckhouse. Проверить, что модуль успешно отключен и все связанные ресурсы удалены. Убедиться, что namespace d8-upmeter больше не существует в кластере. | Модуль upmeter был отключен, и namespace d8-upmeter удален из кластера. |  |
| 13 | П.3.4.8 | Ф-16, Возможность использования внешних модулей | Низкий | Установить внешний оператор в Deckhouse Kubernetes Platform, используя манифесты или Helm-чарт. Проверить создание необходимых ресурсов оператора, включая namespace и deployment. Убедиться, что поды оператора успешно запущены и находятся в статусе Running. | Внешний оператор установлен, его поды успешно запущены и находятся в статусе Running. |  |
| П.5.1.3 |
| П.5.2.8 |
| 14 | П.6.1.10 | Ф-9, Возможность дополнительной конфигурации runtime-компонентов узлов кластера | Высокий | Применить настройку ресурса NodeGroup с необходимыми параметрами для конфигурации runtime-компонентов. Проверить работу systemd-сервиса bashible на узле кластера и его логи для подтверждения успешного выполнения изменений. Убедиться, что параметр на узле кластера изменился на заданное значение. | Настройка ресурса NodeGroup была применена, systemd-сервис bashible успешно отработал, и параметр на узле кластера изменился на необходимое значение. |  |
| 15 | П.3.5.1 | Ф-2, Автоматическое обновление платформы Deckhouse | Высокий | Установить Deckhouse платформу, указав версию на единицу ниже текущего минорного релиза выбранного канала обновления, и настройте автоматический механизм обновления. Убедиься, что платформа настроена для получения обновлений с использованием репозиториев канала на сайте releases.deckhouse.ru. Проверить логи и статус ресурса deckhouserelease, чтобы подтвердить успешное обновление и статус Deployed для нового релиза. | Платформа Deckhouse автоматически обновляется до актуальной версии выбранного канала обновления, а статус deckhouserelease отображается как Deployed. |  |
| П.3.5.2 |
| П.3.5.4 |
| 16 | П.3.1.2 | Ф-8, Автоматическая настройка узлов кластера | Высокий | Применить ресурс NodeGroupConfiguration с заданными параметрами для настройки узлов кластера. Проверить работу systemd-сервиса bashible на узле и убедиться, что конфигурация была применена. Проверить, что параметр на узле кластера изменился на указанное значение. | Ресурс NodeGroupConfiguration был применен, systemd-сервис bashible отработал корректно, а параметр на узле изменился на необходимое значение. |  |
| П.3.1.8 |



Таблица 3. Оценка трудозатрат на тестирование

|  |  |
| --- | --- |
| **Количество проверок** | **Общее время прохождения** |
| 16 |  |

### Критерии завершения

Все запланированные тесты были выполнены. Все выявленные ошибки зафиксированы.

## Тестирование безопасности

### Цель тестирования

Безопасность уровня приложения: проверить, что пользователю каждого типа доступны только те функции / данные, на которые предоставлены права данному типу пользователей.

Безопасность уровня системы: проверить, что только те пользователи, которым предоставлен доступ к системе и приложениям, могут получить к ним доступ.

Средства обеспечения информационной безопасности в средах контейнерной оркестрации: проверить обеспечение соблюдения стандартов безопасности сред контейнерной оркестрации, проверить работоспособность и возможность настройки механизмов обеспечения информационной безопасности.

### Проверяемые требования

Таблица 4. Требования тестирования безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| Номер | Код требования в ТЗ | Краткое описание | Тестовые сценарии в ПМИ |
| 1 | П. 5.2.11 | Журналирование операций Kubernetes и работы с etcd, выгрузка на syslog-сервер. | Б-1 |
| 2 | П. 6.12.1 | Раздел аудита для протоколирования действий пользователя. | Б-1, Б-6, Б-7, Б-8, Б-9, Б-10, Б-11, Б-12, Б-13, Б-19, Б-20, Б-21, Б-22 |
| 3 | П. 6.12.2 | Модули регистрации событий: логирование, SQL-доступ, аудит. | Б-1, Б-19, Б-22 |
| 4 | П. 4.2.1 | Поддержка CNI плагинов с Network Policy. | Б-2 |
| 5 | П. 6.10.3 | Поддержка внутрикластерных сетевых политик. | Б-2, Б-3, Б-4, Б-6, Б-14, Б-15, Б-21 |
| 6 | П. 3.2.1 | CNI с фильтрацией пакетов на уровнях L, L OSI. | Б-3, Б-20, Б-21 |
| 7 | П. 3.3.1 | Веб-интерфейс с HTML. | Б-4,Б-17 |
| 8 | П. 6.1.13 | Отображение схемы сетевых взаимодействий с ПО Luntry. | Б-4 |
| 9 | П. 4.2.3 | Автонастройка компонентов Платформы для работы по HTTPS. | Б-5, Б-13 |
| 10 | П. 6.10.1.2 | Управление сертификатами безопасности централизованно или по компонентам. | Б-5, Б-8, Б-13 |
| 11 | П. 6.10.1.4 | Поддержка защищенных протоколов (TLS ., HTTPS). | Б-5 |
| 12 | П. 4.2.5 | Интеграция с LDAPS, OAuth /SAML, двухфакторная аутентификация. | Б-5, Б-8, Б-9 |
| 13 | П. 5.3.4 | RBAC for Kubernetes и ролевая модель для ПРОД/не-ПРОД. | Б-7, Б-9, Б-10, Б-11, Б-12 |
| 14 | П. 3.1.10 | ACL и RBAC для управления правами доступа. | Б-7, Б-11, Б-21 |
| 15 | П. 3.11.9 | Исключение запуска процессов в контейнере под root. | Б-14 |
| 16 | П. 6.10.7 | Настройка Pod Security Standards. | Б-14, Б-16 |
| 17 | П. 3.11.3 | Проверка ресурсов кластера на соответствие политикам безопасности. | Б-14,Б-15,Б-16 |
| 18 | П. 3.11.8 | Запуск контейнеров только с минимальными разрешениями. | Б-14 |
| 19 | П. 3.11.4 | Блокировка деплоя на основе проверки политик безопасности. | Б-15, Б-16 |
| 20 | П. 6.1.14 | Формирование профиля приложения через Luntry. | Б-15 |
| 21 | П. 3.3.5 | Лимиты ресурсов для пространств имен (квоты). | Б-17, Б-18 |
| 22 | П. 3.3.19 | Учет лимитов ресурсов при деплое манифестов. | Б-17 |
| 23 | П. 6.1.11 | Централизованное управление квотированием ресурсов. | Б-17 |
| 24 | П. 3.1.7 | Управление распределением подов между узлами. | Б-17 |
| 25 | П. 6.3.1 | Автомасштабирование кластера без остановки сервиса. | Б-17 |
| 26 | П. 3.3.6 | Поддержка Hierarchical Namespaces. | Б-18 |
| 27 | П. 3.3.8 | Автодобавление аннотаций и меток к пространствам имен. | Б-18 |
| 28 | П. 6.1.9 | Группировка ресурсов по изолированным средам (ПРОД/не-ПРОД). | Б-18 |
| 29 | П. 6.1.10 | Хранение настроек системы в ConfigMap с масштабированием и резервированием. | Б-18 |
| 30 | П. 6.1.15 | Формирование сетевых политик на базе данных обучения в Luntry. | Б-18 |
| 31 | П. 3.11.5 | Протоколирование изменений, включая неавторизованные. | Б-19 |
| 32 | П. 5.2.5 | Контроль событий runtime (запуск приложений, сетевые соединения). | Б-19, Б-21,Б-22 |
| 33 | П. 5.2.10 | Мониторинг команд и ограничивающих правил для sudo. | Б-19 |
| 34 | П. 3.11.1 | Поддержка CIS Benchmark для Kubernetes. | Б-19, Б-22 |
| 35 | П. 5.2.8 | Мониторинг шифрования соединений (TLS). | Б-20 |
| 36 | П. 5.2.9 | Контроль TLS для соединений между подами. | Б-20 |
| 37 | П. 3.1.3 | Автоматический выпуск сертификатов кластеров. | Б-20 |
| 38 | П. 3.1.12 | Функционал Service Mesh. | Б-20 |
| 39 | П. 5.2.3 | Контроль изменений и авторизаций RBAC и политик СЗИ. | Б-21 |
| 40 | П. 5.2.2 | Проверяемость компонентов системы по заданным критериям. | Б-22 |
| 41 | П. 6.10.4 | Контроль конфигурации кластера по CIS Benchmarks. | Б-22 |

### Методика тестирования

Тестирование безопасности и контроля доступа предполагает выполнение тестовых процедур, приведенных в таблице ниже.

Таблица 5. Порядок проведения тестирования безопасности и контроля доступа

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Код требования в ТЗ** | **Название Тестового сценария** | **Приоритет проверки** | **Шаги** | **Ожидаемый результат** | **Время прохождения** |
| 1 | П. 5.2.11, 6.12.1, 6.12.2, | Б-1, Аудит событий Kubernetes API | Средний | Настроить сбор Kubernetes Audit Log, добавив соответствующую конфигурацию в манифест API-сервера. Убедиться, что файлы аудита записываются в указанное хранилище с полным логированием действий в кластере. Проверить содержимое файла аудита, чтобы подтвердить запись всех операций в Kubernetes API. | Сбор Kubernetes Audit Log настроен, и в файле аудита корректно записываются все действия, выполненные в Kubernetes. |  |
| 2 | П. 4.2.1, 6.10.3, | Б-2, Фильтрации трафика внутри кластера (поддержка NetworkPolicy). Только для кластеров с CNI Cilium | Высокий | Настроить CNI Cilium с включением режима policyAuditMode, добавив соответствующие параметры в конфигурацию. Создать NetworkPolicy для ограничения трафика между подами в кластере. Протестировать работу NetworkPolicy, убедившись, что разрешенный и запрещенный трафик соответствует настроенным правилам. | Режим policyAuditMode успешно настроен, NetworkPolicy работает корректно, трафик фильтруется в соответствии с заданными правилами. |  |
| 3 | П. 3.2.1, 6.10.3, | Б-3, Фильтрации трафика на уровне L7 внутри кластера (поддержка CiliumNetworkPolicy). Только для кластеров с CNI Cilium | Высокий | Настроить кластер с CNI Cilium, добавив необходимые параметры для поддержки L7 фильтрации трафика. Создать CiliumNetworkPolicy, задав правила фильтрации на уровне L7 (например, HTTP методы или URI). Протестировать работу политики, проверив, что трафик соответствует заданным правилам, а неразрешенные запросы блокируются. | CiliumNetworkPolicy успешно настроена, фильтрация трафика на уровне L7 работает корректно, разрешенные запросы проходят, а запрещенные блокируются. |  |
| 4 | П. 3.3.1, 6.1.13, 6.10.3 | Б-4, Отображения действия политик (NetworkPolicy) в веб-интерфейсе. Только для кластеров с CNI Cilium | Низкий | Включить модуль cilium-hubble через конфигурацию Deckhouse, следуя документации. Проверить доступность веб-интерфейса Hubble и убедиться, что интерфейс отображает события, связанные с срабатыванием NetworkPolicy. Протестировать несколько сценариев фильтрации трафика, чтобы убедиться в корректной визуализации действий политик. | Модуль cilium-hubble включен, веб-интерфейс доступен, и в нем отображаются события, связанные с срабатыванием NetworkPolicy. |  |
| 5 | П. 4.2.3, 6.10.1.2, 6.10.1.4 | Б-5, Возможность использования корпоративного TLS/SSL сертификата для компонентов платформы | Высокий | Настроить Deckhouse Platform для использования корпоративного промежуточного сертификата, указав параметры в конфигурации. Заказать выпуск TLS/SSL сертификата через модуль управления сертификатами Deckhouse. Убедиться, что сертификат успешно выпущен и используется компонентами платформы. | TLS/SSL сертификат был успешно выпущен с использованием корпоративного промежуточного сертификата и корректно применяется компонентами платформы. |  |
| 6 | П. 4.2.5, 6.10.3, 6.12.1 | Б-6, Использования временных статических пользователей в кластере | Высокий | Создать временного статического пользователя через конфигурацию Deckhouse, указав его данные в соответствующем ресурсе. Настроить права доступа для созданного пользователя, обеспечив возможность входа в веб-интерфейсы платформы. Проверить успешную авторизацию пользователя в веб-интерфейсах с использованием указанных учетных данных. | Статический пользователь был успешно создан и использован для входа в веб-интерфейсы платформы. |  |
| 7 | П. 5.3.4, 3.1.10,6.12.1 | Б-7, Использование статических групп пользователей в кластере | Высокий | Создать статическую группу пользователей, добавив соответствующую конфигурацию в Deckhouse. Настроить роль (Role) или роль с областью (ClusterRole), а также привязку роли (RoleBinding/ClusterRoleBinding) для предоставления прав доступа этой группе. Проверить успешное использование группы для выполнения операций через Kubernetes API. | Статическая группа пользователей была успешно создана и использована для выдачи прав доступа в Kubernetes API. |  |
| 8 | П. 4.2.5, 6.10.1.2, 6.12.1 | Б-8, Использование внешнего провайдера аутентификации (LDAP/ /OIDC) | Высокий | Включить модуль user-authn и настроить DexProvider для интеграции с внешним провайдером аутентификации (LDAP или OIDC). Настроить параметры подключения к LDAP-серверу, включая URL, базовый DN, фильтры пользователей и групп. Проверить успешную авторизацию пользователя в веб-интерфейсах Deckhouse Platform с использованием учетных данных LDAP. | Модуль user-authn был включен, DexProvider настроен, и вход в веб-интерфейсы Deckhouse Platform с использованием LDAP-учетных данных выполнен успешно. |  |
| 9 | П. 4.2.5, 5.3.4, 6.12.1 | Б-9, Настройка ролевой модели доступа на основе групп, атрибутов пользователя | Средний | Настроить ролевую модель доступа в Deckhouse, создав Role/ClusterRole и RoleBinding/ClusterRoleBinding с привязкой к группам пользователей из LDAP или OIDC. В конфигурации DexProvider указать соответствие групп в внешнем провайдере атрибутам пользователя. Проверить, что пользователь, входящий в указанную группу, успешно получает доступ в соответствии с заданными правами. | Доступ пользователю был успешно предоставлен на основе его принадлежности к группе в LDAP или OIDC, а права доступа применены корректно. |  |
| 10 | П. 5.3.4, 6.12.1 | Б-10, Ограничение доступа пользователей к определенным namespace | Высокий | Создать Role и RoleBinding для заданного namespace, привязав их к пользователю/группе. Попробовать выполнить действия в этом namespace от имени пользователя. Проверить, что доступ к другим namespace отсутствует. | Пользователь получил доступ к заданному namespace и не имеет прав на работу с другими namespace. |  |
| 11 | П. 5.3.4, 3.1.10, 6.12.1 | Б-11, Возможность расширения прав доступа |  | Обновить роль доступа User, добавив в нее разрешения на работу с секретами (например, get, list, create). Применить обновленную роль через RoleBinding или ClusterRoleBinding для конкретного пользователя. Проверить, что пользователь получил дополнительные права и успешно выполняет операции с секретами. | Роль доступа User успешно расширена правами на работу с секретами, пользователь получил дополнительные права и может выполнять соответствующие операции. |  |
| 12 | П. 5.3.4, 6.12.1 | Б-12, Использование сервисной учетной записи для выката прикладного ПО в платформу | Высокий | Создать сервисную учетную запись (ServiceAccount) в заданном namespace. Настроить Role и RoleBinding, предоставив учетной записи права на выкат приложений в этом namespace и ограничив доступ к другим namespace. Выполнить выкат приложения, используя созданную учетную запись, и проверить успешность операции. | Сервисная учетная запись создана с ограниченными правами, приложение успешно выкачено в заданный namespace, доступ к другим namespace отсутствует. |  |
| 13 | П. 4.2.3, 6.10.1.2, 6.12.1 | Б-13, Создание статического пользователя с помощью клиентского сертификата | Высокий | Сгенерировать клиентский сертификат и ключ с использованием утилиты openssl или аналогичного инструмента. Создать соответствующий объект CertificateSigningRequest (CSR) в Kubernetes для выдачи сертификата. Одобрить запрос сертификата, получить подписанный сертификат и настроить контекст пользователя в kubeconfig для работы с кластером. | Статический пользователь создан с помощью клиентского сертификата, успешно настроен и может выполнять операции в кластере согласно выданным правам. |  |
| 14 | П. 3.11.9, 6.10.7, 3.11.3, 3.11.8, 6.10.3 | Б-14, Использование политик безопасности Kubernetes (Pod Security Standards) | Высокий | Применить политику безопасности Kubernetes (Pod Security Standards) с уровнем Restricted в заданном namespace. Попробовать создать под с параметром privileged: true, нарушающим требования политики. Проверить, что под не был создан, а в событиях кластера отображается сообщение об ошибке, связанное с нарушением политики безопасности. | Политика Restricted успешно применена, под с параметром privileged: true не создан, а соответствующая ошибка зафиксирована в событиях кластера. |  |
| 15 | П. 3.11.3, 3.11.4, 6.10.3, 6.1.14. | Б-15, Использование операционных политик для безопасной работы прикладного ПО | Низкий | Применить OperationPolicy, задающую ограничения на выполнение определенных операций в кластере (например, запрет запуска подов с некорректными настройками). Попробовать создать под, который нарушает правила, установленные в OperationPolicy. Проверить, что под не был создан, а в событиях кластера отображается ошибка о нарушении политики. | OperationPolicy успешно применена, под с нарушением политики не создан, а соответствующая ошибка зафиксирована в событиях кластера. |  |
| 16 | П. 3.11.3, 3.11.4, 6.10.7. | Б-16, Использование политик безопасности для безопасной работы прикладного ПО | Высокий | Создать и применить SecurityPolicy, определяющую ограничения для работы подов (например, запрет привилегированных контейнеров или использование определенных объемов). Попробовать создать под, который нарушает заданные правила безопасности в SecurityPolicy. Проверить, что под не был создан, а в событиях кластера отображается ошибка, связанная с нарушением политики. | SecurityPolicy успешно применена, под с нарушением правил не создан, а соответствующая ошибка зафиксирована в событиях кластера. |  |
| 17 | П. 3.3.5, 3.3.19, 6.1.11, 3.1.7, 6.3.1. | Б-17, Возможность использовать квот в рамках namespaces | Высокий | Создать ресурс ResourceQuota в заданном namespace, указав ограничения на использование вычислительных ресурсов (CPU, памяти и т.д.). Запустить поды, которые запрашивают ресурсов больше, чем разрешено квотой. Проверить, что такие поды не созданы, а в событиях кластера отображаются соответствующие ошибки о превышении квоты. | Ресурс ResourceQuota успешно применен, поды с запросами ресурсов, превышающими ограничения, не созданы, а соответствующие ошибки зафиксированы в событиях кластера. |  |
| 18 | П. 3.3.6, 3.3.8, 6.1.9, 6.1.10, 3.3.5, 6.1.15. | Б-18, Создание изолированного окружения по заготовленному шаблону | Низкий | Создать проект из заранее подготовленного шаблона, используя команду kubectl apply или соответствующий API. Убедиться, что все ресурсы из шаблона автоматически созданы в указанном namespace. Проверить корректность создания ресурсов, включая их статусы и работу. | Проект успешно создан из шаблона, все ресурсы автоматически появились в заданном namespace и работают корректно. |  |
| 19 | П. 3.11.5, 5.2.5, 5.2.10, 3.11.1, 6.12.1, 6.12.2 | Б-19, Обнаружение угроз безопасности анализируя прикладное ПО и контейнеры | Низкий | Настроить модуль безопасности Deckhouse для обнаружения угроз, включая контроль выполнения команд внутри контейнеров. Запустить shell в контейнере прикладного ПО и выполнить действия, которые должны быть зафиксированы системой безопасности. Проверить, что уведомление о подозрительной активности сработало корректно и отобразилось в логах или системах оповещения. | Уведомление о запуске shell в контейнере было успешно зафиксировано и обработано системой безопасности. |  |
| 20 | П. 3.1.3, 3.1.12, 3.2.1, 5.2.8, 5.2.9, 6.12.1 | Б-20, Организация mTLS между узлами прикладного ПО | Высокий | Создать два сервиса, включив в их конфигурацию sidecar istio-proxy. Настроить политику безопасности Istio (PeerAuthentication) для включения mTLS между сервисами. Проверить взаимодействие между сервисами, убедившись, что оно происходит с использованием mTLS, через логи или диагностические инструменты Istio. | Два сервиса с istio-proxy взаимодействуют друг с другом через mTLS, подтвержденное настройками и логами. |  |
| 21 | П. 3.1.10, 3.2.1, 5.2.3, 5.2.5, 6.10.3, 6.12.1. | Б-21, Организация авторизации доступа между сервисами | Высокий | Настроить AuthorizationPolicy в Deckhouse Platform для ограничения взаимодействия между двумя сервисами. Применить политику, определяющую правила авторизации, и включить ее для тестируемых сервисов. Проверить, что неавторизованные запросы между сервисами завершаются с ошибкой. | AuthorizationPolicy успешно применена, и неавторизованные запросы между сервисами завершаются с ошибкой. |  |
| 22 | П. 3.1.9, 3.3.9, 3.11.1, 5.2.2, 5.2.5, 6.10.4, 6.12.1, 6.12.2. | Б-22, Сканирование образов прикладного ПО на наличие известных уязвимостей | Низкий | Запустить контейнеры прикладного ПО в платформе Deckhouse, используя доступные манифесты или Helm-чарты. Настроить модуль безопасности Deckhouse для автоматического сканирования контейнерных образов на наличие известных уязвимостей. Проверить, что результаты сканирования отображаются в CustomResource и на дашбордах Grafana. | Контейнерные образы были успешно отсканированы, результаты сканирования отобразились в CustomResource и дашбордах Grafana. |  |



Таблица 6. Оценка трудозатрат на тестирование

|  |  |
| --- | --- |
| **Количество проверок** | **Общее время прохождения** |
| 22 |  |

### Критерии завершения

Все запланированные тесты были выполнены. Все выявленные ошибки зафиксированы.

## Мониторинг

### Цель тестирования

Проверить, что обеспечиваются требования к ИС "Платформа" на предмет производительности, доступности и корректности работы в реальном времени.

### Проверяемые требования

Таблица 7. Требования тестирования мониторинга

|  |  |  |  |
| --- | --- | --- | --- |
| Номер | Код требования в ТЗ | Краткое описание | Тестовые сценарии в ПМИ |
| 1 | П.3.3.9 | Встроенная система мониторинга на основе стека Prometheus и Grafana | М-1,М-2, М-3, М-8, М-4, М-7, М-6 |
| 2 | П.6.1.10 | Хранение всех настроек системы с поддержкой резервирования и версионирования | М-6, М-7, М-8 |
| 3 | П.6.1.16 | Постоянный контроль соответствия сетевых политик заранее заданным критериям. | М-1 |
| 4 | П.6.3.2 | Возможность вертикального масштабирования Кластера | М-6, М-7 |
| 5 | П.6.6.1 | Наличие механизма автоматического распределения нагрузки. | М-2, М-4, М-6 |
| 6 | П.6.12.2 | Подсистема регистрации событий с модулями для записи, хранения и анализа данных. | М-7, М-8, М-6 |
| 7 | П.3.3.17 | Агрегация доступности компонентов кластера по функциональности и всем кластерам. | М-1, М-2, М-3, М-4, М-7 |
| 8 | П.3.4.2 | Интеграция с системой сбора логов и событий Opensearch. | М-10 |
| 9 | П.6.1.13 | Поддержка отображения схем сетевых взаимодействий через Luntry. | М-1, М-3, М-4 |
| 10 | П.6.2.2 | Архитектура высокой доступности без единой точки отказа. | М-1, М-2, М-3, М-4, М-6 |
| 11 | П.6.3.1. | Горизонтальное масштабирование кластеров без остановки сервиса. | М-7, М-6, М-5 |
| 12 | 6.10.3 | Поддержка сетевых политик внутрикластерного взаимодействия. | М-6, М-10 |

### Методика тестирования

Тестирование отказоустойчивости/восстановления предполагает выполнение тестовых процедур, приведенных в таблице ниже.

Таблица 8. Порядок проведения тестирования мониторинга

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Код требования в ТЗ** | **Название Тестового сценария** | **Приоритет проверки** | **Шаги** | **Ожидаемый результат** | **Время прохождения** |
| **1** | П. 3.3.9 | М-1, Встроенный мониторинг состояния служебных компонент кластера | Высокий | Убедиться, что модуль мониторинга Deckhouse включен и корректно настроен. Проверить наличие в Grafana предустановленных дашбордов и метрик, связанных с состоянием служебных компонентов кластера, включая Deckhouse. Открыть соответствующие дашборды и убедиться в отображении актуальных метрик. | В Grafana присутствуют дашборды с метриками по Deckhouse, отображающими состояние служебных компонентов кластера, и данные обновляются корректно. |  |
| П. 3.3.17 |
| П. 6.1.13 |
| П. 6.1.16 |
| П. 6.2.2 |
| 2 | П. 3.3.9 | М-2, Мониторинг аппаратных ресурсов платформы | Высокий | Убедиться, что модуль мониторинга аппаратных ресурсов (например, node-exporter) включен и настроен в Deckhouse Platform. Проверить наличие в Grafana предустановленных дашбордов и метрик, связанных с мониторингом аппаратных ресурсов узлов кластера. Открыть соответствующие дашборды и убедиться, что метрики по CPU, памяти, диску и сети отображаются корректно. | В Grafana присутствуют дашборды и метрики по аппаратным ресурсам (node-exporter), данные отображаются и обновляются корректно. |  |
| П. 3.3.17 |
| П. 6.2.2 |
| П. 6.6.1 |
| 3 | П. 3.3.9 | М-3, Мониторинг Kubernetes в составе платформы | Высокий | Убедиться, что модуль мониторинга Kubernetes control plane включен и настроен в Deckhouse Platform. Проверить наличие в Grafana предустановленных дашбордов и метрик, отображающих состояние компонентов Kubernetes control plane (API Server, Scheduler, Controller Manager и др.). Открыть соответствующие дашборды и убедиться, что метрики отображаются корректно и обновляются в реальном времени. | В Grafana присутствуют дашборды с метриками по Kubernetes control plane, данные отображаются и обновляются корректно. |  |
| П. 3.3.17 |
| П. 6.1.13 |
| П. 6.2.2 |
| 4 | П. 3.3.9 | М-4, Встроенный мониторинг входящего трафика | Низкий | Убедиться, что модуль мониторинга Ingress Nginx включен и настроен в Deckhouse Platform. Проверить наличие в Grafana дашбордов и метрик, связанных с входящим трафиком, включая состояние и производительность Ingress Nginx. Открыть дашборды и убедиться, что метрики по входящему трафику отображаются корректно. | В Grafana присутствуют дашборды с метриками по Ingress Nginx, данные о входящем трафике отображаются и обновляются корректно. |  |
| П. 3.3.17 |
| П. 6.1.13 |
| П. 6.2.2 |
| П. 6.6.1 |
| 5 | П. 6.3.1 | М-5, Оценка использования ресурсов | Высокий | Убедиться, что модуль мониторинга ресурсов и Capacity Planning включен и настроен в Deckhouse Platform. Проверить наличие в Grafana дашбордов и метрик, связанных с анализом использования ресурсов кластера (CPU, память, диск). Открыть дашборды и убедиться, что данные по текущей загрузке и прогнозированию использования ресурсов отображаются корректно. | В Grafana присутствуют дашборды с метриками по Capacity Planning, данные по использованию ресурсов отображаются и обновляются корректно. |  |
| П. 6.3.2 |
| 6 | П. 3.3.9 | М-6, Уведомления (alerts) по нагрузке серверов кластера, количество ошибочных запросов ingress и пр. | Высокий | Проверить настройки Prometheus в Deckhouse Platform, убедившись, что включены предустановленные правила для уведомлений (alerts). Просмотреть список доступных правил оповещений в Prometheus, связанных с нагрузкой серверов, ошибочными запросами Ingress и другими метриками. Смоделировать условия, вызывающие срабатывание правил, и убедиться, что уведомления генерируются корректно. | В платформе настроен обширный набор уведомлений в Prometheus, правила оповещения работают корректно и охватывают метрики нагрузки серверов, ошибочных запросов Ingress и другие показатели. |  |
| П. 6.2.2 |
| П. 6.6.1 |
| П. 6.12.2 |
| П. 6.1.10 |
| П. 6.3.1 |
| П. 6.3.2 |
| П. 6.10.3 |
| 7 | П. 3.3.9 | М-7, Расширенный мониторинг состояния прикладных сервисов | Средний | Применить лейбл для активации мониторинга на выбранный namespace. Создать заведомо неработающий Deployment в этом namespace (например, указав недоступный образ контейнера). Убедиться, что в Prometheus появляются уведомления (alerts) о проблемах с состоянием Deployment, и проверить отображение соответствующих метрик в Grafana. | После применения лейбла и создания неработающего Deployment в namespace система мониторинга генерирует уведомления о проблемах, и метрики отображаются в Grafana. |  |
| П. 3.3.17 |
| П. 6.1.10 |
| П. 6.3.1 |
| П. 6.3.2 |
| П. 6.12.2 |
| 8 | П. 3.3.9 | М-8, Мониторинг прикладных сервисов | Высокий | Развернуть приложение в кластере, которое генерирует метрики в формате Prometheus. Настроить сбор метрик, создав ServiceMonitor или аналогичный объект для интеграции с Prometheus. Убедиться, что метрики приложения появились в интерфейсе Prometheus и отображаются корректно. | Приложение успешно развернуто, метрики в формате Prometheus собраны и отображаются в интерфейсе Prometheus. |  |
| П. 6.12.2 |
| П. 6.1.10 |
| 9 | П. 6.12.2 | М-9, Возможность добавления своего набора уведомлений (alerts) | Высокий | Создать ресурс CustomPrometheusRule, указав в нем пользовательские правила уведомлений (alerts), включая их условия и действия. Применить созданный ресурс в кластере с помощью команды kubectl apply. Проверить в интерфейсе Prometheus, что новое правило успешно загружено и отображается в списке активных правил. | CustomPrometheusRule успешно создан, пользовательские уведомления подгрузились в Prometheus и отображаются в списке правил. |  |
| П. 6.1.10 |
| 10 | П. 3.4.2 | М-10, Возможность отправки уведомлений (alerts) во внешнюю систему | Высокий | Создать и настроить ресурс CustomAlertmanager, указав конфигурацию для отправки уведомлений во внешнюю систему (например, Slack, email или PagerDuty). Применить конфигурацию в кластере с помощью команды kubectl apply. Создать тестовое условие для срабатывания уведомления и убедиться, что оно успешно отправлено во внешнюю систему. | CustomAlertmanager успешно настроен, уведомления из кластера отправляются во внешнюю систему, и тестовое уведомление было доставлено. |  |
| П. 6.12.2 |
| П. 6.1.10 |
| П. 6.10.3 |



Таблица 9. Оценка трудозатрат на тестирование

|  |  |
| --- | --- |
| **Количество проверок** | **Общее время прохождения** |
| 10 |  |

### Критерий завершения

Все запланированные тесты были выполнены. Все выявленные ошибки зафиксированы.

## Тестирование масштабируемости

### Цель тестирования

Цель тестирования масштабируемости - определение способности системы эффективно справляться с увеличением нагрузки и расширением ресурсов, сохраняя при этом стабильность и удовлетворительное время отклика.

### Проверяемые требования

Таблица 10. Требования тестирования масштабируемости

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер** | **Код требования в ТЗ** | **Краткое описание** | **Тестовые сценарии в ПМИ** |
| 1 | П. 3.1.7 | Платформа должна позволять управлять механизмом распределения подов между узлами кластера. | МШ-1, МШ-5 |
| 2 | П. 3.3.9 | Наличие встроенной системы мониторинга на основе стека Prometheus и Grafana. | МШ-2, МШ-3, МШ-4, МШ-5 |
| 3 | П. 6.1.10 | Все настройки Системы должны храниться в виде объектов или ресурсов кластера (ConfigMap), поддерживать масштабирование, резервирование и версионирование. | МШ-4 |
| 4 | П. 6.1.13 | Состояние Системы должно поддерживать отображение схемы сетевых взаимодействий с помощью ПО Luntry. | МШ-5 |
| 5 | П. 6.10.3 | Поддержка сетевых политик внутрикластерного взаимодействия. | МШ-5 |
| 6 | П. 6.12.2 | Подсистема регистрации событий должна включать модули регистрации, хранения, аудита событий и программного доступа к информации о событиях. | МШ-2 |
| 7 | П. 6.2.2 | Наличие архитектуры высокой доступности, отсутствие единой точки отказа для всех компонентов Системы. | МШ-2, МШ-3, МШ-4 |
| 8 | П. 6.3.1 | Возможность автоматического горизонтального масштабирования Кластера (путем добавления или изъятия узлов) без остановки сервиса. | МШ-1, МШ-2, МШ-4 |
| 9 | П. 6.3.2 | Возможность вертикального масштабирования Кластера (путем добавления вычислительных ресурсов на узлы) без остановки прикладного сервиса. | МШ-2, МШ-3 |
| 10 | П. 6.3.3 | Возможность использования предварительно подготовленных узлов в горячем резерве для моментального масштабирования | МШ-3, МШ-4 |
| 11 | П. 6.6.1 | Наличие механизма автоматического распределения нагрузки. | МШ-1, МШ-2, МШ-3, МШ-4, МШ-5 |
| 12 | П. 6.6.2 | Наличие механизма ограничения нагрузки. | МШ-1 |
| 13 | П. 6.6.3 | Обновления Системы должны выполняться без простоя рабочих нагрузок. | МШ-1 |

### Методика тестирования

Тестирование масштабируемости предполагает выполнение тестовых процедур, приведенных в таблице ниже.

Таблица 11. Порядок проведения тестирования масштабируемости



|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№** | **Код требования в ТЗ** | **Название Тестового сценария** | **Шаги** | **Ожидаемый результат** | **Время прохождения** |
| 1 | П. 3.1.7 | МШ-1, Балансировка нагрузки контейнеров между узлами кластера | Создать Deployment с настройкой podAntiAffinity. Проверить, что поды распределились на разные узлы с помощью команды kubectl get pods -o wide. | Поды Deployment распределились между узлами кластера, соблюдая правила podAntiAffinity. |  |
| П. 6.2.2 |
| П. 6.3.1 |
| П. 6.6.1 |
| П. 6.6.2 |
| П. 6.6.3 |
| 2 | П. 3.3.9 | МШ-2, Масштабирование прикладных сервисов на основе бизнес метрик | Выкатить приложение с метриками в формате Prometheus. Настроить сбор метрик, создать ресурсы IngressMetric/ServiceMetric/PodMetric и HorizontalPodAutoscaler. Подать нагрузку и наблюдать масштабирование через kubectl get hpa. | При увеличении нагрузки сервис автоматически масштабируется, создавая новые поды. |  |
| П. 6.3.1 |
| П. 6.6.1 |
| П. 6.3.2 |
| П. 6.12.2 |
| 3 | П. 3.3.9 | МШ-3, Масштабирование прикладных сервисов на основе потребления ресурсов | Развернуть приложение, создать ресурс VerticalPodAutoscaler в одном из режимов (Auto, Recreate). Подать нагрузку и проверить изменение запросов ресурсов с помощью kubectl describe pods. | Поды пересозданы или ресурсы обновлены в соответствии с нагрузкой, в зависимости от выбранного режима VerticalPodAutoscaler. |  |
| П. 6.3.2 |
| П. 6.3.3 |
| П. 6.6.1 |
| П. 6.12.2 |
| 4 | П. 6.3.1 | МШ-4, Автоматические масштабирование количества узлов кластера | Выкатить Deployment с запросами CPU/RAM, превышающими доступные ресурсы. Подождать 10 минут и проверить, что новый узел добавлен, с помощью команды kubectl get nodes. | К кластеру добавлен новый узел автоматически, обеспечивая удовлетворение запросов приложения. |  |
| П. 6.6.1 |
| П. 3.3.9 |
| П. 6.3.3 |
| П. 6.12.2 |
| П. 6.1.10 |
| 5 | П. 6.6.1 | МШ-5, Автоматические распределение ресурсов между узлами кластера | Создать приложение с нарушением одной из стратегий descheduler (например, дисбаланс CPU). Убедиться, что descheduler перераспределил поды с помощью команды kubectl describe pod. | Поды перераспределены между узлами кластера в соответствии со стратегиями descheduler. |  |
| П. 3.1.7 |
| П. 6.2.2 |
| П. 6.1.13 |
| П. 3.3.9 |
| П. 6.10.3 |

Таблица 12. Оценка трудозатрат на тестирование

|  |  |
| --- | --- |
| **Количество проверок** | **Общее время прохождения** |
| 5 |  |

### Критерий завершения

Все запланированные тесты были выполнены. Все выявленные ошибки зафиксированы.

## Интеграционное тестирование

Интеграционные тесты не предусмотрены, так как система не содержит интеграций с внешними компонентами или системами.

## Прочее тестирование

### Цель тестирования

Цель тестирования – убедиться в корректной работе встроенных механизмов безопасности и управления, включая автоматическое распространение секретов, перезапуск приложений при изменении конфигураций, настройку Ingress для входящего трафика, удалённый сбор и кратковременное хранение логов, а также безопасный доступ к кластеру

### Проверяемые требования

Таблица 13. Требования к прочему тестированию

|  |  |  |  |
| --- | --- | --- | --- |
| **Номер** | **Код требования в ТЗ** | **Краткое описание** | **Тестовые сценарии в ПМИ** |
| 1 | П.3.3.8 | Платформа предоставляет автоматизированный механизм добавления аннотаций и меток к пространствам имен с использованием Annotations. | ПР-1 |
| 2 | П.6.1.8 | Многоарендность реализована с помощью изоляции пространств имен через networkPolicy, RBAC и resourceQuota. | ПР-1 |
| 3 | П.6.1.10 | Все настройки Системы хранятся в объектах ConfigMap с поддержкой масштабирования, резервирования и версионирования. | ПР-2, ПР-4 |
| 4 | П.5.1.3 | Платформа поддерживает интеграцию с решениями для управления секретами | ПР-2 |
| 5 | П.6.10.5 | Gatekeeper проверяет сущности кластера на соответствие политикам безопасности. | ПР-2 |
| 6 | П.3.2.1 | Используемый CNI Cilium обеспечивает фильтрацию пакетов на уровнях L4 и L7. | ПР-3 |
| 7 | П.6.10.3 | Платформа поддерживает создание и применение сетевых политик для управления взаимодействием в кластере. | ПР-3 |
| 8 | П.6.10.4 | Платформа обеспечивает проверку безопасности в соответствии с CIS Benchmark для Kubernetes. | ПР-3 |
| 9 | П.3.3.18 | Платформа поддерживает сбор логов с использованием Vector, Opensearch и Logstash. | ПР-4, ПР-5 |
| 10 | П.6.12.2 | Включены инструменты для работы с Serverless архитектурами, такие как Kubeless и Fission. | ПР-4, ПР-5 |
| 11 | П.5.2.11 | Платформа позволяет журналировать действия и выгружать логи в формате syslog на удаленный сервер. | ПР-4, ПР-5 |
| 12 | П.4.2.5 | Поддерживается интеграция с LDAPS, OAuth 2.0/SAML и двухфакторная аутентификация. | ПР-6 |
| 13 | П.6.10.1.4 | Обеспечивается использование защищенных протоколов TLS 1.3 и HTTPS для взаимодействия между компонентами. | ПР-6 |
| 14 | П.6.10.4 | Наличие средства контроля соответствия конфигурации кластера рекомендациям CIS Benchmarks. | ПР-6 |

### Методика тестирования

Таблица 14. Порядок проведения прочего тестирования

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Код требования в ТЗ** | **Название Тестового сценария** | **Приоритет проверки** | **Шаги** | **Ожидаемый результат** | **Время прохождения** |
| 1 | П. 3.3.8, 6.1.8 | ПР-1, Встроенная возможность автоматического распространения secrets | Высокий | Создать Secret в namespace default с необходимой аннотацией для автоматического распространения. Проверить, что Secret появился во всех namespace с помощью команды kubectl get secrets --all-namespaces. | Secret автоматически распространился во все namespaces. |  |
| 2 | П.6.1.10, 5.1.3, 6.10.5 | ПР-2,Автоматический перезапуск прикладного ПО в случае изменения secret / configmap | Средний | Создать Deployment с аннотацией, активирующей автоматический перезапуск, и использовать ConfigMap. Изменить параметры в ConfigMap и проверить, что поды Deployment перезапустились. | Поды Deployment перезапустились автоматически после изменения ConfigMap. |  |
| 3 | П. 3.2.1, 6.10.3, 6.10.4 | ПР-3, Настройка входящего трафика для кластера (Ingress) | Высокий | Настроить IngressNginx с использованием конфигураций для приема входящего трафика. Создать соответствующие ресурсы Ingress и убедиться, что трафик успешно направляется к целевым приложениям. | Входящий трафик успешно направляется через IngressNginx. |  |
| 4 | П. 3.3.18, 6.12.2, 5.2.11, 6.1.10 | ПР-4, Встроенные инструменты удаленного ведения и агрегации журналов (логов) | Низкий | Настроить модуль логирования для отправки журналов в удаленное хранилище (например, Elasticsearch). Проверить, что журналы отправляются и доступны в удаленном хранилище. | Журналы собираются и отправляются в удаленное хранилище, где доступны для анализа. |  |
| 5 | П. 3.3.18, 6.12.2, 5.2.11 | ПР-5, Встроенная система кратковременного хранения логов | Средний | Установить модуль loki и настроить log-shipper для отправки логов платформы. Убедиться, что логи доступны в интерфейсе Loki. | Логи платформы успешно отправляются и доступны в интерфейсе Loki. |  |
| 6 | П. 4.2.5, 6.10.4, 6.10.1.4 | ПР-6, Доступ к кластеру через OpenVPN | Высокий | Включить модуль OpenVPN, настроить клиента для подключения и подключиться к серверу OpenVPN. Проверить, что подключение установлено, и доступ к кластеру осуществляется через VPN. | Подключение к OpenVPN серверу успешно выполнено, доступ к кластеру через VPN работает корректно. |  |



Таблица 15. Оценка трудозатрат на тестирование

|  |  |
| --- | --- |
| **Количество проверок** | **Общее время прохождения** |
| 6 |  |

### Критерий завершения

Все запланированные тесты были выполнены. Все выявленные ошибки зафиксированы.