

# Установка и настройка VMware vRealize Orchestrator

6 октября 2020 г.  
vRealize Orchestrator 8.2

Актуальная техническая документация доступна на веб-сайте VMware:

<https://docs.vmware.com/ru/>

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**VMware Россия**  
Россия, 125284, г. Москва  
ул. Беговая, д.3, стр.1  
Бизнес-центр "NORDSTAR TOWER" 30й этаж  
Телефон: +7 495 212 29 00  
[www.vmware.com/ru](http://www.vmware.com/ru)

© 2008–2020 VMware, Inc. Все права защищены. [Информация об авторских правах и товарных знаках.](#)

# Содержание

Установка и настройка VMware vRealize Orchestrator	6
<b>1 Знакомство с VMware vRealize Orchestrator</b>	<b>7</b>
Основные характеристики платформы Orchestrator	7
Роли пользователей в vRealize Orchestrator	10
Архитектура vRealize Orchestrator	11
Подключаемые модули vRealize Orchestrator	12
<b>2 Требования к системе для vRealize Orchestrator</b>	<b>13</b>
Требования к оборудованию для vRealize Orchestrator Appliance	13
Браузеры, поддерживаемые vRealize Orchestrator	14
База данных vRealize Orchestrator	14
Компоненты vRealize Orchestrator Appliance	14
Уровень поддержки интернационализации и локализации	14
Порты и конечные точки vRealize Orchestrator	15
<b>3 Настройка компонентов vRealize Orchestrator</b>	<b>17</b>
Настройка vCenter Server	17
Способы проверки подлинности	17
<b>4 Установка vRealize Orchestrator</b>	<b>19</b>
Загрузка и развертывание vRealize Orchestrator Appliance	19
Включение vRealize Orchestrator Appliance и переход на главную страницу	21
Изменение срока действия пароля пользователя root	21
Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH	21
<b>5 Первичная настройка</b>	<b>23</b>
Настройка автономного сервера vRealize Orchestrator	23
Настройка автономного сервера vRealize Orchestrator с проверкой подлинности vRealize Automation	23
Настройка автономного сервера vRealize Orchestrator с проверкой подлинности vSphere	25
Включение функций vRealize Orchestrator с помощью лицензий	26
Подключение базы данных vRealize Orchestrator	27
Управление сертификатами	27
Управление сертификатами vRealize Orchestrator	27
Настройка подключаемых модулей vRealize Orchestrator	32
Управление подключаемыми модулями vRealize Orchestrator	32
Установка и обновление подключаемого модуля vRealize Orchestrator	33

Удаление подключаемого модуля	34
Доступность и масштабируемость vRealize Orchestrator	34
Настройка кластера vRealize Orchestrator	35
Удаление узла из кластера vRealize Orchestrator	37
Горизонтальное масштабирование автономного развертывания vRealize Orchestrator	37
Мониторинг кластера vRealize Orchestrator	39
Настройка программы улучшения качества программного обеспечения	39
Категории информации, предоставляемой компании VMware	39
Присоединение к программе улучшения качества программного обеспечения и выход из нее	40
<b>6 Использование служб API-интерфейса vRealize Orchestrator</b>	<b>41</b>
Управление сертификатами SSL с помощью REST API	41
Удаление сертификата TLS с помощью REST API	42
Импорт сертификатов TLS с помощью REST API	42
Создание хранилища ключей с помощью REST API	43
Удаление хранилища ключей с помощью REST API	44
Добавление ключа с помощью REST API	44
<b>7 Дополнительные параметры конфигурации</b>	<b>46</b>
Повторная настройка проверки подлинности	46
Изменение поставщика проверки подлинности	46
Изменение параметров проверки подлинности	47
Настройка свойств выполняемого рабочего процесса	47
Файлы журналов vRealize Orchestrator	48
Сохраняемость журналов	48
Настройка журналов vRealize Orchestrator	49
Настройка интеграции ведения журнала с vRealize Log Insight	50
Создание или перезапись интеграции системного журнала в vRealize Orchestrator	50
Включение ведения журнала отладки Kerberos	52
Включение расширений Opentracing и Wavefront	53
Настройка расширения Opentracing	54
Настройка расширения Wavefront	54
Включение синхронизации времени в vRealize Orchestrator	56
Отключение синхронизации времени в vRealize Orchestrator	57
<b>8 Конфигурация: примеры использования и устранение неполадок</b>	<b>58</b>
Настройка подключаемого модуля vRealize Orchestrator для vSphere Web Client	58
Отмена выполняемых рабочих процессов	59
Включение отладки сервера vRealize Orchestrator	60
Изменение размера дисков vRealize Orchestrator Appliance	62
Масштабирование объема памяти кучи на сервере vRealize Orchestrator	62

Аварийное восстановление vRealize Orchestrator с помощью Site Recovery Manager	64
Настройка виртуальных машин для vSphere Replication	64
Создание групп защиты	65
Создание плана восстановления	67
Упорядочение планов восстановления по папкам	68
Изменение плана восстановления	69

## **9 Настройка свойств системы 70**

Настройка доступа к файловой системе сервера для рабочих процессов и действий	70
Правила в файле js-io-rights.conf, разрешающие доступ для записи в системе vRealize Orchestrator	70
Настройка доступа к файловой системе сервера для рабочих процессов и действий	71
Настройка доступа к командам операционной системы для рабочих процессов и действий	72
Настройка доступа JavaScript к классам Java	73
Задание свойства настраиваемого времени ожидания	74
Добавление соединителя JDBC для подключаемого модуля SQL vRealize Orchestrator	75

## **10 Дальнейшие действия 77**

# Установка и настройка VMware vRealize Orchestrator

В руководстве *Установка и настройка VMware vRealize Orchestrator* представлены сведения и инструкции по установке и настройке VMware® vRealize Orchestrator.

## Целевая аудитория

Эта информация предназначена для профессиональных администраторов vSphere и опытных системных администраторов, знакомых с технологией виртуальных машин и функционированием центра обработки данных.

# Знакомство с VMware vRealize Orchestrator

# 1

VMware vRealize Orchestrator — платформа для автоматизации разработки и процессов, которая предоставляет библиотеку расширяемых рабочих процессов, позволяющую создавать и запускать автоматизированные настраиваемые процессы для управления продуктами VMware, а также технологическими решениями сторонних разработчиков.

vRealize Orchestrator автоматизирует управление и рабочие задачи и приложений VMware, и сторонних приложений, таких как службы поддержки, системы управления изменениями и системы управления ИТ-ресурсами.

В эту главу входят следующие разделы:

- [Основные характеристики платформы Orchestrator](#)
- [Роли пользователей в vRealize Orchestrator](#)
- [Архитектура vRealize Orchestrator](#)
- [Подключаемые модули vRealize Orchestrator](#)

## Основные характеристики платформы Orchestrator

vRealize Orchestrator состоит из трех уровней: платформа оркестрации, которая предоставляет общие функции, необходимые для инструмента оркестрации; архитектура подключаемых модулей для интеграции управления подсистемами; библиотека рабочих процессов. vRealize Orchestrator — это открытая платформа, которую можно расширить с помощью новых подключаемых модулей и содержимого, а также интегрировать в более крупные архитектуры посредством REST API.

vRealize Orchestrator обладает несколькими ключевыми возможностями, которые помогают в выполнении рабочих процессов и управлении ими.

### Устойчивость

База данных промышленного уровня PostgreSQL используется для хранения необходимой информации, такой как процессы, состояния рабочих процессов и конфигурация vRealize Orchestrator.

### Централизованное управление

vRealize Orchestrator предоставляет средство для централизованного управления процессами. Платформа на основе сервера приложений с полным журналом версий может хранить сценарии и примитивы, связанные с процессами, в одном месте хранения. Это позволяет избежать присутствия на серверах сценариев без контроля версий и надлежащего управления изменениями.

### Контрольные точки

Каждый этап рабочего процесса сохраняется в базе данных, что предотвращает потерю данных при необходимости перезапустить сервер. Эта функция особенно полезна для длительных процессов.

### Центр управления

Центр управления — это веб-портал, который позволяет повысить эффективность администрирования экземпляров vRealize Orchestrator за счет предоставления централизованного административного интерфейса для операций среды выполнения, мониторинга рабочих процессов и сопоставления запущенных рабочих процессов и системных ресурсов.

### Управление версиями

Каждый объект платформы vRealize Orchestrator имеет связанный журнал версий. Журнал версий полезен для базового управления изменениями при распределении процессов по этапам или местоположениям проекта.

### Интеграция Git

vRealize Orchestrator Client позволяет интегрировать репозитории Git, чтобы дополнительно улучшить управление версиями и исходным кодом содержимого vRealize Orchestrator. С помощью Git можно управлять разработкой рабочих процессов сразу в нескольких экземплярах vRealize Orchestrator. См. раздел *Использование Git с клиентом vRealize Orchestrator* руководства *Использование клиента VMware vRealize Orchestrator*.

### Обработчик сценариев

Обработчик JavaScript Mozilla Rhino позволяет создавать строительные блоки для платформы vRealize Orchestrator Client. Этот обработчик сценариев дополнен базовыми функциями контроля версий, проверки типов переменных, управления пространством имен и обработки исключений. Его можно использовать в следующих строительных блоках:

- Действия
- Рабочие процессы
- Политики

### Обработчик рабочих процессов

Обработчик рабочих процессов позволяет автоматизировать бизнес-процессы. В нем используются следующие объекты для пошаговой автоматизации в рабочих процессах:

- Рабочие процессы и действия, которые предоставляет vRealize Orchestrator Client.
- Пользовательские строительные блоки, созданные заказчиком.
- Объекты, добавляемые в vRealize Orchestrator Client подключаемыми модулями.



Рабочие процессы могут запускаться пользователями, другими рабочими процессами, планировщиками и политиками.

### Обработчик политик

Обработчик политик используется для мониторинга и создания событий в целях реагирования на изменение условий на сервере vRealize Orchestrator Client или в технологии подключаемого модуля. Политики могут объединять события платформы и подключаемых модулей, что помогает обрабатывать изменения в условиях любой из интегрированных технологий.

### vRealize Orchestrator Client

Создавайте, запускайте, изменяйте и отслеживайте рабочие процессы с помощью vRealize Orchestrator Client. Кроме того, vRealize Orchestrator Client можно использовать для управления действиями, настройками, политиками и элементами ресурсов. См. руководство *Использование клиента VMware vRealize Orchestrator*.

### Разработка и ресурсы

На начальной странице vRealize Orchestrator предоставляется быстрый доступ к ресурсам, которые позволяют разрабатывать собственные подключаемые модули для использования в vRealize Orchestrator. Кроме того, там находится информация об использовании vRealize Orchestrator REST API для отправки запросов на сервер vRealize Orchestrator.

### Безопасность

vRealize Orchestrator предоставляет следующие расширенные возможности безопасности.

- Инфраструктура открытых ключей (Public Key Infrastructure, PKI) для подписи и шифрования содержимого, импортируемого и экспортируемого между серверами.
- Управление цифровыми правами (Digital Rights Management, DRM) позволяет указывать, как можно просматривать, изменять и распространять экспортируемое содержимое.
- Протокол TLS (Transport Layer Security) для обеспечения зашифрованного обмена данными между vRealize Orchestrator Client, сервером vRealize Orchestrator и доступом по протоколу HTTPS к пользовательскому веб-интерфейсу.
- Расширенное управление правами доступа для контроля доступа к процессам и объектам, которыми управляют эти процессы.

### Шифрование

vRealize Orchestrator использует стандарт AES, соответствующий требованиям Федерального стандарта по обработке информации (Federal Information Processing Standard, FIPS), с 256-битным ключом шифрования для шифрования строк. Ключ шифра создается случайным образом и уникален для устройств, которые не являются частью кластера. Все узлы в кластере совместно используют один ключ шифра.

## Роли пользователей в vRealize Orchestrator

vRealize Orchestrator предоставляет различные инструменты и интерфейсы на основе определенных обязанностей глобальных ролей пользователей. В vRealize Orchestrator можно создавать пользователей с полными правами, которые являются частью группы администраторов (**администраторы**), разработчиков (**разработчики рабочих процессов**) и пользователей с ограниченным доступом.

### Роли и обязанности в vRealize Orchestrator

Управлять ролями пользователей vRealize Orchestrator можно с помощью меню **Управление ролями** в vRealize Orchestrator Client. Дополнительные сведения о настройке ролей пользователей в vRealize Orchestrator Client см. в разделе *Назначение ролей в клиенте vRealize Orchestrator* руководства *Использование клиента VMware vRealize Orchestrator*.

---

**Примечание** Для развертываний vRealize Orchestrator с проверкой подлинности vRealize Automation или лицензией vRealize Automation роли пользователей назначаются службой управления учетными данными и доступом платформы vRealize Automation. См. раздел *Настройка ролей клиента vRealize Orchestrator в vRealize Automation* в руководстве *Использование клиента VMware vRealize Orchestrator*.

---

#### Администратор

Этот пользователь имеет полный доступ ко всем возможностям и содержимому платформы vRealize Orchestrator, в том числе к содержимому, созданному конкретными группами. Основные обязанности администратора включают следующее:

- установка и настройка vRealize Orchestrator;
- добавление пользователей в vRealize Orchestrator Client, назначение ролей, создание и удаление групп (см. раздел *Создание групп в клиенте vRealize Orchestrator* в руководстве *Использование клиента VMware vRealize Orchestrator*);
- создание интеграции с репозиторием Git для разработчиков в их среде vRealize Orchestrator (см. раздел *Настройка подключения к репозиторию Git* в руководстве *Использование клиента VMware vRealize Orchestrator*);
- устранение неполадок в среде vRealize Orchestrator с помощью таких функций, как проверка рабочих процессов и отладочные сценарии для рабочих процессов.

#### Разработчик рабочего процесса

Этот пользователь может расширить функциональные возможности платформы vRealize Orchestrator, создавая и изменяя объекты. Разработчики рабочих процессов не имеют доступа к функциям администрирования и устранения неполадок vRealize Orchestrator Client. Основные обязанности разработчиков рабочих процессов включают следующие:

- создание, редактирование, запуск и удаление объектов vRealize Orchestrator, таких как рабочие процессы, действия, политики и элементы конфигурации;

- планирование запусков рабочих процессов (см. раздел *Планирование рабочих процессов в клиенте vRealize Orchestrator* в руководстве *Использование клиента VMware vRealize Orchestrator*);
- добавление содержимого, созданного разработчиком рабочего процесса, в группы, членами которых они являются;
- отправка локальных изменений в иерархии содержимого vRealize Orchestrator в подключенные репозиторий Git (см. раздел *Отправка изменений в репозиторий Git* в руководстве *Использование клиента VMware vRealize Orchestrator*).

### Пользователи с ограниченными правами

Пользователи, которым не назначена роль, по-прежнему могут входить в vRealize Orchestrator Client, но имеют ограниченный доступ к функциям и содержимому клиента. Если пользователь включен в группу, он может просматривать и запускать содержимое этой группы.

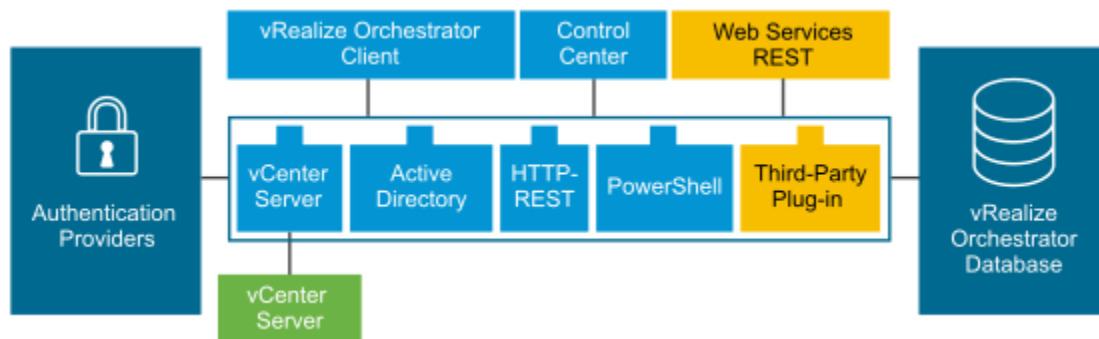
## Архитектура vRealize Orchestrator

vRealize Orchestrator содержит библиотеку рабочих процессов и обработчик рабочих процессов, что позволяет создавать и запускать рабочие процессы, которые обеспечивают автоматизацию процессов оркестрации. Можно запускать рабочие процессы на объектах различных технологий, доступ к которым в vRealize Orchestrator осуществляется с помощью ряда подключаемых модулей.

vRealize Orchestrator предоставляет стандартный набор подключаемых модулей, в том числе подключаемый модуль для vCenter Server, который позволяет управлять задачами в разных средах, предоставляемых подключаемыми модулями.

Решение vRealize Orchestrator основано на открытой архитектуре, позволяющей подключать к платформе оркестрации внешние сторонние приложения. Можно запускать рабочие процессы на объектах самостоятельно определяемых подключенных внешних технологий. vRealize Orchestrator подключается к средству проверки подлинности (для управления учетными записями пользователей), а также к предварительно настроенной базе данных PostgreSQL (для сохранения информации из выполняемых рабочих процессов). Работать с решением vRealize Orchestrator, объектами, которые оно предоставляет, и рабочими процессами vRealize Orchestrator можно через интерфейс клиента vRealize Orchestrator Client или через веб-службы. Мониторинг и настройка рабочих процессов и служб vRealize Orchestrator осуществляется через vRealize Orchestrator Client и центр управления.

Рис. 1-1. Архитектура VMware vRealize Orchestrator



## Подключаемые модули vRealize Orchestrator

Подключаемые модули позволяют использовать vRealize Orchestrator для получения доступа к сторонним системам и приложениям, а также управлять ими. Использование внешних решений в подключаемых модулях vRealize Orchestrator предоставляет возможность включать объекты и функции в рабочие процессы, которые обеспечивают получение доступа к объектам и функциям этих внешних решений.

Внешние решения, которые можно использовать с помощью подключаемых модулей, включают в себя средства управления виртуализацией, системы электронной почты, базы данных, службы каталогов и интерфейсы удаленного управления.

vRealize Orchestrator предоставляет набор стандартных подключаемых модулей, которые можно использовать для внедрения в рабочие процессы таких технологий, как API-интерфейс VMware vCenter Server и возможности электронной почты. С помощью подключаемых модулей можно автоматизировать предоставление новых ИТ-услуг или адаптировать возможности существующей инфраструктуры и служб приложений. Кроме того, открытая архитектура подключаемых модулей для vRealize Orchestrator дает возможность разрабатывать подключаемые модули для доступа к другим приложениям.

Подключаемые модули vRealize Orchestrator, разрабатываемые VMware, распространяются в виде файлов VMOAPP. Дополнительные сведения о подключаемых модулях vRealize Orchestrator, разрабатываемых и предоставляемых VMware, см. в разделе [Внешние подключаемые модули vRealize Orchestrator](#). Дополнительные сведения о подключаемых модулях vRealize Orchestrator сторонних производителей см. на странице [VMware Solution Exchange](#).

# Требования к системе для vRealize Orchestrator

## 2

Для правильной работы vRealize Orchestrator система должна соответствовать техническим требованиям.

Список поддерживаемых версий vCenter Server, vSphere Web Client, vRealize Automation и других решений VMware см. в разделе [Матрица совместимости продуктов VMware](#).

В эту главу входят следующие разделы:

- [Требования к оборудованию для vRealize Orchestrator Appliance](#)
- [Браузеры, поддерживаемые vRealize Orchestrator](#)
- [База данных vRealize Orchestrator](#)
- [Компоненты vRealize Orchestrator Appliance](#)
- [Уровень поддержки интернационализации и локализации](#)
- [Порты и конечные точки vRealize Orchestrator](#)

## Требования к оборудованию для vRealize Orchestrator Appliance

vRealize Orchestrator Appliance — это предварительно настроенная виртуальная машина на базе Photon, запуск которой осуществляется в контейнерах. Перед развертыванием устройства убедитесь, что система соответствует минимальным требованиям к оборудованию.

vRealize Orchestrator Appliance предъявляет следующие требования к оборудованию:

- 4 ЦП
- 12 ГБ памяти
- 200 ГБ на жестком диске

Не уменьшайте размер памяти по умолчанию, поскольку для сервера vRealize Orchestrator требуется по крайней мере 8 ГБ свободной памяти.

## Браузеры, поддерживаемые vRealize Orchestrator

Убедитесь, что используемые браузеры поддерживают vRealize Orchestrator.

Для доступа к vRealize Orchestrator Client и центру управления необходимо использовать один из следующих браузеров:

- Microsoft Edge
- Mozilla Firefox
- Google Chrome

## База данных vRealize Orchestrator

Сервер vRealize Orchestrator включает предварительно настроенную базу данных PostgreSQL, полностью готовую к работе.

## Компоненты vRealize Orchestrator Appliance

vRealize Orchestrator Appliance является виртуальным устройством на базе Photon, запуск которого осуществляется в контейнерах.

vRealize Orchestrator Appliance Включает следующие компоненты:

- слой Kubernetes уровня инфраструктуры;
- предварительно настроенная база данных PostgreSQL;
- основные службы vRealize Orchestrator: служба сервера, служба центра управления и служба пользовательского интерфейса оркестрации.

Конфигурация базы данных vRealize Orchestrator Appliance, заданная по умолчанию, подходит для использования в производственной среде.

---

**Примечание** Чтобы использовать vRealize Orchestrator Appliance в производственной среде, необходимо настроить для сервера vRealize Orchestrator проверку подлинности vRealize Automation или vSphere. См. раздел [Настройка автономного сервера vRealize Orchestrator](#).

---

## Уровень поддержки интернационализации и локализации

Центр управления vRealize Orchestrator и vRealize Orchestrator Client включают поддержку операционных систем и форматов данных на языках, отличных от английского, а также многоязычную поддержку для центра управления и пользовательского интерфейса клиента.

Центр управления vRealize Orchestrator и vRealize Orchestrator Client поддерживают использование операционных систем, ввода и вывода, а также форматов данных, таких как дата, время и числа, на языках, отличных от английского.

Пользовательские интерфейсы vRealize Orchestrator и vRealize Orchestrator Client переведены на следующие языки:

- Испанский
- Французский
- Немецкий
- Китайский (традиционное письмо)
- Китайский (упрощенное письмо)
- Корейский
- Японский
- Итальянский
- Голландский
- Португальский (Бразилия)
- Русский

## Порты и конечные точки vRealize Orchestrator

Служба Kubernetes vRealize Orchestrator включает две конечные точки и несколько основных сетевых портов.

### Сетевые порты и конечные точки vRealize Orchestrator

Доступ к vRealize Orchestrator можно получить через порт 443. Порт 443 защищен самозаверяющим сертификатом, который создается при установке и не может быть заменен пользователем. При использовании внешней подсистемы балансировки нагрузки ее необходимо настроить для балансировки по порту 443.

Протокол	Номер порта	Описание
TCP	22	Порт для доступа к vRealize Orchestrator Appliance по протоколу SSH.
TCP	443	Порт для доступа к vRealize Orchestrator.
TCP	2379	Внутренний порт, используемый хранилищем «ключ-значение» etcd.
TCP	2380	Внутренний порт, используемый хранилищем «ключ-значение» etcd.
TCP	6443	Внутренний порт, используемый сервером API-интерфейса kube-apiserver.
TCP	8008	Внутренний порт, используемый сетевым прокси-сервером kube-proxy.

Протокол	Номер порта	Описание
TCP	10250	Порт, используемый агентом kubelet.
TCP	16000	Внутренний порт.
TCP	20849	Внутренний порт.
TCP	30333	Внутренний порт, используемый службой mitm proxy.
TCP	30821	Внутренний порт.
TCP	31090	Внутренний порт.
UDP	500	Внутренний порт, используемый службой трафика внутреннего обмена ключами (IKE).
UDP	4500	Внутренний порт, используемый службой преобразования сетевых адресов (NAT).
UDP	8285	Внутренний порт, используемый сетевым прокси-сервером kube-proxy.

Доступ к службам клиента и центра управления vRealize Orchestrator можно получить в следующих конечных точках:

[https://FQDN\\_оркестратора/orchestration-ui](https://FQDN_оркестратора/orchestration-ui)

[https://FQDN\\_оркестратора/vco-controlcenter](https://FQDN_оркестратора/vco-controlcenter)



# Настройка компонентов vRealize Orchestrator

# 3

После загрузки и развертывания vRealize Orchestrator Appliance сервер vRealize Orchestrator является предварительно настроенным. После развертывания службы запускаются автоматически.

Чтобы повысить доступность и масштабируемость настроек vRealize Orchestrator, следуйте приведенным ниже рекомендациям.

- Выполните установку и настройку поставщика проверки подлинности и настройте vRealize Orchestrator для работы с ним. См. раздел [Настройка автономного сервера vRealize Orchestrator](#).
- Для кластерных сред vRealize Orchestrator установите и настройте сервер балансировки нагрузки и настройте его для распределения рабочей нагрузки между серверами vRealize Orchestrator.

В эту главу входят следующие разделы:

- [Настройка vCenter Server](#)
- [Способы проверки подлинности](#)

## Настройка vCenter Server

Увеличение количества экземпляров vCenter Server в настройках vRealize Orchestrator приводит к тому, что vRealize Orchestrator приходится управлять дополнительными сеансами. Слишком большое число активных сеансов может привести к превышению времени ожидания в vRealize Orchestrator при наличии более 10 подключений к vCenter Server.

Список поддерживаемых версий vCenter Server см. в разделе [Матрица совместимости продуктов VMware](#).

---

**Примечание** Если сеть имеет достаточную пропускную способность и низкую задержку, можно запустить несколько экземпляров vCenter Server на разных виртуальных машинах, входящих в настройку vRealize Orchestrator. При использовании локальной сети для улучшения связи между vRealize Orchestrator и vCenter Server требуется подключение со скоростью не менее 100 Мбит.

---

## Способы проверки подлинности

Для проверки подлинности и управления разрешениями пользователей в vRealize Orchestrator требуется подключение к экземпляру сервера vRealize Automation или vSphere.

При загрузке и развертывании vRealize Orchestrator Appliance необходимо указать в настройках сервер с проверкой подлинности vRealize Automation или vSphere. См. раздел [Настройка автономного сервера vRealize Orchestrator](#).

---

**Примечание** Проверка подлинности vRealize Orchestrator 8.x с vRealize Automation поддерживается только для vRealize Automation 8.x.

---

# Установка vRealize Orchestrator

# 4

vRealize Orchestrator состоит из сервера и клиента.

Чтобы использовать vRealize Orchestrator, необходимо развернуть vRealize Orchestrator Appliance и настроить сервер vRealize Orchestrator.

Параметры конфигурации vRealize Orchestrator по умолчанию можно изменить с помощью центра управления vRealize Orchestrator.

В эту главу входят следующие разделы:

- [Загрузка и развертывание vRealize Orchestrator Appliance](#)

## Загрузка и развертывание vRealize Orchestrator Appliance

Чтобы получить доступ к содержимому и службам vRealize Orchestrator, необходимо загрузить и развернуть vRealize Orchestrator Appliance.

### Необходимые условия

- Убедитесь, что запущен экземпляр vCenter Server. Необходимо использовать vCenter Server версии 6.0 или более поздней.
- Убедитесь, что узел, на котором проводится развертывание vRealize Orchestrator Appliance, соответствует минимальным требованиям к оборудованию. См. раздел [Требования к оборудованию для vRealize Orchestrator Appliance](#).
- Если система изолирована и не имеет доступа к Интернету, необходимо загрузить файл .ova для устройства с веб-сайта VMware.

### Процедура

1. Войдите в vSphere Web Client от имени **администратора**.
2. Выберите объект иерархии, который является действующим родительским объектом виртуальной машины (например, центр обработки данных, папка, кластер, пул ресурсов или узел).
3. Выберите **Действия > Развернуть шаблон OVF**.
4. Введите путь или URL-адрес для доступа к файлу .ova и нажмите кнопку **Далее**.

5. Введите имя и местоположение vRealize Orchestrator Appliance, затем нажмите кнопку **Далее**.
6. Выберите узел, кластер, пул ресурсов или vApp в качестве места назначения, где будет выполнен запуск устройства, и нажмите **Далее**.
7. Прочтите сведения о развертывании и нажмите кнопку **Далее**.
8. Примите условия лицензионного соглашения и нажмите кнопку **Далее**.
9. Выберите формат хранения для vRealize Orchestrator Appliance.

Формат	Описание
<b>Формат «толстой» подготовки типа Lazy Zero</b>	Создание виртуального диска в толстом формате по умолчанию. Пространство, необходимое для виртуального диска, выделяется при создании виртуального диска. Если какие-либо данные останутся на физическом устройстве, они не удаляются во время создания, но могут быть удалены по требованию при первой записи с виртуальной машины.
<b>Формат «толстой» подготовки типа Eager Zero</b>	Поддержка возможностей кластеризации, например отказоустойчивости. Пространство, необходимое для виртуального диска, выделяется при создании виртуального диска. Если на физическом устройстве остались данные, они будут сброшены после создания виртуального диска. Создание дисков в этом формате может занимать намного больше времени, чем создание дисков в других форматах.
<b>Формат «тонкой» подготовки</b>	Экономия места на жестком диске. Для тонкого диска подготавливается столько пространства хранилища данных, сколько диску необходимо в соответствии со значением, выбранным в качестве размера диска. Тонкий диск не требует ресурсов и использует столько пространства хранилища данных, сколько нужно для первоначальных операций.

10. Нажмите кнопку **Далее**.
11. Настройте параметры сети и введите пароль пользователя **root**.

При настройке параметров сети для vRealize Orchestrator Appliance необходимо использовать протокол IPv4. Для настройки конфигурации DHCP и статической сети необходимо добавить для vRealize Orchestrator Appliance полное доменное имя (FQDN).

Если в качестве имени узла, которое отображается в оболочке vRealize Orchestrator Appliance после развертывания, указано *photon-machine*, значит, вышеупомянутые требования к конфигурации сети не выполняются.

12. (дополнительно) Настройте дополнительные параметры сети для vRealize Orchestrator Appliance, такие как включение доступа по протоколу SSH.
13. Нажмите кнопку **Далее**.
14. Ознакомьтесь с содержимым страницы **Готово к выполнению** и нажмите кнопку **Готово**.

## Результаты

Развертывание vRealize Orchestrator Appliance успешно проведено.

### Следующие шаги

Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root** и убедитесь, что можете выполнять прямой или обратный просмотр DNS.

- Чтобы выполнить прямой просмотр DNS, запустите команду `nslookup FQDN_оркестратора`. Команда должна вернуть IP-адрес vRealize Orchestrator Appliance.
- Чтобы выполнить обратный просмотр DNS, выполните команду `nslookup IP-адрес_оркестратора`. Команда должна вернуть полное доменное имя vRealize Orchestrator Appliance.

## Включение vRealize Orchestrator Appliance и переход на главную страницу

Чтобы использовать автономный экземпляр vRealize Orchestrator Appliance, необходимо сначала включить его.

### Процедура

1. Войдите в vSphere Web Client в качестве **администратора**.
2. Щелкните правой кнопкой мыши vRealize Orchestrator Appliance и выберите **Питание > Включить**.
3. В веб-браузере перейдите к адресу узла виртуальной машины vRealize Orchestrator Appliance, которая была настроена во время развертывания OVA.

`https://FQDN_оркестратора/vco.`

## Изменение срока действия пароля пользователя root

По умолчанию срок действия пароля пользователя root в vRealize Orchestrator Appliance истекает через 365 дней.

### Необходимые условия

- Загрузите и разверните vRealize Orchestrator Appliance.
- Убедитесь, что vRealize Orchestrator Appliance находится в рабочем состоянии.

### Процедура

1. Войдите в vRealize Orchestrator Appliance через SSH в качестве **пользователя root**.
2. Запустите команду `passwd -x число_днейчисло_днейroot`.
3. Чтобы увеличить срок действия пароля пользователя root до бесконечности, запустите команду `passwd -x 99999 root`.

## Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH

Можно включать и отключать доступ к vRealize Orchestrator Appliance по протоколу SSH.

### Необходимые условия

- Загрузите и разверните vRealize Orchestrator Appliance.
- Убедитесь, что vRealize Orchestrator Appliance находится в рабочем состоянии.

### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Чтобы включить доступ по протоколу SSH, запустите команду `/usr/bin/toggle-ssh enable`.
3. Чтобы отключить доступ по протоколу SSH, запустите команду `/usr/bin/toggle-ssh disable`.

# Первичная настройка

# 5

Прежде чем приступать к автоматизации задач и управлению системами и приложениями с помощью vRealize Orchestrator, необходимо задать настройки внешнего поставщика проверки подлинности с помощью центра управления vRealize Orchestrator. Кроме того, центр управления vRealize Orchestrator можно использовать для дополнительных задач настройки, таких как управление сведениями о лицензиях и сертификатах, установка подключаемых модулей и мониторинг состояния кластера vRealize Orchestrator.

В эту главу входят следующие разделы:

- [Настройка автономного сервера vRealize Orchestrator](#)
- [Включение функций vRealize Orchestrator с помощью лицензий](#)
- [Подключение базы данных vRealize Orchestrator](#)
- [Управление сертификатами](#)
- [Настройка подключаемых модулей vRealize Orchestrator](#)
- [Доступность и масштабируемость vRealize Orchestrator](#)
- [Настройка программы улучшения качества программного обеспечения](#)

## Настройка автономного сервера vRealize Orchestrator

vRealize Orchestrator Appliance является предварительно настроенной виртуальной машиной на базе Photon, однако, чтобы получить доступ к полному набору возможностей центра управления vRealize Orchestrator и vRealize Orchestrator Client, необходимо сначала задать конфигурацию поставщика проверки подлинности.

### Настройка автономного сервера vRealize Orchestrator с проверкой подлинности vRealize Automation

Чтобы подготовить vRealize Orchestrator Appliance к использованию, необходимо настроить параметры узла и поставщика проверки подлинности. Можно настроить выполнение проверки подлинности в vRealize Orchestrator с помощью vRealize Automation. Для проверки подлинности vRealize Automation следует использовать vRealize Automation 8.x.

## Необходимые условия

- Загрузите и разверните последнюю версию vRealize Orchestrator Appliance. См. раздел [Загрузка и развертывание vRealize Orchestrator Appliance](#).
- Установите и настройте vRealize Automation 8.x. Убедитесь, что сервер vRealize Automation работает. См. документацию по vRealize Automation.

Если планируется создать кластер, выполните следующие действия.

- Настройте подсистему балансировки нагрузки для распределения трафика между несколькими экземплярами vRealize Orchestrator. См. [Руководство по балансировке нагрузки для VMware vRealize Orchestrator](#).

## Процедура

1. Откройте центр управления, чтобы запустить мастер настройки.
  - а) Перейдите по адресу `https://FQDN_оркестратора/vco-controlcenter`.
  - б) Войдите в качестве **пользователя root** с помощью пароля, который использовался в процессе развертывания OVA.
2. Настройте поставщика проверки подлинности.
  - а) На странице **Настройка поставщика проверки подлинности** выберите **vRealize Automation** в раскрывающемся меню **Режим проверки подлинности**.
  - б) В текстовом поле **Адрес узла** введите адрес узла vRealize Automation и нажмите **ПОДКЛЮЧИТЬ**.

Адрес узла vRealize Automation должен быть в формате `https://имя_хоста_vra`.
  - в) Щелкните **Принять сертификат**.
  - г) Введите учетные данные владельца организации vRealize Automation, от имени которых будет выполнена настройка vRealize Orchestrator. Нажмите **ЗАРЕГИСТРИРОВАТЬ**.
  - д) Нажмите **СОХРАНИТЬ ИЗМЕНЕНИЯ**.

Появится сообщение об успешном сохранении конфигурации.

## Результаты

Настройка сервера vRealize Orchestrator была выполнена успешно.

## Следующие шаги

- Перейдите на страницу **Лицензирование** и убедитесь, что поставщиком лицензии является **CSP**.
- Перейдите на страницу **Проверить конфигурацию** и убедитесь, что узел настроен правильно.

---

**Примечание** После настройки поставщика проверки подлинности сервер vRealize Orchestrator будет автоматически перезагружен через 2 минуты. Если проверить конфигурацию сразу после проверки подлинности, можно получить недопустимое состояние конфигурации.

---



## Настройка автономного сервера vRealize Orchestrator с проверкой подлинности vSphere

Для регистрации сервера vRealize Orchestrator на сервере vCenter Single Sign-On используется режим проверки подлинности vSphere. Проверка подлинности vCenter Single Sign-On поддерживается в vCenter Server 6.0 и более поздних версий.

### Необходимые условия

- Загрузите и разверните последнюю версию vRealize Orchestrator Appliance. См. раздел [Загрузка и развертывание vRealize Orchestrator Appliance](#).
- Установите и настройте vCenter Server, предварительно запустив vCenter Single Sign-On. См. документацию по vSphere.

Если планируется создать кластер, выполните следующие действия.

- Настройте подсистему балансировки нагрузки для распределения трафика между несколькими экземплярами vRealize Orchestrator. См. [Руководство по балансировке нагрузки для VMware vRealize Orchestrator](#).

### Процедура

1. Откройте центр управления, чтобы запустить мастер настройки.
  - а) Перейдите по адресу `https://FQDN_оркестратора/vco-controlcenter`.
  - б) Войдите в качестве **пользователя root** с помощью пароля, который использовался в процессе развертывания OVA.
2. Настройте поставщика проверки подлинности.
  - а) На странице **Настройка поставщика проверки подлинности** выберите **vSphere** в раскрывающемся меню **Режим проверки подлинности**.
  - б) В текстовом поле **Адрес узла** введите полное доменное имя или IP-адрес экземпляра Platform Services Controller, содержащего vCenter Single Sign-On, и нажмите **Подключить**.

---

**Примечание** При использовании внешнего контроллера Platform Services Controller или нескольких экземпляров Platform Services Controller с подсистемой балансировки нагрузки необходимо вручную импортировать сертификаты всех этих контроллеров, имеющих доступ к домену vCenter Single Sign-On.

---



---

**Примечание** Чтобы интегрировать с настроенной средой vRealize Orchestrator другой клиент vSphere Client, необходимо настроить в vSphere использование того же контроллера Platform Services Controller, зарегистрированного в vRealize Orchestrator. Для сред vRealize Orchestrator с высокой доступностью необходимо реплицировать экземпляры PCS, используемые с сервером подсистемы балансировки нагрузки vRealize Orchestrator.

---

- в) Ознакомьтесь со сведениями о сертификате поставщика проверки подлинности и нажмите **Принять сертификат**.

- г) Введите данные учетной записи локального администратора для домена vCenter Single Sign-On. Нажмите **ЗАРЕГИСТРИРОВАТЬ**.

В качестве учетной записи по умолчанию используется **administrator@vsphere.local**, а в качестве имени арендатора по умолчанию — **vsphere.local**.

- д) В текстовом поле **Группа администраторов** введите имя группы администраторов и нажмите **ПОИСК**.

Например, введите **vsphere.local\vcoadmins**

- е) Выберите группу администраторов.

- ж) Нажмите **СОХРАНИТЬ ИЗМЕНЕНИЯ**.

Появится сообщение об успешном сохранении конфигурации.

### Результаты

Настройка сервера vRealize Orchestrator была выполнена успешно.

### Следующие шаги

- Перейдите на страницу **Лицензирование** и убедитесь, что поставщиком лицензии является **CIS**.
- Перейдите на страницу **Проверить конфигурацию** и убедитесь, что узел настроен правильно.

---

**Примечание** После настройки поставщика проверки подлинности сервер vRealize Orchestrator будет автоматически перезагружен через 2 минуты. Если проверить конфигурацию сразу после проверки подлинности, можно получить недопустимое состояние конфигурации.

---

## Включение функций vRealize Orchestrator с помощью лицензий

Доступ к определенным функциям vRealize Orchestrator зависит от лицензии, применяемой к развертыванию vRealize Orchestrator.

После проверки подлинности экземпляру vRealize Orchestrator назначается лицензия на основе поставщика проверки подлинности. Лицензии контролируют доступ к следующим функциям vRealize Orchestrator:

- Интеграция Git
- Управление ролями
- Поддержка нескольких языков (Python, Node.js и PowerShell)

Лицензию сервера vRealize Orchestrator можно изменить вручную на странице **Лицензии** в центре управления.

Проверка подлинности	Лицензия	Интеграция Git	Управление ролями	Поддержка нескольких языков
vSphere	vSphere	Нет	Нет	Нет
vSphere	vRealize Automation/vRealize Suite	Да	Да	Да
vRealize Automation	vRealize Automation/vRealize Suite	Да	Управление ролями осуществляется из экземпляра vRealize Automation, используемого для проверки подлинности vRealize Orchestrator.	Да

## Подключение базы данных vRealize Orchestrator

Серверы vRealize Orchestrator необходима база данных для хранения информации.

В развёртывание vRealize Orchestrator Appliance входит предварительно настроенная база данных PostgreSQL, которая используется сервером vRealize Orchestrator для хранения данных.

База данных PostgreSQL недоступна для пользователей.

## Управление сертификатами

Сертификат, выданный для конкретного сервера и содержащий сведения об общедоступном ключе сервера, позволяет подписать все элементы, созданные в vRealize Orchestrator, и гарантировать подлинность.

Когда клиент получает элемент с сервера (обычно это пакет), он проверяет ваше удостоверение и определяет, можно ли доверять вашей подписи.

### ■ Управление сертификатами vRealize Orchestrator

Сертификатами vRealize Orchestrator можно управлять на странице **Сертификаты** в центре управления vRealize Orchestrator или в vRealize Orchestrator Client с помощью рабочих процессов с тегом *SSL\_Trust\_Manager*.

## Управление сертификатами vRealize Orchestrator

Сертификатами vRealize Orchestrator можно управлять на странице **Сертификаты** в центре управления vRealize Orchestrator или в vRealize Orchestrator Client с помощью рабочих процессов с тегом *SSL\_Trust\_Manager*.

## Импорт сертификата в хранилище доверия Orchestrator

Центр управления vRealize Orchestrator использует безопасное соединение для обмена данными с vCenter Server, системой управления реляционными базами данных (РСУБД), LDAP, единым входом и другими серверами. Требуемый сертификат TLS можно импортировать из URL-адреса или файла в кодировке PEM. Каждый раз, когда требуется использовать TLS-подключение к экземпляру сервера, нужно импортировать соответствующий сертификат TLS на вкладке **Доверенные сертификаты** страницы **Сертификаты**.

Сертификат TLS можно загрузить в vRealize Orchestrator из URL-адреса или файла в кодировке PEM.

Параметр	Описание
<b>Импорт из URL-адреса или URL-адреса прокси-сервера</b>	URL-адрес удаленного сервера: <b>https://IP-адрес_сервера</b> или <b>IP-адрес_сервера :порт</b>
<b>Импорт из файла</b>	Укажите путь к файлу сертификата в кодировке PEM.  <b>Примечание</b> Кроме того, можно импортировать доверенный сертификат, запустив рабочий процесс <b>Импорт доверенного сертификата из файла</b> в vRealize Orchestrator Client. Файл, импортированный с помощью этого рабочего процесса, должен быть закодирован в формате DER.

Дополнительные сведения об импорте сертификатов см. в разделе [Импорт доверенного сертификата в центре управления](#).

## Сертификат подписи пакета

Пакеты, экспортируемые с сервера vRealize Orchestrator, получают цифровую подпись. Сертификаты, используемые для подписи пакетов, можно импортировать, экспортировать и создавать самостоятельно. Сертификаты подписи пакета — это форма цифровой идентификации, которая используется для обеспечения зашифрованного соединения и подписи пакетов Orchestrator.

vRealize Orchestrator Appliance включает сертификат подписи пакета, который создается автоматически на основе настроек сети устройства. При изменении параметров сети устройства необходимо вручную создать новый сертификат для подписи пакета. После создания нового сертификата подписи пакета все последующие экспортируемые пакеты будут подписываться новым сертификатом.

## Создание настраиваемого сертификата TLS для vRealize Orchestrator

С помощью vRealize Orchestrator Appliance можно создать новый сертификат TLS для среды или задать существующий настраиваемый сертификат.

В vRealize Orchestrator Appliance имеется сертификат TLS, который создается автоматически в соответствии с сетевыми настройками устройства. При изменении сетевых настроек устройства необходимо создать новый сертификат вручную. Можно создать цепочку сертификатов, что обеспечит шифрование связи и предоставление подписи для пакетов. Однако получатель никак не сможет проверить, что самозаверенный пакет в самом деле был выдан вашим сервером, а не третьей стороной, выдающей себя за вас. Чтобы доказать подлинность сервера, используйте сертификат, подписанный центром сертификации (ЦС).

vRealize Orchestrator создает уникальный сертификат сервера для вашей среды. Закрытый ключ хранится в таблице vmo\_keystore базы данных vRealize Orchestrator.

---

**Примечание** Сведения о том, как задать в vRealize Orchestrator Appliance использование существующего настраиваемого сертификата TLS, см. в разделе [Установка настраиваемого сертификата TLS для vRealize Orchestrator](#).

---

#### Необходимые условия

Убедитесь, что для vRealize Orchestrator Appliance включен доступ по протоколу SSH. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).

#### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
2. Выполните команду `vracli certificate ingress --generate auto --set stdin`.
3. Чтобы применить настраиваемый сертификат к vRealize Orchestrator Appliance, запустите сценарий развертывания.
  - а) Перейдите в каталог `/opt/scripts/`.

```
cd /opt/scripts/
```

- б) Запустите сценарий `./deploy.sh`.

---

**Важно!** Не прерывайте выполнение сценария развертывания. После завершения выполнения сценария появится следующее сообщение:

```
Вводная часть программы успешно развернута. Чтобы получить доступ, перейдите по адресу  
адрес_оркестратора
```

---

#### Следующие шаги

Чтобы проверить, применяется ли новая цепочка сертификатов, запустите команду `vracli certificate ingress --list`.

### Установка настраиваемого сертификата TLS для vRealize Orchestrator

Установите настраиваемый сертификат TLS для vRealize Orchestrator Appliance.

В vRealize Orchestrator Appliance имеется сертификат TLS, который создается автоматически в соответствии с сетевыми настройками устройства.

В vRealize Orchestrator Appliance можно настроить использование существующего настраиваемого сертификата TLS. Можно задать сертификат путем импорта соответствующего файла PEM с локального компьютера в vRealize Orchestrator Appliance. Кроме того, можно задать настраиваемый сертификат TLS путем копирования цепочки сертификатов непосредственно в vRealize Orchestrator Appliance. В обоих случаях потребуется запустить сценарий `./deploy.sh` перед использованием нового сертификата TLS в развертывании vRealize Orchestrator.

Сведения о создании нового настраиваемого сертификата TLS см. в разделе [Создание настраиваемого сертификата TLS для vRealize Orchestrator](#).

#### Необходимые условия

- Убедитесь, что для vRealize Orchestrator Appliance включен доступ по протоколу SSH. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).
- Убедитесь, что файл PEM, содержащий сертификат TLS, содержит следующие компоненты в указанном порядке:
  - а) закрытый ключ для сертификата;
  - б) основной сертификат;
  - в) если применимо, промежуточный сертификат или сертификаты центра сертификации (Certificate Authority, CA);
  - г) корневой сертификат центра сертификации.

Например, сертификат TLS может иметь следующую структуру:

```
-----BEGIN RSA PRIVATE KEY-----
<Private Key>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Primary TLS certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA certificate>
-----END CERTIFICATE-----
```

## Процедура

### 1. Задайте сертификат путем импорта файла PEM в vRealize Orchestrator Appliance.

- а) Импортируйте сертификат PEM с локального компьютера, запустив команду безопасного копирования (SCP) из оболочки SSH.

В Linux можно использовать команду SCP терминала:

```
scp ~/PEM_local_filepath/your_cert_file.PEM root@orchestrator_FQDN_or_IP:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

В Windows можно использовать команду PSCP клиента PuTTY:

```
pscp C:\PEM_local_filepath\your_cert_file.PEM root@<orchestrator_FQDN_or_IP>:/
PEM_orchestrator_filepath/your_cert_file.PEM
```

- б) Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
  - в) Выполните команду `vracli certificate ingress --set файл_сертификата.PEM`.
- ### 2. (дополнительно) Задайте сертификат путем копирования цепочки сертификатов непосредственно в устройство.

- а) Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
- б) Выполните команду `vracli certificate ingress --set stdin`.
- в) Скопируйте и вставьте цепочку сертификатов и нажмите комбинацию клавиш CTRL+D.

### 3. Чтобы применить новый сертификат TLS, запустите сценарий развертывания.

- а) Перейдите в каталог `/opt/scripts/`.

```
cd /opt/scripts/
```

- б) Запустите сценарий `./deploy.sh`.

---

**Важно!** Не прерывайте выполнение сценария развертывания. После завершения выполнения сценария появится следующее сообщение:

```
Вводная часть программы успешно развернута. Для получения доступа перейдите по адресу https://
FQDN_оркестратора
```

---

## Результаты

Настраиваемый сертификат TLS для vRealize Orchestrator Appliance успешно установлен.

## Следующие шаги

Чтобы проверить, применяется ли новая цепочка сертификатов, запустите команду `vracli certificate ingress --list`.

## Импорт доверенного сертификата в центре управления

Для безопасного обмена данными с другими серверами сервер vRealize Orchestrator должен иметь возможность подтвердить свою подлинность. Для этой цели может потребоваться импортировать сертификат TLS удаленного объекта в хранилище доверия vRealize Orchestrator. Чтобы заверить сертификат, его можно импортировать в хранилище доверия, подключившись к определенному URL-адресу либо напрямую в виде файла с кодировкой PEM.

### Процедура

1. Выполните вход в Центр управления в качестве **привилегированного пользователя root**.
2. Перейдите на страницу **Сертификаты**.
3. Выберите **Доверенные сертификаты** и нажмите **Импортировать**.
4. Чтобы импортировать сертификат из файла, выберите **Импорт из файла в кодировке PEM**.
5. Перейдите к файлу сертификата и нажмите **Импортировать**.
6. Чтобы импортировать сертификат с URL-адреса, выберите **Импортировать с URL-адреса**.
7. Введите URL-адрес, где хранится сертификат, и нажмите **Импортировать**.

### Результаты

Сертификат удаленного сервера успешно импортирован в хранилище доверия vRealize Orchestrator.

## Настройка подключаемых модулей vRealize Orchestrator

Подключаемые модули vRealize Orchestrator по умолчанию настраиваются с помощью специальных рабочих процессов, выполняемых в vRealize Orchestrator Client.

vRealize Orchestrator Appliance предоставляет доступ к готовой библиотеке подключаемых модулей по умолчанию. Для настройки этих подключаемых модулей по умолчанию можно запустить из vRealize Orchestrator Client предназначенные для них рабочие процессы.

Например, при вводе тегов *AMQP* и *Configuration* в текстовом поле поиска библиотеки рабочих процессов будет выполнен поиск рабочих процессов, которые используются для управления брокерами и подписками AMQP.

## Управление подключаемыми модулями vRealize Orchestrator

На странице **Управление подключаемыми модулями** центра управления vRealize Orchestrator можно просмотреть список всех подключаемых модулей, установленных в vRealize Orchestrator, и выполнить основные операции управления.

### Установка или обновление подключаемого модуля

Подключаемые модули vRealize Orchestrator позволяют серверу vRealize Orchestrator выполнять интеграцию с другими программными продуктами. vRealize Orchestrator Appliance включает в себя набор предварительно установленных подключаемых модулей. Возможности платформы vRealize Orchestrator можно дополнительно расширить, установив настраиваемые подключаемые модули.



Подключаемые модули можно установить или модернизировать на странице **Управление подключаемыми модулями** в vRealize Orchestrator. Поддерживаемые форматы файлов: VMOAPP и DAR. Файл VMOAPP может содержать в себе набор из нескольких файлов DAR, и его можно установить как приложение. Файл DAR содержит все ресурсы, связанные с одним подключаемым модулем.

---

**Примечание** Предпочтительным форматом файла для подключаемых модулей vRealize Orchestrator является VMOAPP.

---

Дополнительные сведения об установке и модернизации подключаемых модулей vRealize Orchestrator см. в разделе [Установка и обновление подключаемого модуля vRealize Orchestrator](#).

## Изменение уровня ведения журнала подключаемых модулей

Вместо изменения уровня ведения журнала для vRealize Orchestrator можно изменить это значение только для отдельных подключаемых модулей.

## Отключение подключаемого модуля

Чтобы отключить подключаемый модуль, снимите флажок **Включить подключаемый модуль** рядом с его именем.

При этом файл подключаемого модуля не удаляется. Дополнительные сведения об удалении подключаемых модулей из vRealize Orchestrator см. в разделе [Удаление подключаемого модуля](#).

## Установка и обновление подключаемого модуля vRealize Orchestrator

Подключаемые модули сторонних разработчиков можно устанавливать и обновлять в центре управления vRealize Orchestrator.

### Необходимые условия

Загрузите файл *.dar* или *.vmoapp* подключаемого модуля.

---

**Примечание** Предпочтительным форматом файла для подключаемых модулей vRealize Orchestrator является VMOAPP.

---

### Процедура

1. Войдите в центр управления от имени пользователя **root**.
2. Перейдите на страницу **Управление подключаемыми модулями**.
3. Нажмите кнопку **Обзор** и выберите файл *.dar* или *.vmoapp* подключаемого модуля, который необходимо установить или обновить.
4. Щелкните **Отправить**.
5. При необходимости ознакомьтесь со сведениями о подключаемом модуле, примите лицензионное соглашение с конечным пользователем и нажмите кнопку **Установить**.

Подключаемый модуль будет установлен или обновлен, а служба сервера vRealize Orchestrator будет перезапущена.

## Следующие шаги

Убедитесь, что на странице **Управление подключаемыми модулями** указаны правильные сведения о подключаемом модуле.

## Удаление подключаемого модуля


Подключаемые модули сторонних разработчиков можно удалить из vRealize Orchestrator Appliance с помощью центра управления.

---

**Примечание** Начиная с vRealize Orchestrator 8.0, больше не требуется вручную удалять пакеты подключаемых модулей из vRealize Orchestrator Client.

---

### Процедура

1. Войдите в центр управления от имени пользователя **root**.
2. Выберите **Управление подключаемыми модулями**.
3. Найдите подключаемый модуль, который необходимо удалить, и щелкните значок удаления (  ).
4. Подтвердите удаление подключаемого модуля и нажмите кнопку **Удалить**.

### Результаты

Подключаемый модуль удален из vRealize Orchestrator Appliance.

## Доступность и масштабируемость vRealize Orchestrator

Чтобы повысить доступность служб vRealize Orchestrator, запустите несколько экземпляров серверов vRealize Orchestrator в кластере с общей базой данных. vRealize Orchestrator работает как единый экземпляр до тех пор, пока он не будет настроен для работы в кластере.

### Кластер vRealize Orchestrator

Несколько экземпляров сервера vRealize Orchestrator с одинаковыми конфигурациями сервера и подключаемых модулей работают совместно в кластере и используют одну базу данных.

Все экземпляры сервера vRealize Orchestrator обмениваются друг с другом данными путем обмена тактовыми импульсами. Каждый тактовый импульс — это временная метка, которую узел записывает в общую базу данных кластера через определенные интервалы времени. Проблемы с сетью, неотвечающий сервер базы данных или перегрузка может привести к зависанию узла кластера vRealize Orchestrator. Если активный экземпляр сервера vRealize Orchestrator не может отправить тактовый импульс в течение времени ожидания аварийного переключения, то он считается неотвечающим. Время ожидания аварийного переключения равно значению интервала тактового импульса, умноженному на количество тактов аварийного переключения. Этот параметр служит определением ненадежного узла и может быть настроен в соответствии с доступными ресурсами и производственной нагрузкой.

Когда узел vRealize Orchestrator теряет подключение к базе данных, он переходит в режим ожидания и остается в нем, пока подключение не будет восстановлено. Другие узлы в кластере перехватывают контроль над активной работой, возобновляя все прерванные рабочие процессы из последних незавершенных элементов, таких как задачи, выполняемые с помощью сценариев, или вызовы рабочих процессов.

Состояние кластера vRealize Orchestrator можно отслеживать на странице **Управление кластером Orchestrator** в центре управления vRealize Orchestrator. На этой странице также можно настроить период тактового импульса кластера, количество тактов аварийного переключения и количество активных узлов vRealize Orchestrator.

## Настройка кластера vRealize Orchestrator

Новое развертывание vRealize Orchestrator можно настроить на работу в режиме высокой доступности. Для этого необходимо развернуть три узла и объединить их в кластер.

Кластер vRealize Orchestrator состоит из трех экземпляров vRealize Orchestrator с общей базой данных PostgreSQL. База данных настроенного кластера vRealize Orchestrator может работать только в асинхронном режиме.

Чтобы создать кластер vRealize Orchestrator, необходимо выбрать один экземпляр vRealize Orchestrator в качестве основного узла кластера. После настройки основного узла к нему следует присоединить дополнительные узлы.

Полученный кластер vRealize Orchestrator по умолчанию настроен на автоматическое аварийное переключение.

---

**Примечание** Сбой автоматического аварийного переключения может привести к потере сведений, содержащихся в базе данных.

---

### Необходимые условия

- Загрузите и разверните три автономных экземпляра vRealize Orchestrator. См. раздел [Загрузка и развертывание vRealize Orchestrator Appliance](#).

---

**Примечание** Для создания кластерной среды vRealize Orchestrator рекомендуется использовать три узла.

---

- Убедитесь, что для всех узлов vRealize Orchestrator включен доступ по протоколу SSH. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).
- Настройте сервер подсистемы балансировки нагрузки. См. [Руководство по балансировке нагрузки для VMware vRealize Orchestrator](#).

## Процедура

### 1. Настройте основной узел.

- а) Войдите в среду vRealize Orchestrator Appliance основного узла через SSH в качестве пользователя **root**.
- б) Чтобы настроить сервер подсистемы балансировки нагрузки в кластере, запустите команду `vracli load-balancer set FQDN_подсистемы_балансировки_нагрузки`.
- в) Войдите в центр управления основного узла и выберите **Настройки узла**.
- г) Щелкните **Изменить** и укажите адрес узла подключенного сервера подсистемы балансировки нагрузки.
- д) Настройте поставщика проверки подлинности. См. раздел [Настройка автономного сервера vRealize Orchestrator](#).

### 2. Присоедините дополнительные узлы к основному.

- а) Войдите в среду vRealize Orchestrator Appliance дополнительного узла через SSH в качестве пользователя **root**.
- б) Чтобы присоединить дополнительный узел к основному, запустите команду `vracli cluster join имя_узла_или_IP-адрес_основного_узла`.
- в) Введите пароль пользователя root основного узла.
- г) Повторите процедуру для другого дополнительного узла.

### 3. (дополнительно) Если основной узел использует настраиваемый сертификат, необходимо либо задать сертификат в устройстве, либо создать новый сертификат. См. раздел [Создание настраиваемого сертификата TLS для vRealize Orchestrator](#).

---

**Примечание** Файл, содержащий цепочку сертификатов, должен иметь кодировку PEM.

---

### 4. Завершите развертывание кластера.

- а) Войдите в среду vRealize Orchestrator Appliance основного узла по протоколу SSH в качестве пользователя **root**.
- б) Убедитесь, что все узлы находятся в состоянии готовности, выполнив команду `kubectl -n prelude get nodes`.
- в) Запустите сценарий `/opt/scripts/deploy.sh` и дождитесь завершения развертывания.

## Результаты

Кластер vRealize Orchestrator создан. После создания кластера доступ к среде vRealize Orchestrator можно получить только с использованием FQDN-адреса сервера подсистемы балансировки нагрузки.

---

**Примечание** Так как доступ к центру управления кластера можно получить только с помощью пароля пользователя `root` подсистемы балансировки нагрузки, изменить конфигурацию кластерного узла, имеющего другой пароль пользователя `root`, невозможно. Чтобы изменить конфигурацию этого узла, удалите его из подсистемы балансировки нагрузки, измените конфигурацию в центре управления и снова добавьте узел в подсистему.

---

## Следующие шаги

Чтобы отслеживать состояние кластера vRealize Orchestrator, войдите в центр управления и откройте страницу **Управление кластером Orchestrator**. См. раздел [Мониторинг кластера vRealize Orchestrator](#).

## Удаление узла из кластера vRealize Orchestrator

Можно удалить узел из кластера vRealize Orchestrator, чтобы уменьшить его емкость.

Узел, удаленный из кластера vRealize Orchestrator, перестает работать. Если потребуется снова использовать узел, необходимо удалить vRealize Orchestrator Appliance данного узла из vCenter Server и повторно развернуть его. См. раздел [Загрузка и развертывание vRealize Orchestrator Appliance](#).

## Необходимые условия

Создайте кластер vRealize Orchestrator. См. раздел [Настройка кластера vRealize Orchestrator](#).

## Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance удаляемого узла в качестве пользователя **root**.
2. Чтобы удалить узел из vRealize Orchestrator, запустите команду `vracli cluster leave`.
3. Войдите в командную строку vRealize Orchestrator Appliance одного из оставшихся узлов в качестве пользователя **root**.
4. Запустите команду `kubectl -n prelude get nodes` и убедитесь, что удаленный узел больше не является частью кластера.

## Горизонтальное масштабирование автономного развертывания vRealize Orchestrator

Путем горизонтального масштабирования можно повысить доступность и масштабируемость настроенного развертывания vRealize Orchestrator.

## Необходимые условия

- Загрузите, разверните и настройте экземпляр vRealize Orchestrator. См. разделы [Загрузка и развертывание vRealize Orchestrator Appliance](#) и [Настройка автономного сервера vRealize Orchestrator](#).
- Загрузите и разверните два дополнительных экземпляра vRealize Orchestrator. См. раздел [Загрузка и развертывание vRealize Orchestrator Appliance](#).
- Настройте сервер подсистемы балансировки нагрузки. См. [Руководство по балансировке нагрузки для VMware vRealize Orchestrator 8.x](#).

## Процедура

### 1. Настройте основной узел.

- а) Войдите в центр управления настроенного развертывания vRealize Orchestrator в качестве пользователя **root**.
- б) Выберите **Настройка поставщика проверки подлинности** и отмените регистрацию своего поставщика проверки подлинности.
- в) Выберите **Настройки узла** и введите имя узла сервера подсистемы балансировки нагрузки.
- г) Выберите **Настройка поставщика проверки подлинности** и снова зарегистрируйте поставщика проверки подлинности.
- д) Войдите в командную строку vRealize Orchestrator Appliance настроенного экземпляра в качестве пользователя **root**.
- е) Чтобы остановить все службы экземпляра vRealize Orchestrator, выполните команду `/opt/scripts/deploy.sh --onlyClean`.
- ж) Чтобы настроить подсистему балансировки нагрузки, выполните команду `vracli load-balancer set FQDN_балансировщика`.
- з) (дополнительно) Если в экземпляре vRealize Orchestrator используется настраиваемый сертификат, выполните команду `vracli certificate ingress --set файл_сертификата.pem`.

---

**Примечание** Файл, содержащий цепочку сертификатов, должен иметь кодировку PEM.

---

### 2. Присоедините дополнительные узлы к настроенному экземпляру.

- а) Войдите в командную строку vRealize Orchestrator Appliance дополнительного узла в качестве пользователя **root**.
- б) Чтобы присоединить дополнительный узел к настроенному экземпляру, выполните команду `vracli cluster join IP_или_имя_основного_узла`.
- в) Повторите эти действия для другого дополнительного узла.

### 3. Завершите процесс горизонтального масштабирования.

- а) Войдите в командную строку vRealize Orchestrator Appliance настроенного экземпляра в качестве пользователя **root**.
- б) Запустите сценарий `/opt/scripts/deploy.sh` и дождитесь завершения его выполнения.

#### Результаты

Горизонтальное масштабирование развертывания vRealize Orchestrator выполнено.

## Мониторинг кластера vRealize Orchestrator

Можно выполнить мониторинг существующего кластера vRealize Orchestrator в центре управления vRealize Orchestrator.

Можно отслеживать состояния синхронизации конфигурации экземпляров vRealize Orchestrator, присоединяемых к кластеру, на странице **Управление кластером Orchestrator** в центре управления.

Состояние синхронизации конфигурации	Описание
ЗАПУЩЕНО	Служба vRealize Orchestrator доступна и может принимать запросы.
ОЖИДАНИЕ	<p>Служба vRealize Orchestrator не может обрабатывать запросы по следующим причинам.</p> <ul style="list-style-type: none"> <li>■ Узел входит в кластер высокой доступности (High Availability, HA) и остается в режиме ожидания до тех пор, пока на основном узле не произойдет сбой.</li> <li>■ Служба не может проверить предварительные требования к конфигурации, например допустимое подключение к базе данных, поставщику проверки подлинности или лицензии на экземпляр vRealize Orchestrator.</li> </ul>
Не удалось получить состояние работоспособности службы	Невозможно связаться со службой сервера vRealize Orchestrator, так как она остановлена, либо возникла проблема в сети.
Ожидание перезапуска	Центр управления обнаружил изменение конфигурации, и сервер vRealize Orchestrator автоматически перезапускается.

## Настройка программы улучшения качества программного обеспечения

Если вы решили участвовать в программе улучшения качества программного обеспечения (CEIP), то компании VMware будет предоставляться анонимная информация, которая поможет улучшить качество, надежность и возможности продуктов и служб VMware.

## Категории информации, предоставляемой компании VMware

В рамках Программы улучшения качества программного обеспечения (Customer Experience Improvement Program, CEIP) компания VMware собирает информацию, благодаря которой может улучшать свои продукты и услуги, а также устранять проблемы.

Сведения о данных, собираемых в рамках CEIP, и целях их использования компанией VMware можно найти на странице Trust & Assurance Center по адресу <http://www.vmware.com/trustvmware/ceip.html>. Сведения о том, как присоединиться к программе CEIP для этого продукта или выйти из нее, см. в разделе [Присоединение к программе улучшения качества программного обеспечения и выход из нее](#).

## Присоединение к программе улучшения качества программного обеспечения и выход из нее

Чтобы присоединиться к программе улучшения качества программного обеспечения, используйте командную строку vRealize Orchestrator Appliance.

### Процедура

1. Выполните вход в vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Чтобы присоединиться к программе улучшения качества программного обеспечения, выполните команду `vracli ceip on`.
3. Просмотрите сведения о программе улучшения качества программного обеспечения и выполните команду `vracli ceip on --acknowledge-ceip`.
4. Перезапустите службы vRealize Orchestrator.
  - а) Чтобы перезапустить службу сервера, выполните команду `kubectl -n prelude exec -it модуль_vro -c vco-server-app /bin/bash`.
  - б) Чтобы остановить службу, выполните команду `kill 1`.
  - в) Чтобы перезапустить службу центра управления, запустите команду `kubectl -n prelude exec -it модуль_vro -c vco-controlcenter-app /bin/bash`.
  - г) Чтобы остановить службу, выполните команду `kill 1`.
5. Чтобы выйти из программы улучшения качества программного обеспечения, выполните команду `vracli ceip off`.
6. Повторите действия для перезапуска служб.



# Использование служб API-интерфейса vRealize Orchestrator

# 6

Кроме настройки vRealize Orchestrator с помощью центра управления параметры конфигурации сервера vRealize Orchestrator можно изменять с помощью REST API vRealize Orchestrator, REST API центра управления и утилиты командной строки в устройстве.

Подключаемый модуль конфигурации включен в пакет vRealize Orchestrator по умолчанию. Доступ к рабочим процессам подключаемого модуля конфигурации можно получить из библиотеки рабочих процессов vRealize Orchestrator или REST API vRealize Orchestrator. С помощью этих рабочих процессов можно изменить доверенный сертификат и параметры хранилища ключей сервера vRealize Orchestrator. Сведения о доступных вызовах служб REST API vRealize Orchestrator см. в документации по *API-интерфейсу сервера vRealize Orchestrator* по адресу [https://FQDN\\_оркестратора/vco/api/docs](https://FQDN_оркестратора/vco/api/docs).

## ■ Управление сертификатами TLS и хранилищами ключей с помощью REST API

Помимо управления сертификатами TLS в центре управления доверенными сертификатами и хранилищами ключей можно также управлять путем запуска рабочих процессов в подключаемом модуле конфигурации или с помощью REST API.

## Управление сертификатами TLS и хранилищами ключей с помощью REST API

Помимо управления сертификатами TLS в центре управления доверенными сертификатами и хранилищами ключей можно также управлять путем запуска рабочих процессов в подключаемом модуле конфигурации или с помощью REST API.

Подключаемый модуль конфигурации содержит рабочие процессы для импорта и удаления сертификатов TLS и хранилищ ключей. Доступ к этим рабочим процессам можно получить, перейдя в разделы **Библиотека > Рабочие процессы > Менеджер доверия SSL** и **Библиотека > Рабочие процессы > Хранилища ключей** в vRealize Orchestrator Client. Эти рабочие процессы также можно запустить с помощью REST API vRealize Orchestrator.

REST API центра управления предоставляет доступ к ресурсам для настройки сервера vRealize Orchestrator. REST API центра управления можно использовать с системами сторонних производителей для автоматизации настройки vRealize Orchestrator. Корневая конечная точка REST API центра управления: [https://FQDN\\_оркестратора/vco/api](https://FQDN_оркестратора/vco/api). Сведения обо всех доступных вызовах служб, которые можно сделать в REST API центра управления, см. в документации по *API-интерфейсу центра управления vRealize Orchestrator* по адресу [https://FQDN\\_оркестратора/vco-controlcenter/docs](https://FQDN_оркестратора/vco-controlcenter/docs).

## Удаление сертификата TLS с помощью REST API

Чтобы удалить сертификат TLS, запустите рабочий процесс удаления доверенного сертификата в подключаемом модуле конфигурации или воспользуйтесь REST API.

### Процедура

1. Отправьте запрос GET на URL-адрес службы рабочих процессов, относящейся к рабочему процессу удаления доверенного сертификата.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows?conditions=name>Delete trusted certificate
```

2. Чтобы извлечь определение рабочего процесса удаления доверенного сертификата, отправьте запрос GET на URL-адрес определения.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd
```

3. Отправьте запрос POST на URL-адрес, содержащий объекты выполнения рабочего процесса удаления доверенного сертификата.

```
POST https://{узел_оркестратора}:{порт}/vco/api/workflows/8a70a326-ffd7-4fef-97e0-2002ac49f5bd/
executions/
```

4. Укажите имя удаляемого сертификата в качестве входного параметра рабочего процесса удаления доверенного сертификата в элементе контекста выполнения в тексте запроса.

## Импорт сертификатов TLS с помощью REST API

Чтобы импортировать сертификаты TLS, запустите рабочий процесс в подключаемом модуле конфигурации или воспользуйтесь REST API.

Доверенный сертификат можно импортировать из файла или с URL-адреса. См. раздел [Импорт доверенного сертификата в центре управления](#)

### Процедура

1. Отправьте запрос GET на URL-адрес службы рабочих процессов.

Параметр	Описание
Импорт доверенного сертификата из файла	Доверенный сертификат импортируется из файла.
Импорт доверенного сертификата с URL-адреса	Доверенный сертификат импортируется с URL-адреса.

Параметр	Описание
<b>Импорт доверенного сертификата с URL-адреса с помощью прокси-сервера</b>	Доверенный сертификат импортируется с URL-адреса с помощью прокси-сервера.
<b>Импорт сертификата с URL-адреса с псевдонимом сертификата</b>	Доверенный сертификат с псевдонимом сертификата импортируется с URL-адреса.

Чтобы импортировать доверенный сертификат из файла, выполните следующий запрос GET:

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows?conditions=name=Import
trusted certificate from a file
```

2. Чтобы извлечь определение рабочего процесса, отправьте запрос GET на URL-адрес определения.

Чтобы извлечь определение рабочего процесса импорта доверенного сертификата из файла, выполните следующий запрос GET:

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5
```

3. Отправьте запрос POST на URL-адрес, содержащий объекты выполнения рабочего процесса.

При использовании рабочего процесса импорта доверенного сертификата из файла выполните следующий запрос POST:

```
POST https://{узел_оркестратора}:{порт}/vco/api/workflows/93a7bb21-0255-4750-9293-2437abe9d2e5/
executions
```

4. Укажите значения входных параметров рабочего процесса в элементе контекста выполнения в теле запроса.

Параметр	Описание
<b>cer</b>	Файл CER, из которого импортируется сертификат TLS. Этот параметр применяется к рабочему процессу импорта доверенного сертификата из файла.
<b>url</b>	URL-адрес, с которого импортируется сертификат TLS. Службы, отличные от HTTPS, поддерживают формат <i>IP_адрес_или_DNS_имя:порт</i> . Этот параметр применяется к рабочему процессу импорта доверенного сертификата с URL-адреса.

## Создание хранилища ключей с помощью REST API

Чтобы создать хранилище ключей, запустите рабочий процесс создания хранилища ключей в подключаемом модуле конфигурации или воспользуйтесь REST API.

### Процедура

1. Отправьте запрос GET на URL-адрес службы рабочих процессов, относящейся к рабочему процессу создания хранилища ключей.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows?conditions=name=Create a keystore
```

2. Чтобы извлечь определение рабочего процесса создания хранилища ключей, отправьте запрос GET на URL-адрес определения.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3. Отправьте запрос POST на URL-адрес, содержащий объекты выполнения рабочего процесса создания хранилища ключей.

```
POST https://{узел_оркестратора}:{порт}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4. Укажите имя хранилища ключей, которое требуется создать, в качестве входного параметра рабочего процесса создания хранилища ключей в элементе контекста выполнения в тексте запроса.

## Удаление хранилища ключей с помощью REST API

Чтобы удалить хранилище ключей, запустите рабочий процесс удаления хранилища ключей в подключаемом модуле конфигурации или воспользуйтесь REST API.

### Процедура

1. Отправьте запрос GET на URL-адрес службы рабочих процессов, относящейся к рабочему процессу удаления хранилища ключей.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows?conditions=name=Delete a keystore
```

2. Чтобы извлечь определение рабочего процесса удаления хранилища ключей, отправьте запрос GET на URL-адрес определения.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
```

3. Отправьте запрос POST на URL-адрес, содержащий объекты выполнения рабочего процесса удаления хранилища ключей.

```
POST https://{узел_оркестратора}:{порт}/vco/api/workflows/7a3389eb-1fab-4d77-860b-81b66bb45b86/
executions/
```

4. Укажите хранилище ключей, которое требуется удалить, в качестве входного параметра рабочего процесса удаления хранилища ключей в элементе контекста выполнения в тексте запроса.

## Добавление ключа с помощью REST API

Чтобы добавить ключ, запустите рабочий процесс добавления ключа в подключаемом модуле конфигурации или воспользуйтесь REST API.

## Процедура

1. Отправьте запрос GET на URL-адрес службы рабочих процессов, относящейся к рабочему процессу добавления ключа.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows?conditions=name=Add key
```

2. Чтобы извлечь определение рабочего процесса добавления ключа, отправьте запрос GET на URL-адрес определения.

```
GET https://{узел_оркестратора}:{порт}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
```

3. Отправьте запрос POST на URL-адрес, содержащий объекты выполнения рабочего процесса добавления ключа.

```
POST https://{узел_оркестратора}:{порт}/vco/api/workflows/6c301bff-e8fe-4ae0-ad08-5318178594b3/
executions/
```

4. В элементе контекста выполнения в тексте запроса задайте следующие входные параметры рабочего процесса добавления ключа: хранилище ключей, псевдоним ключа, ключ в кодировке PEM, цепочка сертификатов и пароль ключа.

# Дополнительные параметры конфигурации

# 7

С помощью центра управления можно изменить поведение vRealize Orchestrator по умолчанию.

В эту главу входят следующие разделы:

- [Повторная настройка проверки подлинности](#)
- [Настройка свойств выполняемого рабочего процесса](#)
- [Файлы журналов vRealize Orchestrator](#)
- [Включение расширений Opentracing и Wavefront](#)
- [Включение синхронизации времени в vRealize Orchestrator](#)
- [Отключение синхронизации времени в vRealize Orchestrator](#)

## Повторная настройка проверки подлинности

После настройки метода проверки подлинности во время первоначальной настройки центра управления вы в любое время можете изменить поставщика проверки подлинности или настроенные параметры.

### Изменение поставщика проверки подлинности

Чтобы изменить режим проверки подлинности или настройки подключения поставщика проверки подлинности, необходимо сначала отменить регистрацию существующего поставщика.

#### Процедура

1. Выполните вход в Центр управления в качестве **привилегированного пользователя root**.
2. На странице **Настройка поставщика проверки подлинности** нажмите кнопку **ОТМЕНИТЬ РЕГИСТРАЦИЮ** рядом с текстовым полем адреса узла, чтобы отменить регистрацию действующего поставщика.

#### Результаты

Регистрация поставщика проверки подлинности отменена.

## Следующие шаги

Перенастройте проверку подлинности в центре управления. См. раздел [Настройка автономного сервера vRealize Orchestrator](#).

## Изменение параметров проверки подлинности

Если в качестве поставщика проверки подлинности в центре управления используется vSphere, можно изменить арендатора по умолчанию для группы администраторов vRealize Orchestrator.

### Необходимые условия

Настройте vSphere в качестве поставщика проверки подлинности для развертывания vRealize Orchestrator. См. раздел [Настройка автономного сервера vRealize Orchestrator с проверкой подлинности vSphere](#).

---

**Примечание** Проверка подлинности vRealize Automation не включает в себя эти параметры.

---

### Процедура

1. Войдите в центр управления от имени пользователя **root**.
2. Выберите **Настройка поставщика проверки подлинности**.
3. Нажмите кнопку **ИЗМЕНИТЬ** рядом с текстовым полем **Арендатор по умолчанию**.
4. Измените имя арендатора.
5. Нажмите кнопку **ИЗМЕНИТЬ** рядом с текстовым полем **Группа администраторов**.

---

**Примечание** Если не перенастроить группу администраторов, она останется пустой, и доступ к центру управления будет невозможен.

---

6. Введите имя группы администраторов и нажмите **ПОИСК**.
7. Выберите группу администраторов.
8. Измените группу администраторов.
9. Чтобы завершить изменение параметров проверки подлинности, нажмите **СОХРАНИТЬ ИЗМЕНЕНИЯ**.

## Настройка свойств выполняемого рабочего процесса

По умолчанию для каждого узла можно запустить до 300 рабочих процессов, а если достигнуто максимальное количество активных рабочих процессов, до 10 000 рабочих процессов можно поставить в очередь.

Если узлу vRealize Orchestrator требуется выполнить более 300 параллельных рабочих процессов, то остальные рабочие процессы будут поставлены в очередь. Когда выполнение активного рабочего процесса завершается, запускается следующий рабочий процесс в очереди. Если количество рабочих процессов, находящихся в очереди, достигает максимального, рабочие процессы не добавляются, пока не начнется выполнение одного из рабочих процессов в очереди.

На странице **Дополнительные параметры** в центре управления можно настроить свойства выполняемого рабочего процесса.

Параметр	Описание
<b>Включение безопасного режима</b>	Если включен безопасный режим, все выполняемые рабочие процессы отменяются и не возобновляются при следующем запуске узла Orchestrator.
<b>Количество параллельных выполняемых рабочих процессов</b>	Максимальное количество параллельных рабочих процессов узла Orchestrator, которые могут выполняться одновременно.
<b>Максимальное количество выполняемых рабочих процессов в очереди</b>	Количество запросов на запуск рабочего процесса, принятых узлом Orchestrator до того, как он стал недоступным.
<b>Максимальное количество сохраненных запусков для каждого рабочего процесса</b>	Максимальное количество завершенных запусков рабочих процессов, регистрируемых в журнале для каждого рабочего процесса в кластере. Если это число превышено, самые старые запуски рабочих процессов удаляются.
<b>Срок действия событий журнала</b>	Количество дней, в течение которых события журнала для данного кластера хранятся в базе данных. После этого события удаляются.

## Файлы журналов vRealize Orchestrator

При отправке запроса на техническую поддержку служба поддержки VMware запросит у вас диагностические сведения. Эта информация включает в себя журналы и файлы конфигурации конкретного продукта с узла, на котором этот продукт работает.

Журналы vRealize Orchestrator Appliance хранятся в каталоге `/data/vco/usr/lib/vco/app-server/logs/`. Чтобы экспортировать журналы развертывания vRealize Orchestrator Appliance, войдите в командную строку устройства и запустите команду `vraccli log-bundle`. Созданный пакет журналов сохранится в корневой папке vRealize Orchestrator Appliance.

## Сохраняемость журналов

В сценарии vRealize Orchestrator любого типа, будь то рабочий процесс, политика или действие, можно записывать данные в журнал. Эти данные имеют тип и уровень. По типу данные разделяются на постоянные и непостоянные. Уровень может принимать значения `DEBUG`, `INFO`, `WARN`, `ERROR`, `TRACE` и `FATAL`.



Таблица 7-1. Создание постоянных и непостоянных журналов

Уровень журнала	Постоянный тип	Непостоянный тип
DEBUG	Server.debug("краткий текст", "полный текст");	System.debug("текст")
INFO	Server.log("краткий текст", "полный текст");	System.log("текст");
WARN	Server.warn("краткий текст", "полный текст");	System.warn("текст");
ERROR	Server.error("краткий текст", "полный текст");	System.error("текст");

## Постоянные журналы

В постоянных журналах (журналах сервера) отслеживается ведение журналов прошлых запусков рабочих процессов; эти журналы хранятся в базе данных vRealize Orchestrator.

## Непостоянные журналы

Если для создания сценариев используется непостоянный журнал (системный журнал), сервер vRealize Orchestrator уведомляет все выполняемые приложения vRealize Orchestrator о данном журнале, но эта информация не сохраняется в базе данных. При перезапуске приложения сведения в журнале утрачиваются. Непостоянные журналы используются для отладки и получения информации в режиме реального времени. Для просмотра системных журналов необходимо выбрать завершенный рабочий процесс в vRealize Orchestrator Client и перейти на вкладку **Журналы**.

## Настройка журналов vRealize Orchestrator

На странице **Настройка журналов** в центре управления можно задать требуемый уровень ведения журнала сервера и журнала сценариев. Если журналы создаются несколько раз в день, становится трудно определить причины проблем.

По умолчанию для журнала сервера и журнала сценариев задан уровень ИНФОРМАЦИЯ. Изменение уровня ведения журнала затрагивает все новые сообщения, которые сервер вносит в журналы, и количество активных подключений к базе данных. Степень подробности ведения журнала уменьшается в порядке убывания.

**Осторожно!** Уровни ОТЛАДКА и ВСЕ используются только на этапе отладки. Не используйте эти параметры в производственной среде, так как это может негативно сказаться на производительности.

## Создание журналов vRealize Orchestrator

Можно экспортировать журналы развертывания, войдя в командную строку vRealize Orchestrator Appliance в качестве пользователя **root** и запустив команду `vraccli log-bundle`. Созданный набор журналов сохраняется в корневой папке устройства.

---

**Примечание** Если в кластере используется несколько экземпляров vRealize Orchestrator, набор журналов включает в себя журналы всех экземпляров vRealize Orchestrator в кластере.

---

## Настройка интеграции ведения журнала с vRealize Log Insight

vRealize Orchestrator можно настроить так, чтобы данные журнала отправлялись на сервер vRealize Log Insight.

Интеграцию ведения журнала с сервером vRealize Log Insight можно настроить с помощью командной строки vRealize Orchestrator Appliance.

---

**Примечание** Дополнительные сведения о настройке интеграции ведения журнала с удаленным сервером системного журнала см. в разделе [Создание или перезапись интеграции системного журнала в vRealize Orchestrator](#).

---

### Необходимые условия

- Настройте сервер vRealize Log Insight. См. *документацию по vRealize Log Insight*.
- Убедитесь, что используется vRealize Log Insight 4.7.1 или более поздней версии.

### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Чтобы настроить интеграцию ведения журнала с vRealize Log Insight, запустите команду `vraccli vrli set vRLI_FQDN`.

---

**Примечание** Если в экземпляре vRealize Orchestrator используется самозаверяющий сертификат, можно отключить проверку подлинности SSL, указав дополнительный аргумент `-k` или `--insecure`.

---

### Следующие шаги

Для получения дополнительных сведений о параметрах конфигурации vRealize Log Insight запустите команду `vraccli vrli -h`.

## Создание или перезапись интеграции системного журнала в vRealize Orchestrator

vRealize Orchestrator можно настроить так, чтобы данные журнала отправлялись на один или несколько удаленных серверов системного журнала.

Для создания интеграции системного журнала или перезаписи существующих интеграций используется команда `vraccli remote-syslog set`.

Интеграция удаленного системного журнала в vRealize Orchestrator поддерживает три типа подключения:

- по протоколу UDP;

- по протоколу TCP без TLS;

---

**Примечание** Чтобы создать интеграцию системного журнала без использования TLS, добавьте флаг `--disable-ssl` в команду `vracli remote-syslog set`.

---

- по протоколу TCP с TLS.

Дополнительные сведения о настройке интеграции ведения журнала с помощью vRealize Log Insight см. в разделе [Настройка интеграции ведения журнала с vRealize Log Insight](#).

#### Необходимые условия

Настройте один или несколько удаленных серверов системного журнала.

#### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Чтобы создать интеграцию с сервером системного журнала, запустите команду `vracli remote-syslog set`.

```
vracli remote-syslog set -id name_of_integration protocol_type://syslog_URL_or_FQDN:syslog_port
```

---

**Примечание** Если в команде `vracli remote-syslog set` не указать порт, то будет использовано значение порта по умолчанию — 514.

---



---

**Примечание** В конфигурацию системного журнала можно добавить сертификат. Чтобы добавить файл сертификата, используйте флаг `--ca-file`. Чтобы добавить сертификат в виде обычного текста, используйте флаг `--ca-cert`.

---

3. (дополнительно) Чтобы перезаписать существующую интеграцию системного журнала, запустите `vracli remote-syslog set` и в качестве значения флага `-id` укажите имя интеграции, которую нужно перезаписать.

---

**Примечание** По умолчанию при попытке перезаписи интеграции системного журнала vRealize Orchestrator Appliance запрашивает подтверждение. Чтобы пропустить запрос подтверждения, добавьте флаг `-f` или `--force` в команду `vracli remote-syslog set`.

---

#### Следующие шаги

Для просмотра текущих интеграций системного журнала в устройстве запустите команду `vracli remote-syslog`.

### Удаление интеграции системного журнала из vRealize Orchestrator

Можно удалить интеграции системного журнала из vRealize Orchestrator Appliance, запустив команду `vracli remote-syslog unset`.

## Необходимые условия

Создайте одну или несколько интеграций системного журнала в vRealize Orchestrator Appliance. См. раздел [Создание или перезапись интеграции системного журнала в vRealize Orchestrator](#).

## Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Удалите интеграции системного журнала из vRealize Orchestrator Appliance.
  - а) Чтобы удалить отдельную интеграцию системного журнала, запустите команду `vraccli remote-syslog unset -id имя_интеграции`.
  - б) Чтобы удалить все интеграции системного журнала в vRealize Orchestrator Appliance, запустите команду `vraccli remote-syslog unset` без флага `-id`.

---

**Примечание** По умолчанию перед удалением всех интеграций системного журнала vRealize Orchestrator Appliance запрашивает подтверждение. Чтобы пропустить запрос подтверждения, добавьте флаг `-f` или `--force` в команду `vraccli remote-syslog unset`.

---

## Включение ведения журнала отладки Kerberos

Для устранения неполадок в подключаемом модуле vRealize Orchestrator можно изменить файл конфигурации Kerberos, используемый этим модулем.

Файл конфигурации Kerberos находится в каталоге `/data/vco/usr/lib/vco/app-server/conf/` vRealize Orchestrator Appliance.

## Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Выполните команду `kubectl -n prelude edit deployment vco-app`.
3. В файле развертывания выберите и измените строку `-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf`.

```
-Djava.security.krb5.conf=/usr/lib/vco/app-server/conf/krb5.conf -Dsun.security.krb5.debug=true'
```

4. Сохраните изменения и выйдите из редактора файлов.
5. Выполните команду `kubectl -n prelude get pods`.  
Дождитесь, когда заработают все модули.
6. Убедитесь, что ведение журнала отладки Kerberos включено.

```
kubectl -n prelude log {vco_app_name} -c vco-server-app | grep krb5
```

Убедитесь, что в журналах содержится сообщение, аналогичное приведенному ниже.

```
kubectl -n prelude log vco-app-5c965f9b9d-v8srd -c vco-server-app | grep krb5
12:23:05,417 INFO 011N:75 - Sysprop: java.security.krb5.conf = /usr/lib/vco/app-server/conf/
krb5.conf
12:23:05,421 INFO 011N:75 - Sysprop: sun.security.krb5.debug = true
2019-10-22 12:23:38.521+0000 [Thread-19] INFO {} [011N] Sysprop: java.security.krb5.conf
= /usr/lib/vco/app-server/conf/krb5.conf
2019-10-22 12:23:38.525+0000 [Thread-19] INFO {} [011N] Sysprop: sun.security.krb5.debug = true
Java config name: /usr/lib/vco/app-server/conf/krb5.conf
EType: sun.security.krb5.internal.crypto.Aes256CtsHmacSha1EType
```

## Включение расширений Opentracing и Wavefront

Расширения Opentracing и Wavefront для vRealize Orchestrator содержат средства сбора данных о среде vRealize Orchestrator. Эти данные можно использовать для устранения неполадок в системе и рабочих процессах vRealize Orchestrator.

Перед тем как настроить в vRealize Orchestrator использование расширений Opentracing и Wavefront, необходимо включить эти расширения в vRealize Orchestrator Appliance.

### Необходимые условия

Убедитесь, что включена служба SSH vRealize Orchestrator Appliance. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).

### Процедура

1. Войдите в vRealize Orchestrator Appliance через SSH в качестве **пользователя root**.
2. Выполните команду `kubectl -n prelude get pod`.
3. Чтобы получить список всех доступных расширений, запустите команду `kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app -- ls /var/lib/vco/app-server/extensions`.

4. Чтобы включить расширение Opentracing, запустите следующую команду:

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app --
mv /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar.inactive /var/lib/vco/app-server/extensions/
opentracing-8.1.0.jar
```

5. Чтобы включить расширение Wavefront, запустите следующую команду:

```
kubectl -n prelude exec -it vco-app-your_pod_ID -c vco-server-app --
mv /var/lib/vco/app-server/extensions/wavefront-8.1.0.jar.inactive /var/lib/vco/
app-server/extensions/wavefront-8.1.0.jar
```

6. Войдите в центр управления и убедитесь, что расширения отображаются на странице **Свойства расширения**.

### Следующие шаги

Настройте интеграцию Opentracing и Wavefront с vRealize Orchestrator на странице **Свойства расширения**. См. разделы [Настройка расширения Opentracing](#) и [Настройка расширения Wavefront](#).

## Настройка расширения Opentracing

Расширение Opentracing отправляет данные о выполнении рабочих процессов на сервер Jaeger. Эти данные включают в себя состояние рабочего процесса, входные и выходные параметры, имя пользователя, который инициировал запуск рабочего процесса, и сведения об идентификаторе рабочего процесса.

### Необходимые условия

- Проверьте, включено ли расширение Opentracing в vRealize Orchestrator Appliance. См. раздел [Включение расширений Opentracing и Wavefront](#).
- Выполните развертывание сервера Jaeger для использования в расширении Opentracing. Дополнительные сведения см. в [документации по началу работы с Jaeger](#).

### Процедура

1. Войдите в центр управления от имени пользователя **root**.
2. Перейдите на страницу **Свойства расширения**.
3. Выберите расширение Opentracing.
4. Введите адрес и порт узла сервера Jaeger.

---

**Примечание** Перед адресом сервера вставьте две косые черты (//).

---

5. Нажмите кнопку **Сохранить**.

### Результаты

Расширение Opentracing для vRealize Orchestrator настроено.

### Следующие шаги

- Для доступа к пользовательскому интерфейсу Jaeger, содержащему данные, собранные расширением Opentracing, перейдите по адресу узла, указанному во время настройки.
- В разделе **Служба** выберите **Рабочие процессы**.
- Чтобы указать данные для просмотра, используйте параметр **Теги**. Например, чтобы просмотреть данные о неудавшихся рабочих процессах, введите **status=failed**.

## Настройка расширения Wavefront

Расширение Wavefront используется для сбора данных о показателях системы vRealize Orchestrator и рабочих процессов.

## Необходимые условия

1. Проверьте, включено ли расширение Wavefront в vRealize Orchestrator Appliance. См. раздел [Включение расширений Opentracing и Wavefront](#).
2. Импортируйте сертификат Wavefront, выполнив следующие действия.
  - а) Войдите в центр управления vRealize Orchestrator от имени пользователя **root**.
  - б) Перейдите на страницу **Сертификаты**.
  - в) Щелкните раскрывающееся меню **Импорт** и выберите **Импортировать с URL-адреса**.
  - г) Введите URL-адрес Wavefront и нажмите **Импортировать**.
3. Настройте прокси-сервер Wavefront. Дополнительные сведения см. в разделе [Прокси-серверы Wavefront: установка и управление](#).

## Процедура

1. Войдите в центр управления vRealize Orchestrator от имени пользователя **root**.
2. Перейдите на страницу **Свойства расширения**.
3. Выберите расширение Wavefront.
4. Настройте свойства Wavefront.

Параметр	Описание
Прокси-сервер	Адрес прокси-сервера Wavefront.
Узел	(Необязательно). Адрес узла Wavefront.
Маркер	(Необязательно). Маркер API-интерфейса Wavefront. Дополнительные сведения о создании маркера API-интерфейса Wavefront см. в разделе <a href="#">Создание маркера API-интерфейса</a> .
Префикс	Добавьте метки префиксов для каждого показателя, отправляемого в Wavefront. Метки префиксов разделяются точкой.

5. (дополнительно) Выберите **Отправить панель управления по умолчанию при следующем запуске**.
6. Нажмите кнопку **Сохранить**.

## Результаты

Расширение Wavefront для vRealize Orchestrator настроено.

## Следующие шаги

- Для доступа к показателям, собранным расширением Wavefront, откройте панель управления по адресу, введенному в ходе настройки.
- Для получения уведомлений о конкретных событиях в среде vRealize Orchestrator можно использовать функцию оповещений Wavefront. Дополнительные сведения см. в [документации по функции оповещений Wavefront](#).

## Включение синхронизации времени в vRealize Orchestrator

Можно включить синхронизацию времени в развертывании vRealize Orchestrator с помощью командной строки vRealize Orchestrator Appliance.

С помощью протокола обмена данными NTP (Network Time Protocol, протокол сетевого времени) можно настроить синхронизацию времени для автономного или кластерного развертывания vRealize Orchestrator. vRealize Orchestrator поддерживает две взаимоисключающие конфигурации NTP:

Конфигурация NTP	Описание
ESXi	<p>Данную конфигурацию можно использовать, если сервер ESXi, на котором размещается vRealize Orchestrator Appliance, синхронизирован с сервером NTP. При использовании кластерного развертывания все узлы ESXi должны быть синхронизированы с сервером NTP. Дополнительные сведения о настройке NTP для ESXi см. в разделе <a href="#">Настройка протокола NTP (Network Time Protocol) на узле ESXi с помощью vSphere Web Client</a>.</p> <p><b>Примечание</b> Если развертывание vRealize Orchestrator переносится на узел ESXi, который не синхронизирован с сервером NTP, может произойти рассинхронизация.</p>
systemd	<p>В этой конфигурации используется управляющая программа systemd-timesyncd, с помощью которой и выполняется синхронизация часов развертывания vRealize Orchestrator.</p> <p><b>Примечание</b> По умолчанию управляющая программа systemd-timesyncd включена, но в ней не настроены серверы NTP. Если в vRealize Orchestrator Appliance используется динамическая настройка IP-адресов, устройство может использовать любые серверы NTP, полученные протоколом DHCP.</p>

### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Включите NTP с помощью ESXi.
  - а) Выполните команду `vracli ntp esxi`.
  - б) Выполните команду `vracli ntp apply`.

Конфигурация NTP ESXi применяется к развертыванию vRealize Orchestrator.



**3.** Включите NTP с помощью systemd.

- а) Запустите команду `vracli ntp systemd --set FQDN_или_IP-адрес_сервера_systemd`.

---

**Примечание** Можно добавить несколько серверов NTP systemd, разделяя их сетевые адреса запятыми.

---

- б) Выполните команду `vracli ntp apply`.

Конфигурация NTP systemd применяется к разворачиванию vRealize Orchestrator.

- 4.** (дополнительно) Чтобы подтвердить состояние конфигурации NTP, запустите команду `vracli ntp status`.

**Следующие шаги**

Настройка NTP может оказаться неудачной, если разница во времени между сервером NTP и разворачиванием vRealize Orchestrator составляет более 10 минут. Чтобы устранить эту проблему, перезагрузите vRealize Orchestrator Appliance.

## Отключение синхронизации времени в vRealize Orchestrator

Можно отключить синхронизацию времени протокола NTP (Network Time Protocol, протокол сетевого времени) в разворачивании vRealize Orchestrator с помощью командной строки vRealize Orchestrator Appliance.

Можно также сбросить конфигурацию NTP в vRealize Orchestrator Appliance до состояния по умолчанию, запустив команду `vracli ntp reset`. После сброса конфигурации необходимо применить изменения, запустив команду `vracli ntp apply`.

**Необходимые условия**

Убедитесь, что настроена синхронизация времени с ESXi или systemd. См. раздел [Включение синхронизации времени в vRealize Orchestrator](#).

**Процедура**

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Чтобы отключить синхронизацию времени с ESXi или systemd, запустите команду `vracli ntp disable`.
3. Выполните команду `vracli ntp apply`.
4. (дополнительно) Чтобы подтвердить состояние конфигурации NTP, запустите команду `vracli ntp status`.

# Конфигурация: примеры использования и устранение неполадок

## 8

В примерах использования конфигураций представлены алгоритмы выполнения задач, позволяющие удовлетворить особые требования к конфигурации сервера vRealize Orchestrator, а также рекомендации по устранению неполадок, которые помогут разобраться в проблеме и решить ее.

В эту главу входят следующие разделы:

- [Настройка подключаемого модуля vRealize Orchestrator для vSphere Web Client](#)
- [Отмена выполняемых рабочих процессов](#)
- [Включение отладки сервера vRealize Orchestrator](#)
- [Изменение размера дисков vRealize Orchestrator Appliance](#)
- [Масштабирование объема памяти кучи на сервере vRealize Orchestrator](#)
- [Аварийное восстановление vRealize Orchestrator с помощью Site Recovery Manager](#)

## Настройка подключаемого модуля vRealize Orchestrator для vSphere Web Client

Чтобы использовать подключаемый модуль vRealize Orchestrator для vSphere Web Client, необходимо зарегистрировать vRealize Orchestrator в качестве расширения vCenter Server.

Зарегистрировав сервер vRealize Orchestrator с помощью vCenter Single Sign-On и настроив его для работы с vCenter Server, необходимо зарегистрировать vRealize Orchestrator в качестве расширения vCenter Server.

### Необходимые условия

- Убедитесь, что для vRealize Orchestrator Appliance включен доступ по протоколу SSH. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).
- Необходимо зарегистрировать vRealize Orchestrator с проверкой подлинности vSphere на том же экземпляре Platform Services Controller, с помощью которого вы управляете проверкой подлинности vCenter Server.

- Скопируйте файл `vco-plugin.zip` в vRealize Orchestrator Appliance.
  - а) Загрузите файл `vco-plugin.zip` с портала [VMware Technology Network](#).
  - б) Откройте SSH-клиент.

---

**Примечание** В средах Linux и MacOS можно использовать интерфейс командной строки терминала. В среде Windows можно использовать клиент PuTTY.

---

- в) Чтобы скопировать файл `vco-plugin.zip`, используйте команду безопасного копирования.

For Linux/MacOS: `scp ~/<zip_download_dir>/vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip`

For Windows: `pscp C:\<zip_download_dir>\vco-plugin.zip root@<orchestrator_FQDN_or_IP>:/data/vco/usr/lib/vco/downloads/vco-plugin.zip`

#### Процедура

1. Выполните вход в vRealize Orchestrator Client.
2. Перейдите в раздел **Библиотека > Рабочие процессы**.
3. Найдите рабочий процесс **Регистрация vCenter Orchestrator в качестве расширения vCenter Server** и нажмите **Запустить**.
4. Выберите экземпляр vCenter Server, используемый для регистрации vRealize Orchestrator.
5. Введите `https://FQDN_оркестратора` или служебный URL-адрес подсистемы балансировки нагрузки, перенаправляющей запросы на узлы сервера vRealize Orchestrator.
6. Нажмите **Запустить**.

## Отмена выполняемых рабочих процессов

С помощью центра управления vRealize Orchestrator можно отменять рабочие процессы, которые не завершаются должным образом.

#### Процедура

1. Выполните вход в Центр управления в качестве **привилегированного пользователя root**.
2. Нажмите **Устранение неполадок**.

### 3. Отмените выполняемые рабочие процессы.

Параметр	Описание
Отмена всех циклов рабочего процесса	Введите идентификатор рабочего процесса, чтобы отменить все маркеры этого рабочего процесса.
Отменить выполнение рабочего процесса по идентификатору	Введите все идентификаторы маркеров, которые следует отменить. В качестве разделителя между идентификаторами используйте запятые.
Отмена всех выполняемых рабочих процессов	Отмена всех выполняемых рабочих процессов на сервере.

**Примечание** Операции по отмене выполнения рабочих процессов по идентификатору могут завершаться неудачно, так как надежного способа мгновенно отменить выполнение потока процессов не существует.

#### Результаты

При следующем запуске сервера отмененные рабочие процессы будут по-прежнему находиться в состоянии отмены.

## Включение отладки сервера vRealize Orchestrator

Для решения проблем, возникших при разработке подключаемого модуля, можно запустить сервер vRealize Orchestrator в режиме отладки.

#### Необходимые условия

Установите и настройте средство командной строки Kubernetes на локальном компьютере. См. раздел [Установка и настройка kubectl](#).

#### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Выполните команду `kubectl -n prelude edit deployment vco-app`.
3. Отредактируйте файл развертывания YAML, добавив переменную среды отладки в контейнер `vco-server-app`. Переменная должна быть добавлена в раздел `env` контейнера `vco-server-app`.

```
containers:
  - command:
    ...
    env:
      - name: DEBUG_PORT
```

```

        value: "your_desired_debug_port"
        ...
    name: vco-server-app
    ...

```

**Примечание** При добавлении переменной среды отладки в раздел `env` необходимо следовать форматированию отступов YAML, как показано в предыдущем примере.

**4.** Сохраните изменения в файле развертывания.

При успешном внесении изменений в файл развертывания появляется сообщение `deployment.extensions/vco-app edited`.

**5.** Создайте файл конфигурации Kubernetes, запустив команду `vracli dev kubeconfig`.

Так как `kubeconfig` является средой разработчика, появится запрос подтвердить дальнейшие действия. Введите **yes** (да) для продолжения или **no** (нет), чтобы прервать процедуру.

**6.** Скопируйте содержимое созданного файла конфигурации, начиная со строки `apiVersion: v1` и заканчивая строкой `client-key-data` включительно.

**7.** Сохраните созданный файл конфигурации Kubernetes на локальном компьютере.

**8.** Выйдите из vRealize Orchestrator Appliance.

**9.** Завершите настройку режима отладки на локальном компьютере.

- а) Откройте оболочку командной строки.
- б) Привяжите переменную среды `KUBECONFIG` к сохраненному файлу конфигурации.

**Примечание** В качестве примера используется среда Linux.

```
export KUBECONFIG=/file/path/fileName
```

- в) Чтобы проверить, запущены ли службы, выполните команду `kubectl cluster-info`.

- г) Чтобы завершить настройку режима отладки, выполните следующий запрос API-интерфейса Kubernetes.

**Примечание** Значение переменной `порт_отладки_локального_узла` — это порт, заданный в конфигурации удаленной отладки интегрированной среды разработки (IDE). Значение переменной `порт_отладки_vro` генерируется при выполнении шага 3 данной процедуры.

```
kubectl port-forward pod/ид_модуля_приложения_vco порт_отладки_локального_узла:порт_отладки_vro
```

**Важно!** При настройке средства отладки укажите параметры DNS и IP-адреса для локального компьютера, на котором была выполнена команда переадресации портов.

## Результаты

Отладка сервера для vRealize Orchestrator Appliance настроена.

## Изменение размера дисков vRealize Orchestrator Appliance

Размер диска vRealize Orchestrator Appliance можно изменить, отредактировав параметры размера диска виртуальной машины vRealize Orchestrator Appliance в vSphere.

### Необходимые условия

Убедитесь, что включена служба SSH vRealize Orchestrator Appliance. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).

### Процедура

1. Проверьте свободное место на диске в vRealize Orchestrator Appliance.

---

**Примечание** Для дисков vRealize Orchestrator Appliance требуется по крайней мере 20 % свободного дискового пространства.

---

- а) Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
  - б) Выполните команду `vracli disk-mgr`.
2. Измените размер диска виртуальной машины vRealize Orchestrator Appliance в vSphere.
    - а) Войдите в vSphere Client от имени **администратора**.
    - б) Выключите виртуальную машину vRealize Orchestrator Appliance.
    - в) Щелкните виртуальную машину правой кнопкой мыши и выберите команду **Изменить параметры**.
    - г) На вкладке **Виртуальное оборудование** разверните **Жесткий диск** для просмотра и изменения параметров диска, а затем нажмите **ОК**.

Дополнительные сведения об изменении размера диска виртуальных машин vSphere см. в разделе *Изменение конфигурации виртуального диска* руководства *Администрирование виртуальных машин vSphere*.

## Масштабирование объема памяти кучи на сервере vRealize Orchestrator

Объем памяти кучи на сервере vRealize Orchestrator можно увеличить, внося изменения в файл развертывания.

Можно настроить объем памяти кучи на сервере vRealize Orchestrator, чтобы среда оркестрации могла управлять изменяющимися нагрузками. Например, можно увеличить память кучи развертывания vRealize Orchestrator, если планируется управление несколькими серверами vCenter.

### Необходимые условия

- Активируйте доступ к vRealize Orchestrator Appliance по протоколу SSH. См. раздел [Включение и отключение доступа к vRealize Orchestrator Appliance по протоколу SSH](#).

- Увеличьте объема ОЗУ виртуальной машины, на которой проводится развертывание vRealize Orchestrator, до следующего допустимого уровня. Сведения о том, как увеличить объем ОЗУ виртуальной машины в vSphere, см. в разделе *Изменение конфигурации памяти* руководства *Администрирование виртуальных машин vSphere*.

#### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
2. Перейдите в каталог `/opt/charts/vco/templates/`.
3. Создайте резервную копию файла `deployment.yaml`.

```
cp deployment.yaml /tmp/
```

4. С помощью текстового редактора внесите изменения в файл `deployment.yaml`.

```
vi deployment.yaml
```

5. Выполните поиск строк, содержащих значение `env`, пока не найдете контейнер `vco-server-app`.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JAVA_PROXY_SCHEMEE
```

6. В разделе `env` добавьте переменную среды `JVM_HEAP` со значением, где `{DESIRED_HEAP_SIZE}` соответствует новому требуемому объему памяти кучи, например `4G`.

```
- name: vco-server-app
  image: {{ .Values.image.repository }}:{{ .Values.image.tag }}
  env:
    - name: JVM_HEAP
      value: {DESIRED_HEAP_SIZE}
    - name: JAVA_PROXY_SCHEME
```

7. Выполните поиск строк, содержащих строку `memory: 5G`, в файле развертывания.

---

**Примечание** В файле развертывания должна присутствовать только одна строка `memory: 5G`.

---

```
resources:
  limits:
    memory: 5G
  requests:
    memory: 4G
```

**8.** Увеличьте количество ограничений и запросов контейнера.

**Осторожно!** Значение ограничений `memory`: должно быть на 2 ГБ больше, чем значение памяти `JVM_HEAP`, указанное в шаге 6. Например, если в шаге 6 указано значение `value: 4G`, необходимо установить значение ограничения объема памяти `memory: 6G`. Значение `requests: memory` должно быть на 1 ГБ больше, чем значение памяти `JVM_HEAP`, указанное в шаге 6. Например, если в шаге 6 в качестве значения кучи указано `value: 4G`, для памяти запросов необходимо указать значение `memory: 5G`.

```
resources:
  limits:
    memory: {Desired heap size + 2G}
  requests:
    memory: {Desired heap size + 1G}
```

**9.** Сохраните изменения в файле разворачивания и перейдите в каталог `/opt/scripts`.

**Примечание** При работе в кластерной среде примените приведенные выше шаги ко всем узлам кластера.

**10.** Выполните команду `deploy.sh`.

**Примечание** Если среда является кластерной, запустите сценарий разворачивания на основном узле.

**Результаты**

Объем памяти кучи для сервера vRealize Orchestrator был изменен.

## Аварийное восстановление vRealize Orchestrator с помощью Site Recovery Manager

Необходимо настроить Site Recovery Manager для защиты vRealize Orchestrator. Чтобы обеспечить защиту, выполните стандартные задачи по настройке в Site Recovery Manager.

### Подготовка среды

Перед настройкой Site Recovery Manager необходимо убедиться, что выполнены следующие необходимые условия.

- Убедитесь, что на защищенных сайтах и в среде аварийного восстановления установлено программное обеспечение vSphere 6.0 или более поздней версии.
- Убедитесь, что используется Site Recovery Manager 8.1 или более поздней версии.
- Убедитесь, что выполнена настройка vRealize Orchestrator.

### Настройка виртуальных машин для vSphere Replication

Необходимо настроить виртуальные машины для vSphere Replication или репликации на основе массива, чтобы использовать Site Recovery Manager.



Чтобы включить vSphere Replication на требуемых виртуальных машинах, выполните следующие действия.

#### Процедура

1. В vSphere Web Client выберите виртуальную машину, на которой нужно включить vSphere Replication, и нажмите **Действия > Все действия vSphere Replication > Настроить репликацию**.
2. В окне **Тип репликации** выберите **Реплицировать в vCenter Server** и нажмите **Далее**.
3. В окне **Целевой сайт** выберите vCenter в качестве среды аварийного восстановления и нажмите **Далее**.
4. В окне **Сервер репликации** выберите сервер vSphere Replication и нажмите **Далее**.
5. В окне **Целевое расположение** нажмите **Изменить**, выберите целевое хранилище данных, где будут храниться реплицированные файлы, и нажмите **Далее**.
6. В окне **Параметры репликации** оставьте настройки по умолчанию и нажмите **Далее**.
7. В окне **Настройки восстановления** введите время для параметра **Целевая точка восстановления (RPO)** и **Экземпляры момента времени**, затем нажмите **Далее**.
8. В окне **Готово к завершению** проверьте настройки и нажмите **Готово**.
9. Повторите эти действия для всех виртуальных машин, на которых необходимо включить vSphere Replication.

## Создание групп защиты

Группы защиты создаются для того, чтобы дать Site Recovery Manager возможность защищать виртуальные машины.

Группы защиты можно распределить по папкам. На вкладке **Группы защиты** отображаются имена групп защиты, но не отображаются папки, в которых они размещены. При наличии двух групп защиты с одинаковыми именами из разных папок их может быть трудно различить. Поэтому необходимо, чтобы имена групп защиты во всех папках были уникальными. В средах, где не все пользователи обладают правами просмотра всех папок, чтобы обеспечить уникальность имен групп защиты, не размещайте группы защиты в папках.

При создании групп защиты дождитесь успешного завершения операций. Убедитесь, что группа защиты создана в Site Recovery Manager и что защита виртуальных машин в группе выполняется успешно.

#### Необходимые условия

Убедитесь, что выполнено одно из следующих действий.

- Виртуальные машины входят в хранилища данных, для которых настроена репликация на основе массива.
- Выполнены *необходимые условия для создания групп защиты политик хранения* и учтены *ограничения групп безопасности политик хранения*, приведенные в руководстве *Администрирование Site Recovery Manager*.

- На виртуальных машинах настроена репликация vSphere Replication.
- Выполнены некоторые или все вышеуказанные действия.

#### Процедура

1. В vSphere Client или vSphere Web Client щелкните **Site Recovery > Открыть Site Recovery**.
2. На главной вкладке Site Recovery выберите пару сайтов и нажмите **Просмотреть сведения**.
3. Перейдите на вкладку **Группы защиты** и нажмите кнопку **Создать**, чтобы создать группу защиты.
4. На странице «Имя и направление» введите имя и описание группы защиты, выберите направление и нажмите **Далее**.
5. На странице «Тип группы защиты» выберите тип группы защиты и нажмите кнопку **Далее**.

Параметр	Действие
Создать группу защиты репликации на основе массива	Выберите <b>Группы хранилищ данных (репликация на основе массива)</b> и пару массивов.
Создать группу защиты vSphere Replication	Выберите <b>Отдельные ВМ (vSphere Replication)</b> .
Создать группу защиты политик хранения	Выберите <b>Политики хранения (репликация на основе массива)</b> .

6. Выберите группы хранилищ данных, виртуальные машины или политики хранения, которые следует добавить в группу защиты.

Параметр	Действие
Группы защиты репликации на основе массива	Выберите группы хранилищ данных и нажмите <b>Далее</b> . При выборе группы хранилищ данных виртуальные машины, которые находятся в группе, отображаются в таблице виртуальных машин.
Группы защиты vSphere Replication	Выберите виртуальные машины из списка и нажмите <b>Далее</b> . В списке отображаются только те виртуальные машины, которые были настроены для vSphere Replication и еще не включены в группу защиты.
Группы защиты политик хранения	Выберите политики хранения из списка и нажмите <b>Далее</b> .

7. На странице «План восстановления» можно при необходимости добавить группу защиты в план восстановления.

Параметр	Действие
Добавить в существующий план восстановления	Добавление группы защиты в существующий план восстановления.
Добавить в новый план восстановления	Добавление группы защиты в новый план восстановления. При выборе этого параметра необходимо ввести имя плана восстановления.
Не добавлять в план восстановления	Выберите этот параметр, чтобы не добавлять группу защиты в план восстановления.

## 8. Проверьте выбранные настройки и нажмите кнопку **Готово**.

Ход создания группы защиты можно отслеживать на вкладке **Группа защиты**.

- Группы защиты репликации на основе массива и группы защиты vSphere Replication: если в Site Recovery Manager к защищенным виртуальным машинам были успешно применены сопоставления иерархии, в качестве состояния группы защиты будет указано *ОК*.
- Группы защиты политик хранения: если в Site Recovery Manager была успешно обеспечена защита всех виртуальных машин, связанных с политикой хранения, в качестве состояния группы защиты будет указано *ОК*.
- Группы защиты репликации на основе массива и группы защиты vSphere Replication: если сопоставления иерархии не были настроены или если Site Recovery Manager не удалось их применить, в качестве состояния группы защиты будет указано *не настроено*.
- Группы защиты политик хранения: если Site Recovery Manager не может обеспечить защиту всех виртуальных машин, связанных с политикой хранения, то в качестве состояния группы защиты будет указано *не настроено*.

### Следующие шаги

Группы защиты репликации на основе массива и группы защиты vSphere Replication: если в качестве состояния защиты групп защиты указано *не настроено*, примените сопоставления иерархии к виртуальным машинам.

- Сведения о том, как применить сопоставления иерархии ко всему сайту или проверить правильность уже настроенных сопоставлений иерархии, см. в разделе *Настройка сопоставлений иерархии* в руководстве *Администрирование Site Recovery Manager*. Сведения о том, как применить эти сопоставления ко всем виртуальным машинам, см. в разделе *Применение сопоставлений иерархии ко всем участникам группы защиты* в руководстве *Администрирование Site Recovery Manager*.
- Сведения о том, как применить сопоставления иерархии по отдельности к каждой виртуальной машине в группе защиты, см. в разделе *Настройка сопоставлений иерархии для отдельной виртуальной машины в группе защиты* в руководстве *Администрирование Site Recovery Manager*.

Группы защиты политик хранения: если в качестве состояния защиты группы защиты указано *не настроено*, убедитесь, что выполнены *необходимые условия для создания групп защиты политик хранения* и учтены *ограничения групп безопасности политик хранения*, приведенные в руководстве *Администрирование Site Recovery Manager*.

## Создание плана восстановления

В плане восстановления содержатся сведения о том, каким образом Site Recovery Manager будет восстанавливать виртуальные машины.

### Процедура

1. В vSphere Client или vSphere Web Client выберите **Site Recovery > Открыть Site Recovery**.
2. На главной вкладке Site Recovery выберите пару сайтов и нажмите **Просмотреть сведения**.

3. Выберите вкладку **Планы восстановления** и нажмите кнопку **Создать**, чтобы создать план восстановления.
4. Введите имя, описание и направление для плана, выберите папку и нажмите кнопку **Далее**.
5. Выберите тип группы в меню.

Параметр	Описание
Группы защиты для отдельных ВМ или групп хранилищ данных	Выберите этот параметр, чтобы создать план восстановления, включающий в себя репликацию на основе массива и группы защиты vSphere Replication.
Группы защиты политик хранения	Выберите этот параметр, чтобы создать план восстановления, включающий в себя группы защиты политик хранения. Данный параметр используется при распределенном хранении.

6. Выберите одну или несколько групп защиты для восстановления с помощью плана и нажмите **Далее**.
7. В раскрывающемся меню **Тестовая сеть** выберите сеть, которая будет использоваться для тестового восстановления, и нажмите **Далее**.

Если сопоставления на уровне сайта отсутствуют, то параметр по умолчанию **Использовать сопоставление на уровне сайта** создаст изолированную тестовую сеть.

8. Ознакомьтесь с данными сводки и нажмите кнопку **Готово**, чтобы создать план восстановления.

## Упорядочение планов восстановления по папкам

Чтобы управлять доступом различных пользователей или групп к планам восстановления, можно упорядочить планы восстановления по папкам.

Упорядочение планов восстановления по папкам полезно при наличии большого количества планов восстановления. Можно ограничить доступ к планам восстановления, размещая их в папках и назначая папкам различные разрешения для различных пользователей или групп. Дополнительные сведения о назначении разрешений для папок см. в разделе *Назначения ролей и разрешений Site Recovery Manager* руководства *Администрирование Site Recovery Manager*.

### Процедура

1. На главной вкладке **Site Recovery** выберите пару сайтов и нажмите **Просмотреть сведения**.
2. Перейдите на вкладку **Планы восстановления**, затем на панели слева щелкните правой кнопкой мыши **Планы восстановления** и выберите **Создать папку**.
3. Введите имя создаваемой папки и нажмите кнопку **Добавить**.
4. Добавьте в папку новые или существующие планы восстановления.

Параметр	Описание
Создание нового плана восстановления	Щелкните правой кнопкой мыши папку и выберите <b>Создать план восстановления</b> .
Добавление существующего плана восстановления	Щелкните правой кнопкой мыши план восстановления в иерархическом древе и выберите <b>Переместить</b> . Выберите целевую папку и нажмите кнопку <b>Переместить</b> .

## Изменение плана восстановления

Планы восстановления можно редактировать, изменяя свойства, которые были указаны при их создании. Планы восстановления можно изменить из среды охраняемого объекта или из среды аварийного восстановления.

### Процедура

1. В vSphere Client или vSphere Web Client нажмите **Site Recovery > Открыть Site Recovery**.
2. На главной вкладке **Site Recovery** выберите пару сайтов и нажмите **Просмотреть сведения**.
3. Перейдите на вкладку **Планы восстановления**, правой кнопкой мыши щелкните план восстановления и выберите **Изменить**.
4. (дополнительно) Измените имя или описание плана и нажмите кнопку **Далее**.  
Направление и расположение плана восстановления изменить нельзя.
5. (дополнительно) Выберите одну или несколько групп защиты, чтобы добавить их в план, либо отмените их выбор, чтобы удалить из плана, и нажмите **Далее**.
6. (дополнительно) В раскрывающемся меню выберите другую тестовую сеть в среде аварийного восстановления и нажмите **Далее**.
7. Просмотрите данные сводки и нажмите кнопку **Готово**, чтобы внести указанные изменения в план восстановления.

Обновления плана можно отслеживать в режиме просмотра **Последние задачи**.

# Настройка свойств системы

# 9

Настроив свойства системы, можно изменить поведение Orchestrator по умолчанию.

В эту главу входят следующие разделы:

- [Настройка доступа к файловой системе сервера для рабочих процессов и действий](#)
- [Настройка доступа к командам операционной системы для рабочих процессов и действий](#)
- [Настройка доступа JavaScript к классам Java](#)
- [Задание свойства настраиваемого времени ожидания](#)
- [Добавление соединителя JDBC для подключаемого модуля SQL vRealize Orchestrator](#)

## Настройка доступа к файловой системе сервера для рабочих процессов и действий

В vRealize Orchestrator рабочие процессы и действия имеют ограниченный доступ к некоторым каталогам файловой системы. Расширить доступ к другим частям файловой системы сервера можно, изменив файл конфигурации `js-io-rights.conf`.

### Правила в файле `js-io-rights.conf`, разрешающие доступ для записи в системе vRealize Orchestrator

Файл `js-io-rights.conf` содержит правила, разрешающие доступ для записи к определенным каталогам в файловой системе сервера.

#### Обязательное содержимое файла `js-io-rights.conf`

Каждая строка в файле `js-io-rights.conf` должна содержать следующую информацию:

- знак плюс (+) или минус (-), указывающий, разрешены или запрещены права;
- уровни прав: чтение (r), запись (w) и запуск (x);

- путь, к которому применяются права.

---

**Примечание** Корневым каталогом для файла `js-io-rights.conf` всегда является `/var/run/vco`. В файловой системе vRealize Orchestrator Appliance эта папка находится в расположении `/data/vco/var/run/vco`. Все содержимое с доступом к файловой системе vRealize Orchestrator должно быть сопоставлено с этой корневой папкой.

---

## Содержимое файла `js-io-rights.conf` по умолчанию

По умолчанию содержимое файла конфигурации `js-io-rights.conf` в Orchestrator Appliance выглядит следующим образом:

```
-rwx /
+rwx /var/run/vco
-rwx /etc/vco/app-server/security/
+rx /etc/vco
+rx /var/log/vco/
```

Первые две строки в файле конфигурации `js-io-rights.conf` по умолчанию предоставляют следующие права доступа:

**-rwx /**

Полный доступ к файловой системе запрещен.

**+rwx /var/run/vco**

Доступ на чтение, запись и запуск разрешен в каталоге `/var/run/vco`.

## Правила в файле `js-io-rights.conf`

vRealize Orchestrator разрешает права доступа в том порядке, в котором они указаны в файле `js-io-rights.conf`. Каждая строка может переопределять предыдущие строки.

---

**Важно!** Можно разрешить доступ ко всем частям файловой системы, задав правило `+rwx /` в файле `js-io-rights.conf`. Однако это представляет большую угрозу для безопасности.

---

## Настройка доступа к файловой системе сервера для рабочих процессов и действий

Чтобы указать, к каким частям файловой системы сервера имеют доступ рабочие процессы и API-интерфейс vRealize Orchestrator, можно изменить файл конфигурации `js-io-rights.conf`. Файл `js-io-rights.conf` создается, когда рабочий процесс пытается получить доступ к файловой системе сервера vRealize Orchestrator.

### Процедура

1. Войдите в командную строку vRealize Orchestrator Appliance в качестве пользователя **root**.
2. Перейдите в каталог `/data/vco/var/run/vco/`.
3. Откройте файл конфигурации `js-io-rights.conf` в текстовом редакторе.

4. Добавьте необходимые строки в файл `js-io-rights.conf`, чтобы разрешить или запретить доступ к областям файловой системы.

Например, следующая строка запрещает права на выполнение в каталоге `/data/vco/var/run/vco/noexec/`:

```
-x /data/vco/var/run/vco/noexec
```

Каталог `/data/vco/var/run/vco/noexec` сохраняет права на выполнение, а `/data/vco/var/run/vco/noexec/bar` — нет. Оба каталога останутся доступными для чтения и записи.

## Результаты

Права доступа к файловой системе для рабочих процессов и API-интерфейса vRealize Orchestrator изменены.

## Настройка доступа к командам операционной системы для рабочих процессов и действий

API-интерфейс vRealize Orchestrator предоставляет класс сценариев `Command`, который выполняет команды в операционной системе сервера vRealize Orchestrator. Для предотвращения несанкционированного доступа к узлу сервера по умолчанию приложениям vRealize Orchestrator не предоставляется разрешение на запуск класса `Command`. Если приложениям vRealize Orchestrator требуется разрешение на выполнение команд в операционной системе узла, класс сценариев `Command` можно активировать.

Предоставить разрешение на использование класса `Command` можно, задав свойство системы конфигурации vRealize Orchestrator.

### Процедура

1. Выполните вход в Центр управления в качестве привилегированного пользователя **root**.
2. Щелкните **Свойства системы**.
3. Нажмите кнопку **Создать**.
4. В текстовом поле **Ключ** введите **com.vmware.js.allow-local-process**.
5. В текстовом поле **Значение** введите **true**.
6. В текстовом поле **Описание** введите описание системного свойства.
7. Нажмите кнопку **Добавить**.
8. Нажмите **Сохранить изменения** во всплывающем меню.  
Появится сообщение с подтверждением сохранения.
9. Дождитесь перезапуска сервера vRealize Orchestrator.



## Результаты

Приложениям vRealize Orchestrator предоставлены разрешения на запуск локальных команд в операционной системе сервера vRealize Orchestrator.

---

**Примечание** Задав для свойства системы `com.vmware.js.allow-local-process` значение `true`, вы разрешили классу сценариев `Command` выполнять запись в любом месте файловой системы. Это свойство переопределяет все разрешения на доступ к файловой системе, установленные в файле `js-io-rights.conf`, только для класса сценариев `Command`. Разрешения на доступ к файловой системе, заданные в файле `js-io-rights.conf`, по-прежнему применяются ко всем прочим классам сценариев помимо `Command`.

---

## Настройка доступа JavaScript к классам Java

По умолчанию vRealize Orchestrator разрешает доступ JavaScript только к ограниченному набору классов Java. Если требуется предоставить JavaScript доступ к более широкому диапазону классов Java, необходимо задать свойство системы vRealize Orchestrator.

Предоставление обработчику JavaScript полного доступа к виртуальной машине Java (JVM) является потенциальной угрозой безопасности. Неправильные или вредоносные сценарии могут получить доступ ко всем компонентам системы, доступным пользователю, запускающему сервер vRealize Orchestrator. Поэтому по умолчанию обработчик JavaScript vRealize Orchestrator имеет доступ только к классам в пакете `java.util.*`.

Если требуется предоставить JavaScript доступ к классам за пределами пакета `java.util.*`, можно указать в файле конфигурации пакеты Java, доступ к которым разрешен. Затем настройте свойство системы `com.vmware.scripting.rhino-class-shutter-file`, чтобы оно указывало на этот файл.

### Процедура

1. Создайте текстовый файл конфигурации для хранения списка пакетов Java, к которым разрешен доступ JavaScript.

Например, чтобы разрешить JavaScript доступ ко всем классам в пакете `java.net` и классу `java.lang.Object`, добавьте в файл следующее содержимое.

```
java.net.*
java.lang.Object
```

2. Введите имя файла конфигурации.
3. Сохраните файл конфигурации в подкаталоге `/data/vco/usr/lib/vco`.

---

**Примечание** Файл конфигурации нельзя сохранить в другом каталоге.

---

4. Выполните вход в Центр управления в качестве **привилегированного пользователя root**.
5. Щелкните **Свойства системы**.
6. Нажмите кнопку **Создать**.

7. В текстовом поле **Ключ** введите `com.vmware.scripting.rhino-class-shutter-file`.
8. В текстовом поле **Значение** введите `vco/usr/lib/vco/подкаталог_файла_конфигурации`.
9. В текстовом поле **Описание** введите описание системного свойства.
10. Нажмите кнопку **Добавить**.
11. Нажмите **Сохранить изменения** во всплывающем меню.  
Появится сообщение с подтверждением сохранения.
12. Дождитесь перезапуска сервера vRealize Orchestrator.

#### Результаты

Модуль JavaScript получил доступ к указанным классам Java.

## Задание свойства настраиваемого времени ожидания

При перезагрузке vCenter Server для возврата ответа на сервер vRealize Orchestrator требуется больше времени, чем заданные по умолчанию 20 000 миллисекунд. Чтобы избежать такой ситуации, необходимо изменить файл конфигурации vRealize Orchestrator и повысить период времени ожидания по умолчанию.

Если время ожидания по умолчанию истекает до завершения определенных операций, в журнал сервера vRealize Orchestrator записываются ошибки.

```
Operation 'getPropertyContent' total time : '5742228' for 1823 calls, mean time :  
'3149.0', min time : '0', max time : '32313' Timeout, unable to get property 'info'  
com.vmware.vmo.plugin.vi4.model.TimeoutException
```

#### Процедура

1. Выполните вход в Центр управления в качестве **привилегированного пользователя root**.
2. Щелкните **Свойства системы**.
3. Нажмите кнопку **Создать**.
4. В текстовом поле **Ключ** введите `com.vmware.vmo.plugin.vi4.waitUpdatesTimeout`.
5. В текстовом поле **Значение** введите новое время ожидания в миллисекундах.
6. (дополнительно) В текстовом поле **Описание** введите описание системного свойства.
7. Нажмите кнопку **Добавить**.
8. Нажмите **Сохранить изменения** во всплывающем меню.  
Появится сообщение с подтверждением сохранения.
9. Перезапустите сервер Orchestrator.

## Результаты

Заданное значение переопределит значение времени ожидания по умолчанию, равное 20 000 миллисекундам.

# Добавление соединителя JDBC для подключаемого модуля SQL vRealize Orchestrator

В этом примере показано, как добавить соединитель MySQL для подключаемого модуля SQL vRealize Orchestrator.

## Процедура

### 1. Добавьте файл соединителя MySQL с расширением JAR в vRealize Orchestrator Appliance.

- а) Войдите в командную строку vRealize Orchestrator Appliance по протоколу SSH в качестве пользователя **root**.
- б) Перейдите в каталог `/data/vco/var/run/vco`.

```
cd /data/vco/var/run/vco
```

- в) Создайте каталог `plugins/SQL/lib/`.

```
mkdir -p plugins/SQL/lib/
```

- г) Скопируйте файл JAR соединителя MySQL с локального компьютера в каталог `/data/vco/var/run/vco/plugins/SQL/lib/`, запустив команду безопасного копирования (SCP).

```
scp ~/local_machine_dir/your_mysql_connector.jar root@orchestrator_FQDN_or_IP:/data/vco/var/run/vco/plugins/SQL/lib/
```

---

**Примечание** Для копирования файла JAR соединителя в vRealize Orchestrator Appliance также можно использовать другие методы, например PSCP.

---

### 2. Добавьте новое свойство MySQL в центр управления.

- а) Войдите в центр управления от имени пользователя **root**.
- б) Выберите **Свойства системы**.
- в) Нажмите кнопку **Создать**.
- г) В поле **Ключ** введите **o11n.plugin.SQL.classpath**.

- д) В поле **Значение** введите `/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar`.

---

**Примечание** В текстовом поле значений можно указать несколько соединителей JDBC, используя в качестве разделителя точку с запятой (;). Пример:

```
/var/run/vco/plugins/SQL/lib/your_mysql_connector.jar;/var/run/vco/plugins/SQL/lib/your_mssql_connector.jar;/var/run/vco/plugins/SQL/lib/your_other_connector.jar
```

- е) (дополнительно) Введите описание свойства системы MySQL.
- ж) Нажмите кнопку **Добавить** и дождитесь перезапуска сервера vRealize Orchestrator.

---

**Примечание** Не сохраняйте файл JAR соединителя JDBC в другом каталоге и не указывайте другое значение для свойства `o11n.plugin.SQL.classpath`. В противном случае соединитель JDBC будет недоступен для развертывания vRealize Orchestrator.

---

## Дальнейшие действия

# 10

После установки и настройки vRealize Orchestrator можно использовать vRealize Orchestrator для автоматизации часто повторяемых процессов, связанных с управлением виртуальной средой.

- Выполните вход в vRealize Orchestrator Client, запустите и запланируйте рабочие процессы на объектах иерархии vCenter Server или других объектах, к которым vRealize Orchestrator получает доступ с помощью подключаемых модулей. См. руководство *Использование клиента VMware vRealize Orchestrator*.
- Скопируйте и измените стандартные рабочие процессы vRealize Orchestrator и напишите собственные действия и рабочие процессы для автоматизации операций в vCenter Server.
- Чтобы расширить функциональные возможности платформы vRealize Orchestrator, можно разработать подключаемые модули.
- Используя интеграцию удаленного репозитория Git, можно управлять иерархией vRealize Orchestrator в нескольких экземплярах vRealize Orchestrator. См. руководство *Использование клиента VMware vRealize Orchestrator*.
- Используя vSphere Web Client, можно запускать рабочие процессы на объектах иерархии vSphere.