

Администрирование vRealize Automation

Октябрь 2022 г.
vRealize Automation 8.7

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

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

© 2022 VMware, Inc. Все права защищены. [Информация об авторских правах и товарных знаках.](#)

Содержание

1	Администрирование vRealize Automation	5
2	Администрирование пользователей	6
	Включение групп Active Directory для проектов	7
	Удаление пользователей из vRealize Automation	8
	Как изменить роли пользователей в vRealize Automation	8
	Как изменить назначения ролей групп в vRealize Automation	9
	Что такое роли пользователей vRealize Automation	10
	Включение уведомления Министерства обороны США и баннера согласия	29
3	Обслуживание устройства	31
	Запуск и остановка vRealize Automation	31
	Горизонтальное масштабирование vRealize Automation с одного узла до трех	33
	Настройка правила разделения и группы виртуальных машин для кластерного экземпляра Workspace ONE Access	34
	Замена узла устройства	35
	Увеличение размера диска устройства vRealize Automation	37
	Обновление назначений DNS для vRealize Automation	37
	Изменение IP-адреса узла или кластера	38
	Включение синхронизации времени	39
	Как сбросить пароль пользователя root	40
4	Использование конфигураций vRealize Automation с несколькими арендаторами	42
	Настройка среды vRealize Automation с несколькими арендаторами	45
	Управление сертификатами и конфигурацией DNS в развертываниях с одним узлом и несколькими арендаторами	47
	Управление сертификатами и конфигурацией DNS в кластерных развертываниях vRealize Automation	49
	Вход в арендаторы и добавление пользователей в vRealize Automation	52
	Использование vRealize Orchestrator в развертываниях vRealize Automation с несколькими организациями	53
5	Работа с журналами	55
	Работа с журналами и наборами журналов	55
	Настройка пересылки журналов в vRealize Log Insight	59
	Создание и обновление интеграции системного журнала	64
	Удаление интеграции системного журнала для ведения журнала	65
	Работа с контент-пакетами	66

6	Участие в программе улучшения качества программного обеспечения	69
	Как присоединиться к программе или выйти из нее	69
	Настройка времени сбора данных для программы	70
7	Включение формы отзыва в продукте	71

Администрирование vRealize Automation

1

В этом руководстве описывается, как отслеживать и контролировать важные аспекты инфраструктуры и управления пользователями в развертывании vRealize Automation.

Задачи, описанные в этом документе, важны для обеспечения надлежащей работы развертывания vRealize Automation. В число этих задач входит управление пользователями и группами и мониторинг системных журналов.

Кроме того, здесь описывается настройка развертываний в нескольких организациях и управление ими.

В то время как некоторые задачи администрирования vRealize Automation выполняются в рамках vRealize Automation, для других требуется использовать связанные продукты, такие как vRealize Suite Lifecycle Manager и Workspace ONE Access. Перед выполнением соответствующих задач пользователи должны ознакомиться с этими продуктами и их возможностями.

Например, сведения о резервном копировании, восстановлении и аварийном восстановлении см. в разделе **Резервное копирование, восстановление и аварийное восстановление > 2019 документации по продукту vRealize Suite**.

Примечание Аварийное восстановление поддерживается в vRealize Automation 8.0.1 и более поздних версиях.

Дополнительные сведения об установке, обновлении vRealize Suite Lifecycle Manager и управлении им см. в документации по продукту [Lifecycle Manager](#).

Администрирование пользователей и групп в vRealize Automation

2

Для импорта пользователей и групп и управления ими vRealize Automation использует VMware Workspace ONE Access — предоставляемое VMware приложение для управления удостоверениями. После импорта или создания пользователей и групп на странице «Управление идентификацией и доступом» можно управлять назначением ролей для развертываний с одним арендатором.

Установка vRealize Automation выполняется с помощью VMware Lifecycle Manager (vRSLCM или LCM). При установке vRealize Automation для управления удостоверениями необходимо импортировать существующий экземпляр Workspace ONE Access или развернуть новый. Эти два сценария определяют варианты управления.

- При развертывании нового экземпляра Workspace ONE Access можно управлять пользователями и группами с помощью LCM. Во время установки можно настроить подключение к Active Directory с помощью Workspace ONE Access. Кроме того, можно просматривать и изменять некоторые параметры пользователей и групп в vRealize Automation на странице «Управление идентификацией и доступом», как описано в этом разделе.
- При использовании существующего экземпляра Workspace ONE Access импортируйте его для использования с vRealize Automation через LCM во время установки. В этом случае можно продолжить управлять пользователями и группами через Workspace ONE Access или использовать функции управления в LCM.

Дополнительные сведения об управлении пользователями в развертывании с несколькими арендаторами см. в разделе [Вход в арендаторы и добавление пользователей в vRealize Automation](#).

Пользователям vRealize Automation должны быть назначены роли. Роли определяют доступ к компонентам приложения. При установке vRealize Automation с экземпляром Workspace ONE Access создается организация по умолчанию, а установившему ее пользователю назначается роль владельца организации. Все остальные роли vRealize Automation назначаются владельцем организации.

В vRealize Automation предусмотрено три типа ролей: роли организации, роли службы и роли проекта. В Cloud Assembly, Service Broker и Code Stream роли уровня пользователя, как правило, предоставляют доступ к ресурсам, а для создания и настройки ресурсов требуются роли уровня администратора. Роли организации определяют разрешения в рамках арендатора. Владелец организации имеет разрешения уровня администратора, а участники организации — уровня пользователя. Владелец организации могут добавлять других пользователей и управлять ими.

Роли организации	Роли служб
■ Владелец организации	■ Администратор Cloud Assembly
■ Участник организации	■ Пользователь Cloud Assembly
	■ Наблюдатель Cloud Assembly
	■ Администратор Service Broker
	■ Пользователь Service Broker
	■ Наблюдатель Service Broker
	■ Администратор Code Stream
	■ Пользователь Code Stream
	■ Обзорщик Code Stream

Кроме того, в таблице не указаны две роли уровня проекта: администратор проекта и пользователь проекта. Эти роли назначаются в индивидуальном порядке для конкретных проектов с помощью Cloud Assembly. Эти роли являются довольно гибкими. Один сотрудник может быть администратором в одном проекте и пользователем в другом. Дополнительные сведения см. в разделе [Что такое роли пользователей vRealize Automation](#).

Дополнительные сведения о работе с vRealize Suite Lifecycle Manager и Workspace ONE Access см. в следующих разделах.

В эту главу входят следующие разделы:

- [Включение групп Active Directory в vRealize Automation для проектов](#)
- [Удаление пользователей из vRealize Automation](#)
- [Как изменить роли пользователей в vRealize Automation](#)
- [Как изменить назначения ролей групп в vRealize Automation](#)
- [Что такое роли пользователей vRealize Automation](#)
- [Включение уведомления Министерства обороны США и баннера согласия](#)

Включение групп Active Directory в vRealize Automation для проектов

Если на странице «Добавление групп» при добавлении пользователей в проекты оказывается, что группа отсутствует, проверьте страницу «Управление идентификацией и доступом» и добавьте группу при ее наличии. Если на странице «Управление Управлением идентификацией и доступом» в vRealize Automation группа отсутствует, ее будет нельзя синхронизировать с экземпляром Workspace ONE Access. Убедитесь, что группа была синхронизировано, а затем используйте следующую процедуру, чтобы добавить группу.

Чтобы добавить в проект участников группы Active Directory, убедитесь, что эта группа синхронизирована с экземпляром Workspace ONE Access и добавлена в организацию.

Необходимые условия

Если группы не синхронизированы, при попытке добавления в проект они будут недоступны. Убедитесь, группы Active Directory синхронизируются с экземпляром Lifecycle Manager.

Процедура

1. Войдите в vRealize Automation в качестве пользователя из того же домена Active Directory, который вы добавляете. Например, @mycompany.com
2. В Cloud Assembly справа на панели навигации заголовка выберите элемент «Управление идентификацией и доступом».
3. Щелкните **Корпоративные группы**, а затем **Назначение ролей**.
4. С помощью функции поиска найдите добавляемую группу и выберите ее.
5. Назначьте роль организации.

Группа должна иметь хотя бы роль «Участник организации». Дополнительные сведения см. в разделе [Что такое роли пользователей Cloud Assembly в vRealize Automation](#).

6. Щелкните **Добавление доступа к службам**, добавьте одну или несколько служб и выберите роль для каждой из них.
7. Нажмите кнопку **Назначить**.

Результаты

Теперь группу Active Directory можно добавить в проект.

Удаление пользователей из vRealize Automation

При необходимости можно удалить пользователей из vRealize Automation.

Все пользователи отображаются по умолчанию, и на странице «Управление идентификацией и доступом» нельзя добавить пользователей. Удалять пользователей можно.

Процедура

1. На странице «Управление идентификацией и доступом» выберите вкладку «Активные пользователи».
2. Найдите и выберите пользователей, которых требуется удалить.
3. Щелкните **Удалить пользователей**.

Результаты

Выбранные пользователи будут удалены.

Как изменить роли пользователей в vRealize Automation

Можно изменять роли, назначенные пользователям Workspace One Access, которые были импортированы в vRealize Automation.

Необходимые условия

Процедура

1. В Cloud Assembly справа на панели навигации заголовка выберите элемент «Управление идентификацией и доступом».
2. Выберите нужного пользователя на вкладке «Активные пользователи» и нажмите **Изменить роли**.
3. Можно изменить организацию и роли службы для пользователя.
 - Щелкните раскрывающееся меню рядом с заголовком «Назначение ролей организации», чтобы изменить связь пользователя с организацией.
 - Нажмите «Добавить доступ к службе», чтобы добавить новые роли службы для пользователя.
 - Чтобы удалить роли пользователей, щелкните X рядом с соответствующей службой.
4. Нажмите **Сохранить**.

Результаты

Назначенные роли пользователя обновлены, как указано.

Как изменить назначения ролей групп в vRealize Automation

Назначения ролей для групп можно изменить в vRealize Automation

Необходимые условия

Пользователи и группы импортированы из допустимого экземпляра vIDM, связанного с развертыванием vRealize Automation.

Процедура

1. В Cloud Assembly справа на панели навигации заголовка выберите элемент «Управление идентификацией и доступом».
2. Выберите вкладку «Корпоративные группы».
3. В поле поиска введите имя группы, для которой необходимо изменить назначения ролей.
4. Измените назначения ролей для выбранной группы. Доступно два варианта.
 - Назначение ролей организации
 - Назначение ролей служб
5. Нажмите кнопку **Назначить**.

Результаты

Назначения ролей обновляются, как указано.

Что такое роли пользователей vRealize Automation

Владелец организации может назначать пользователям роли на уровне организации и служб. Роли определяют, какие действия пользователи могут выполнять и какие данные просматривать. Затем в службах администратор службы может назначать роли на уровне проекта. Чтобы определить, какую роль требуется назначить, ознакомьтесь с задачами, описанными в следующих таблицах.

Роли службы Cloud Assembly

Роли службы Cloud Assembly определяют отображаемое содержимое и доступные действия в Cloud Assembly. Эти роли службы определяются в консоли владельцем организации.

Таблица 2-1. Описание ролей службы Cloud Assembly

Роль	Описание
Администратор Cloud Assembly	Пользователь должен иметь доступ для чтения и записи ко всему пользовательскому интерфейсу и ресурсам API. Это единственная роль пользователя, которая позволяет просматривать и выполнять все действия, в том числе добавлять облачные учетные записи, создавать новые проекты и назначать администратора проекта.
Пользователь Cloud Assembly	Пользователь, у которого нет роли администратора Cloud Assembly. В проекте Cloud Assembly администратор добавляет пользователей в качестве участников, администраторов или обозревателей проекта. Администратор также может добавить администратора проекта.
Наблюдатель Cloud Assembly	Пользователь с правом чтения может просматривать сведения, но не может создавать, обновлять или удалять какие-либо значения. Это роль «только для чтения» для всех проектов. Пользователи с ролью обозревателя могут видеть всю информацию, доступную администратору. Он не может выполнять никакие действия, пока не будет назначен в качестве администратора или участника проекта. Если пользователь связан с проектом, у него есть разрешения, связанные с ролью. Обозреватель проекта не может расширять свои разрешения так же, как администратор или участник.

В дополнение к ролям служб в Cloud Assembly доступны роли проектов. Любой проект доступен во всех службах.

Роли проекта определяются в Cloud Assembly и могут различаться в зависимости от проекта.

В следующих таблицах указаны возможности различных ролей по просмотру и выполнению задач в рамках служб и проектов. Следует помнить, что администраторы служб имеют полный доступ ко всем областям пользовательского интерфейса.

Описание ролей проекта поможет решить, какие разрешения следует предоставить пользователям.

- Администраторы проектов используют инфраструктуру, созданную администратором службы, и обеспечивают наличие ресурсов, необходимых участникам проектов на этапе разработки.

- Участники проектов работают в своих проектах над проектированием и развертыванием облачных шаблонов. В следующей таблице проекты могут включать только ресурсы, которыми вы владеете, или ресурсы, которые используются совместно с другими участниками проекта.
- Обзорщики проекта имеют ограниченный доступ «только чтение», кроме нескольких случаев, когда они могут выполнять неразрушающие операции, такие как загрузка облачных шаблонов.
- Координаторы проекта являются утверждающими в Service Broker для своих проектов, для которых в политике утверждения определено утверждение координатором проекта. Чтобы предоставить координатору контекст для утверждений, можно также назначить ему роль участника или наблюдателя проекта.

Таблица 2-2. Роли служб и проектов Cloud Assembly

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly			
				Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Доступ к Cloud Assembly							
Консоль	Консоль vRA позволяет найти и открыть Cloud Assembly.	Да	Да	Да	Да	Да	Да
Инфраструктура							
	Просмотр и открытие вкладки «Инфраструктура»	Да	Да	Да	Да	Да	Да
Настройка — Проекты	Создание проектов	Да					
	Обновление или удаление значений сводки проекта, параметров предоставления, Kubernetes, интеграций и конфигураций тестовых проектов.	Да					
	Добавление пользователей и групп, назначение ролей в проектах.	Да		Да. Проекты.			
	Просмотр проектов.	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	Да. Проекты

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Настройка — Облачные зоны	Создание, обновление и удаление облачных зон	Да					
	Просмотр облачных зон.	Да	Да				
	Просмотр панели управления «Ключевые сведения» для облачной зоны	Да	Да				
	Просмотр оповещений для облачных зон	Да	Да				
Настройка — зоны Kubernetes	Создание, обновление и удаление зон Kubernetes	Да					
	Просмотр зон Kubernetes	Да	Да				
Настройка — конфигурации ресурсов	Создание, обновление и удаление конфигураций ресурсов	Да					
	Просмотр конфигураций ресурсов	Да	Да				
Настройка — Сопоставления образов	Создание, обновление и удаление сопоставлений образов	Да					
	Просмотр сопоставлений образов	Да	Да				
Настройка — Профили сети	Создание, обновление и удаление профилей сети	Да					

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Просмотр профилей сети образа	Да	Да				
Настройка — Профили хранилища	Создание, обновление и удаление профилей хранилища	Да					
	Просмотр профилей хранилища образа	Да	Да				
Настройка — карточки ценообразования	Создание, обновление и удаление карточек ценообразования	Да					
	Просмотр карточек ценообразования	Да	Да				
Настройка — Теги	Создание, обновление и удаление тегов	Да					
	Просмотр тегов	Да	Да				
Ресурсы — Вычислительные ресурсы	Добавление тегов для обнаруженных вычислительных ресурсов	Да					
	Просмотр обнаруженных вычислительных ресурсов	Да	Да				
Ресурсы — сети	Изменение тегов, диапазонов IP- адресов и IP- адресов сетей	Да					
	Просмотр обнаруженных сетевых ресурсов	Да	Да				

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Ресурсы — безопасность	Добавление тегов к обнаруженным группам безопасности	Да					
	Просмотр обнаруженных групп безопасности	Да	Да				
Ресурсы — Хранилище	Добавление тегов к обнаруженному хранилищу	Да					
	Просмотр хранилища	Да	Да				
Ресурсы — Kubernetes	Развертывание или добавление кластеров Kubernetes, а также создание или добавление пространств имен	Да					
	Просмотр кластеров и пространств имен Kubernetes	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Действия — Запросы	Удаление записей запросов на развертывание	Да					
	Просмотр записей запросов на развертывание	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Действие — журналы событий	Просмотр журналов событий	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Подключения — Облачные учетные записи	Создание, обновление и удаление облачных учетных записей	Да					
	Просмотр облачных учетных записей	Да	Да				

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Подключения — Интеграции	Создание, обновление или удаление интеграций	Да					
	Просмотр интеграций	Да	Да				
Внедрение	Создание, обновление или удаление планов внедрений	Да					
	Просмотр планов внедрений	Да	Да			Да. Проекты	
Расширяемость							
	Просмотр и открытие вкладки «Расширяемость»	Да	Да			Да	
События	Просмотр событий расширяемости	Да	Да				
Подписки	Создание, обновление и удаление подписок на расширяемость	Да					
	Деактивация подписок	Да					
	Просмотр подписок	Да	Да				
Библиотека — темы событий	Просмотр тем событий	Да	Да				
Библиотека — действия	Создание, обновление и удаление действий по расширению	Да					
	Просмотр действий по расширению	Да	Да				

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Библиотека — рабочие процессы	Просмотр рабочих процессов расширяемости	Да	Да				
Действие — запуски действий	Отмена или удаление запусков действий по расширению	Да					
	Просмотр запусков действий по расширению	Да	Да			Да. Проекты	
Действие — запуски рабочих процессов	Просмотр запусков рабочих процессов расширяемости	Да	Да				
Проектирование							
Проектирование	Открытие вкладки «Проектирование»	Да	Да	Да.	Да.	Да.	Да
Облачные шаблоны	Создание, обновление и удаление облачных шаблонов	Да		Да. Проекты	Да. Проекты		
	Просмотр облачных шаблонов	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
	Загрузка облачных шаблонов	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
	Отправка облачных шаблонов	Да		Да. Проекты	Да. Проекты		
	Развертывание облачных шаблонов	Да		Да. Проекты	Да. Проекты		
	Создание версии и восстановление облачных шаблонов	Да		Да. Проекты	Да. Проекты		

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Выпуск облачных шаблонов в каталог	Да		Да. Проекты	Да. Проекты		
Настраиваемые ресурсы	Создание, обновление и удаление настраиваемых ресурсов	Да					
	Просмотр настраиваемых ресурсов	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Настраиваемые действия	Создание, обновление и удаление настраиваемых действий	Да					
	Просмотр настраиваемых действий	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Ресурсы							
	Просмотр и открытие вкладки «Ресурсы»	Да	Да	Да	Да	Да	Да
Развертывания	Просмотр развертываний, включая сведения о развертывании, журнал развертывания, цену, мониторинг, оповещения, оптимизацию и информацию об устранении неполадок	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
	Управление оповещениями	Да		Да. Проекты	Да. Проекты		

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Запуск действий по регулярному обслуживанию в развертываниях на основе политик	Да		Да. Проекты	Да. Проекты		
Ресурсы — Все ресурсы	Просмотр всех обнаруженных ресурсов	Да	Да				
	Выполнение действий по регулярному обслуживанию на обнаруженных ресурсах. Действия доступны только на компьютерах и ограничены включением и выключением для всех компьютеров, а также консолью удаленного доступа для компьютеров vSphere.	Да					
Ресурсы — Все ресурсы	Просмотр развернутых, внедренных и перенесенных ресурсов	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных ресурсах в соответствии с политиками	Да	Да	Да. Проекты.	Да. Проекты.		

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Ресурсы — Виртуальные машины	Просмотр обнаруженных компьютеров	Да	Да				
	Выполнение действий по регулярному обслуживанию на обнаруженных компьютерах. Действия ограничены включением и выключением, а также консолью удаленного доступа для компьютеров vSphere.	Да					
	Создание новой ВМ	Да					
	Просмотр развернутых, внедренных и перенесенных ресурсов.	Да		Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных ресурсах в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Ресурсы — Тома	Просмотр обнаруженных томов	Да	Да				
	Нет доступных действий по регулярному обслуживанию						

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Просмотр развернутых, внедренных и перенесенных томов	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных томах в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Ресурсы — Сети и безопасность	Просмотр обнаруженных сетей, подсистем балансировки нагрузки и групп безопасности	Да	Да				
	Нет доступных действий по регулярному обслуживанию						
	Просмотр развернутых, внедренных и перенесенных сетей, подсистем балансировки нагрузки и групп безопасности	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	

Таблица 2-2. Роли служб и проектов Cloud Assembly (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Cloud Assembly	Наблюдатель Cloud Assembly	Пользователь Cloud Assembly Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором или участником проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Выполнение действий по регулярному обслуживанию с развернутыми, внедренными и перенесенными сетями, подсистемами балансировки нагрузки и группами безопасности в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Оповещения							
	Просмотр и открытие вкладки «Оповещения»	Да	Да	Да	Да	Да	
	Управление оповещениями	Да		Да. Проекты	Да. Проекты		
	Просмотр оповещений	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	

Роли службы Service Broker

Роли службы Service Broker определяют отображаемое содержимое и доступные действия в Service Broker. Эти роли службы определяются в консоли владельцем организации.

Таблица 2-3. Описание ролей службы Service Broker

Роль	Описание
Администратор Service Broker	Должен иметь доступ для чтения и записи ко всему пользовательскому интерфейсу и ресурсам API. Это единственная роль пользователя, которая позволяет выполнять все задачи, в том числе создавать новые проекты и назначать администраторов проектов.
Пользователь Service Broker	Любой пользователь, у которого нет роли администратора Service Broker. В проекте Service Broker администратор добавляет пользователей в качестве участников, администраторов или обозревателей проекта. Администратор также может добавить администратора проекта.
Наблюдатель Service Broker	Пользователь с правом чтения может просматривать сведения, но не может создавать, обновлять или удалять какие-либо значения. Пользователи с ролью обозревателя могут видеть всю информацию, доступную администратору. Он не может выполнять никакие действия, пока не будет назначен в качестве администратора или участника проекта. Если пользователь связан с проектом, у него есть разрешения, связанные с ролью. Обозреватель проекта не может расширять свои разрешения так же, как администратор или участник.

В дополнение к ролям служб в Service Broker доступны роли проектов. Любой проект доступен во всех службах.

Роли проекта определяются в Service Broker и могут различаться в зависимости от проекта.

В следующих таблицах указаны возможности различных ролей по просмотру и выполнению задач в рамках служб и проектов. Следует помнить, что администраторы служб имеют полный доступ ко всем областям пользовательского интерфейса.

Следующее описание ролей проекта поможет решить, какие разрешения следует предоставить пользователям.

- Администраторы проектов используют инфраструктуру, созданную администратором службы, и обеспечивают наличие ресурсов, необходимых участникам проектов на этапе разработки.
- Участники проектов работают в своих проектах над проектированием и развертыванием облачных шаблонов. В следующей таблице проекты могут включать только ресурсы, которыми вы владеете, или ресурсы, которые используются совместно с другими участниками проекта.
- Наблюдатели проекта имеют ограниченный доступ «только чтение».
- Координаторы проекта являются утверждающими в Service Broker для своих проектов, для которых в политике утверждения определено утверждение координатором проекта. Чтобы предоставить координатору контекст для утверждений, можно также назначить ему роль участника или наблюдателя проекта.

Таблица 2-4. Роли службы и роли проектов Service Broker

Контекст пользовательского интерфейса	Задача	Администратор	Наблюдатель	Пользователь Service Broker			
		Service Broker	Service Broker	Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Доступ к Service Broker							
Консоль	Консоль позволяет найти и открыть Service Broker	Да	Да	Да	Да	Да	Да
Инфраструктура							
	Просмотр и открытие вкладки «Инфраструктура»	Да	Да				
Настройка — Проекты	Создание проектов	Да					
	Обновление или удаление значений сводки проекта, параметров предоставления, Kubernetes, интеграций и конфигураций тестовых проектов.	Да					
	Добавление пользователей и групп, назначение ролей в проектах.	Да		Да. Проекты.			
	Просмотр проектов.	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
Настройка — Облачные зоны	Создание, обновление и удаление облачных зон	Да					
	Просмотр облачных зон.	Да	Да				
Настройка — зоны Kubernetes	Создание, обновление и удаление зон Kubernetes	Да					
	Просмотр зон Kubernetes	Да	Да				

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Подключения — Облачные учетные записи	Создание, обновление и удаление облачных учетных записей	Да					
	Просмотр облачных учетных записей	Да	Да				
Подключения — Интеграции	Создание, обновление или удаление интеграций	Да					
	Просмотр интеграций	Да	Да				
Действия — Запросы	Удаление записей запросов на развертывание	Да					
	Просмотр записей запросов на развертывание	Да					
Действие — журналы событий	Просмотр журналов событий	Да					
Содержимое и политики							
	Просмотр и открытие вкладки «Содержимое и политики»	Да	Да				
Источники содержимого	Создание, обновление и удаление источников содержимого	Да					
	Просмотр источников содержимого	Да	Да				
Общий доступ к содержимому	Добавление или удаление общего содержимого	Да					
	Просмотр общего содержимого	Да	Да				

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Содержимое	Настройка форм и настройка элементов	Да					
	Просмотр содержимого	Да	Да				
Политики — определения	Создание, обновление и удаление определений политик	Да					
	Просмотр определений политик	Да	Да				
Политики — применение	Просмотр журнала применения	Да	Да				
Уведомления — почтовый сервер	Настройка почтового сервера	Да					
Каталог							
	Просмотр и открытие вкладки «Каталог»	Да	Да	Да	Да	Да	Да
	Просмотр доступных элементов каталога	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
	Запрос элемента каталога	Да		Да. Проекты	Да. Проекты		
Ресурсы							
	Просмотр и открытие вкладки «Ресурсы»	Да	Да	Да.	Да	Да	Да

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Развертывания	Просмотр развертываний, включая сведения о развертывании, журнал развертывания, цену, мониторинг, оповещения, оптимизацию и информацию об устранении неполадок	Да	Да	Да. Проекты	Да. Проекты	Да. Проекты	
	Управление оповещениями	Да		Да. Проекты	Да. Проекты		
	Запуск действий по регулярному обслуживанию в развертываниях на основе политик	Да		Да. Проекты	Да. Проекты		
Ресурсы — Все ресурсы	Просмотр всех обнаруженных ресурсов	Да	Да				
	Выполнение действий по регулярному обслуживанию на обнаруженных ресурсах. Действия доступны только на компьютерах и ограничены включением и выключением для всех компьютеров, а также консолью удаленного доступа для компьютеров vSphere.	Да					

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
Ресурсы — Все ресурсы	Просмотр развернутых, внедренных и перенесенных ресурсов	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных ресурсах в соответствии с политиками	Да	Да	Да. Проекты.	Да. Проекты.		
Ресурсы — Виртуальные машины	Просмотр обнаруженных компьютеров	Да	Да				
	Выполнение действий по регулярному обслуживанию на обнаруженных компьютерах. Действия ограничены включением и выключением, а также консолью удаленного доступа для компьютеров vSphere.	Да					
	Создание новой VM	Да					
	Просмотр развернутых, внедренных и перенесенных ресурсов.	Да		Да. Проекты.	Да. Проекты.	Да. Проекты.	

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных ресурсах в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Ресурсы — Тома	Просмотр обнаруженных томов	Да	Да				
	Нет доступных действий по регулярному обслуживанию						
	Просмотр развернутых, внедренных и перенесенных томов	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию на развернутых, внедренных и перенесенных томах в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Ресурсы — Сети и безопасность	Просмотр обнаруженных сетей, подсистем балансировки нагрузки и групп безопасности	Да	Да				
	Нет доступных действий по регулярному обслуживанию						

Таблица 2-4. Роли службы и роли проектов Service Broker (продолжение)

Контекст пользовательского интерфейса	Задача	Администратор Service Broker	Наблюдатель Service Broker	Пользователь Service Broker Для просмотра и выполнения задач, связанных с проектом, пользователь должен быть администратором проекта.			
				Администратор проекта	Участник проекта	Наблюдатель проекта	Координатор проекта
	Просмотр развернутых, внедренных и перенесенных сетей, подсистем балансировки нагрузки и групп безопасности	Да	Да	Да. Проекты.	Да. Проекты.	Да. Проекты.	
	Выполнение действий по регулярному обслуживанию с развернутыми, внедренными и перенесенными сетями, подсистемами балансировки нагрузки и группами безопасности в соответствии с политиками	Да		Да. Проекты.	Да. Проекты.		
Подтверждения							
	Просмотр и открытие вкладки «Подтверждения»	Да	Да	Да	Да	Да	Да
	Ответ на запросы подтверждения	Да		Да. Утверждающим проектов и политик является администратор проекта	Только назначенные утверждающие	Только назначенные утверждающие	Да. Утверждающим проектов и политик является координатор проекта

Включение уведомления Министерства обороны США и баннера согласия

Для некоторых государственных заказчиков администратор должен настроить стандартное уведомление Министерства обороны США (DoD) и баннер согласия в Workspace ONE Access, чтобы пользователи имели доступ к vRealize Automation.

Стандартное обязательное уведомление DoD и баннер согласия содержат следующий текст.

Вы получаете доступ к информационной системе (ИС) правительства США (USG), которая предоставляется только при наличии разрешения USG. Используя данную ИС (включая любые устройства, подключенные к этой ИС), вы соглашаетесь на следующие условия:

- USG в рабочем порядке перехватывает и отслеживает сеансы связи с этой ИС для целей, включая, среди прочего, тестирование на возможность проникновения, мониторинг COMSEC, анализ сетевых операций и защиты сети, неправомерных действий персонала (PM), охранно-розыскных мероприятий (LE) и защиты от средств разведки (CI).
- USG в любое время может инспектировать и изымать данные, хранящиеся в данной ИС.
- Сеансы связи с использованием настоящей ИС или данные, хранящиеся в ней, не являются частными, подлежат регламентному мониторингу, перехвату и поиску, и могут быть разглашены или использованы для любых целей с разрешения USG.

Ниже приведена процедура настройки этого баннера в Workspace ONE Access. Дополнительные сведения см. в документации по консоли администрирования для Workspace ONE Access.

Процедура

1. Войдите в консоль администрирования Workspace ONE в качестве администратора.
2. На консоли VMware Identity Manager перейдите на вкладку «Управление идентификацией и доступом».
3. Щелкните «Настроить», а затем перейдите на вкладку «Соединители».
4. Щелкните ссылку «Рабочий процесс» для каждого соединителя, который необходимо настроить.
5. Перейдите на вкладку «Адаптеры проверки подлинности», а затем щелкните CertificateAuthAdapter.
6. Установите флажок «Включить форму выражения согласия перед проверкой подлинности».
7. Вставьте текст стандартного обязательного уведомления DoD и баннера согласия в окно «Содержимое формы выражения согласия».
8. Сохраните изменения.

Результаты

Обслуживание устройства vRealize Automation

3

Чтобы обеспечить надлежащую работу установленного приложения vRealize Automation, системному администратору может потребоваться выполнять различные задачи.

Если вы только начинаете работу с vRealize Automation, эти задачи не являются обязательными. Знать процедуру выполнения этих задач полезно на тот случай, если потребуется устранить проблемы, связанные с производительностью или особенностями работы продукта.

В эту главу входят следующие разделы:

- [Запуск и остановка vRealize Automation](#)
- [Горизонтальное масштабирование vRealize Automation с одного узла до трех](#)
- [Настройка правила разделения и группы виртуальных машин для кластерного экземпляра Workspace ONE Access](#)
- [Замена узла устройства vRealize Automation](#)
- [Увеличение размера диска устройства vRealize Automation](#)
- [Обновление назначений DNS для vRealize Automation](#)
- [Изменение IP-адресов узла или кластера vRealize Automation](#)
- [Включение синхронизации времени для vRealize Automation](#)
- [Как сбросить пароль пользователя root для vRealize Automation](#)

Запуск и остановка vRealize Automation

При запуске или завершении работы vRealize Automation необходимо соблюдать соответствующие процедуры.

Рекомендуемый способ выключения и запуска компонентов vRealize Automation — с помощью функций «Выключить» и «Включить» в меню **Lifecycle Operations > Среды** продукта vRealize Suite Lifecycle Manager. В следующих процедурах описаны ручные способы выключения и включения компонентов vRealize Automation, когда vRealize Suite Lifecycle Manager по какой-либо причине недоступен.

Завершение работы vRealize Automation

Чтобы сохранить целостность данных, перед выключением питания виртуальных устройств необходимо завершить работу служб vRealize Automation. С помощью SSH или VMRC можно выключить или включить все узлы с любого устройства.

Примечание По возможности старайтесь не использовать команды `vracli reset vidm`. Эта команда сбрасывает все настройки Workspace ONE Access и разрывает связь между пользователями и подготовленными ресурсами.

1. Войдите в консоль любого устройства vRealize Automation, используя протокол SSH или VMRC.
2. Чтобы завершить работу служб vRealize Automation на всех узлах кластера, выполните следующий набор команд.

Примечание Если после копирования одной из этих команд ее выполнение завершается сбоем, сначала вставьте ее в блокнот, а затем скопируйте оттуда и запустите. Эта процедура позволяет убрать все скрытые символы и другие артефакты, которые могут присутствовать в исходной документации.

```
/opt/scripts/deploy.sh --shutdown
```

3. Завершите работу устройств vRealize Automation.

Теперь развертывание vRealize Automation выключено.

Запустите vRealize Automation

После незапланированного завершения работы, управляемого завершения работы или процедуры восстановления необходимо перезапустить компоненты vRealize Automation в определенном порядке. Компонент vRLCM не является критическим, поэтому его можно запустить в любое время. Компоненты VMware Workspace ONE Access (предыдущее название VMware Identity Management) должны быть запущены перед запуском vRealize Automation.

Примечание Перед запуском компонентов vRealize Automation убедитесь, что запущены соответствующие подсистемы балансировки нагрузки.

1. Включите питание всех устройств vRealize Automation и дождитесь их запуска.
2. Войдите в консоль любого устройства, используя протокол SSH или VMRC, и выполните следующую команду, чтобы восстановить службы на всех узлах.

```
/opt/scripts/deploy.sh
```

3. Убедитесь, что все службы запущены, выполнив следующую команду.

```
kubectl get pods --all-namespaces
```

Примечание Должны отображаться три экземпляра каждой службы с состоянием «Выполняется» или «Завершено».

Если все службы имеют состояние «Выполняется» или «Завершено», система vRealize Automation готова к использованию.

Перезапуск vRealize Automation

Все службы vRealize Automation можно централизованно перезапустить с любого устройства в кластере. Следуйте указанным выше инструкциям, чтобы завершить работу vRealize Automation, а затем выполните инструкции для запуска vRealize Automation. Перед перезагрузкой vRealize Automation убедитесь, что запущены все применимые подсистемы балансировки нагрузки и компоненты VMware Workspace ONE Access.

Если все службы имеют состояние «Выполняется» или «Завершено», система vRealize Automation готова к использованию.

Выполните следующую команду, чтобы убедиться, что все службы запущены.

```
kubectl -n prelude get pods
```

Горизонтальное масштабирование vRealize Automation с одного узла до трех

По мере необходимости развертывание vRealize Automation можно горизонтально масштабировать с одного узла до трех.

Для выполнения этой процедуры необходимо использовать vRealize Suite Lifecycle Manager. Дополнительные сведения об установке, обновлении vRealize Suite Lifecycle Manager и управлении им см. в [документации по продукту Lifecycle Manager](#).

При использовании кластерного развертывания с тремя узлами служба vRealize Automation может, как правило, выдерживать сбой одного узла и продолжать нормально функционировать. В случае сбоя двух узлов в кластере с тремя узлами служба vRealize Automation будет неработоспособна.

Необходимые условия

В этой процедуре предполагается, что у вас уже есть работающее развертывание vRealize Automation с одним узлом.

Процедура

1. Завершите работу всех устройств vRealize Automation.

Чтобы завершить работу служб vRealize Automation на всех узлах кластера, выполните следующий набор команд.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

Теперь можно завершить работу устройств vRealize Automation.

2. Сделайте моментальный снимок развертывания.

Используйте параметр «Создать моментальный снимок» в меню vRealize Suite Lifecycle Manager **Операции жизненного цикла > Среды > vRA > Просмотреть сведения**.

Примечание Моментальные снимки по сети без отключения узлов vRealize Automation можно делать начиная с версии 8.0.1. В среде vRealize Automation 8.0 сначала необходимо остановить узлы vRealize Automation.

3. Включите устройство vRealize Automation и активируйте все контейнеры.
4. С помощью функции Locker в меню **LCM > Locker > Сертификаты** в vRealize Suite Lifecycle Manager создайте или импортируйте сертификаты vRealize Automation для всех компонентов, в том числе полные доменные имена (FQDN) узлов vRealize Suite Lifecycle Manager и полное доменное имя подсистемы балансировки нагрузки vRealize Automation.

Добавьте имена всех трех устройств в альтернативные имена субъектов.
5. Импортируйте новый сертификат в vRealize Suite Lifecycle Manager.
6. Замените существующий сертификат vRealize Suite Lifecycle Manager, созданный на предыдущем шаге, в меню **LCM Операции жизненного цикла > Среды > vRA > Просмотреть сведения** Заменить сертификат.
7. Выполните горизонтальное масштабирование vRealize Automation до трех узлов с помощью параметра «Добавить компоненты» в меню **LCM > Операции жизненного цикла > Среды > vRA > Просмотреть сведения**.

Результаты

Для vRealize Automation выполнено масштабирование до развертывания с тремя узлами.

Настройка правила разделения и группы виртуальных машин для кластерного экземпляра Workspace ONE Access

Если в среде vRealize Automation используется кластерный экземпляр Workspace ONE Access, создайте правило разделения и кластер компьютеров, чтобы обеспечить надлежащий рабочий процесс обеспечения высокой доступности vSphere.

Чтобы защитить любые кластерные узлы Workspace ONE Access от сбоя на уровне узла, настройте правило разделения для запуска виртуальных машин, которые существуют на разных узлах в кластере управления vSphere. После создания правила разделения настройте группу виртуальных машин, чтобы определить необходимый порядок запуска компьютеров. Благодаря использованию заданного порядка запуска компьютеров можно гарантировать, что функция обеспечения высокой доступности vSphere будет включать питание на кластерных узлах Workspace ONE Access в требуемом порядке для вашей среды.

Дополнительные сведения о настройке правил разделения и группы виртуальных машин см. в разделе [Настройка правила разделения и группы виртуальных машин для кластерного экземпляра Workspace ONE Access](#) в документации по продукту VMware Cloud Foundation.

Особенности правил разделения при переходе с одной версии vRealize Automation на другую

vRealize Suite Lifecycle Manager не поддерживает правила разделения для vRealize Automation 8.x. Так как во время обновления vRealize Automation служба vRealize Suite Lifecycle Manager используется продуктом vRealize Easy Installer и нет заданного порядка выключения и включения питания для узлов vRealize Automation во время обновления, могут возникать проблемы, если применяемый порядок конфликтует с правилами сходства, которые определяют порядок выключения и включения питания для компьютеров. При использовании vRealize Suite Lifecycle Manager или vRealize Easy Installer для обновления с одной версии vRealize Automation на другую перед началом обновления отключите правила сходства.

Дополнительные сведения об обновлении с одной версии vRealize Automation на другую см. в разделе [Установка vRealize Automation с помощью vRealize Easy Installer](#) в документации по продукту vRealize Automation.

Замена узла устройства vRealize Automation

Если в устройстве vRealize Automation, которое находится в конфигурации «несколько узлов, высокая доступность (HA)» происходит отказ, может потребоваться замена неисправного узла.

Осторожно! Прежде чем продолжить, компания VMware рекомендует обратиться в службу технической поддержки, попросить устранить проблему с HA и убедиться, что неисправен только один узел.

Если техническая поддержка решит, что узел необходимо заменить, выполните следующие действия.

1. В vCenter создайте моментальные снимки для резервного копирования каждого устройства в конфигурации HA.

Не включайте в эти моментальные снимки для резервного копирования память виртуальной машины.

2. Завершите работу неисправного узла.
3. Запишите номер сборки программного обеспечения неисправного узла vRealize Automation и параметры сети.

Запишите полное доменное имя, IP-адрес, шлюз, DNS-серверы и обязательно MAC-адрес. В дальнейшем эти значения нужно будет назначить сменному узлу.

4. Основной узел базы данных должен быть исправен. Выполните следующие действия.

- а) Войдите в командную строку исправного узла как пользователь root.
- б) Определите имя основного узла базы данных с помощью следующей команды.

```
vracli status | grep primary -B 1
```

Результат должен быть похож на следующий пример, где `postgres-1` — основной узел базы данных.

```
"Conninfo":
"host=postgres-1.postgres.prelude.svc.cluster.local
dbname=repmgr-db user=repmgr-db passfile=/scratch/repmgr-db.cred
connect_timeout=10",
"Role": "primary",
```

- в) Убедитесь, что основной узел базы данных исправен, выполнив следующую команду.

```
kubectl -n prelude get pods -o wide | grep postgres
```

Результат должен быть похож на следующий пример, где `postgres-1` указан в списке как работающий и исправный.

```
postgres-1 1/1 Running 0 39h 12.123.2.14 vc-vm-224-84.company.com <none> <none>
postgres-2 1/1 Running 0 39h 12.123.1.14 vc-vm-224-85.company.com <none> <none>
```

Важно! Если основной узел базы данных неисправен, обратитесь в службу технической поддержки перед продолжением процедуры.

- Используя командную строку исправного узла с правами пользователя `root`, удалите неисправный узел.

```
vraccli cluster remove полное-доменное-имя-неисправного-узла
```

- Используйте vCenter для развертывания нового сменного узла vRealize Automation.

Разверните тот же номер сборки программного обеспечения vRealize Automation и примените параметры сети из неисправного узла. Введите полное доменное имя, IP-адрес, шлюз, DNS-серверы и обязательно MAC-адрес, записанные ранее.

- Включите сменный узел.
- Войдите в командную строку сменного узла как пользователь `root`.
- Убедитесь, что процесс начальной загрузки завершен, с помощью следующей команды.

```
vraccli status first-boot
```

Найдите сообщение `First boot complete`.

- На сменном узле присоединитесь к кластеру vRealize Automation.

```
vraccli cluster join полное-доменное-имя-узла-основной-БД
```

- Войдите в командную строку основного узла базы данных как пользователь `root`.
- Разверните восстановленный кластер с помощью следующего сценария.

```
/opt/scripts/deploy.sh
```

Увеличение размера диска устройства vRealize Automation

Может возникнуть необходимость увеличить размер диска устройства vRealize Automation, например, для хранилища файлов журнала.

Процедура

1. Для расширения VMDK-диска на устройстве vRealize Automation используйте vSphere.
2. Войдите в командную строку устройства vRealize Automation как пользователь root.
3. В командной строке выполните следующую команду vRealize Automation:

```
vracli disk-mgr resize
```

Если изменить размер vRealize Automation не удалось, см. [статью базы знаний 79925](#).

Обновление назначений DNS для vRealize Automation

Администратор может обновить назначения DNS для vRealize Automation.

Процедура

1. Войдите в консоль любого устройства vRealize Automation, используя протокол SSH или VMRC.
2. Выполните следующую команду.

```
vracli network dns set --servers DNS1,DNS2
```

3. Убедитесь, что команда `vracli network dns status` правильно применила новые DNS-серверы ко всем узлам vRealize Automation.
4. Запустите следующий набор команд для завершения работы служб vRealize Automation на всех узлах кластера.

```
/opt/scripts/svc-stop.sh
sleep 120
/opt/scripts/deploy.sh --onlyClean
```

5. Перезапустите узлы vRealize Automation и дождитесь их полного запуска.
6. Войдите в каждый узел vRealize Automation с помощью SSH и убедитесь, что новые DNS-серверы перечислены в файле `/etc/resolv.conf`.
7. В одном из узлов vRealize Automation выполните следующую команду, чтобы запустить службы vRealize Automation: `/opt/scripts/deploy.sh`

Результаты

Параметры DNS в vRealize Automation изменяются указанным образом.

Изменение IP-адресов узла или кластера vRealize Automation

IP-адрес узла или кластера vRealize Automation можно изменить.

Это может потребоваться, чтобы, например, перенести развернутую среду vRealize Automation в более подходящий vCenter или обеспечить аварийное переключение vRealize Automation.

Администратор vRealize Automation может использовать следующую процедуру, чтобы задать новый IP-адрес для узла или кластера vRealize Automation, а затем повторно выполнить развертывание служб с новым IP-адресом.

Примечание Перед изменением IP-адреса узла или кластера vRealize Automation необходимо убедиться, что они находятся в работоспособном состоянии. Если выполнить эту процедуру на неработающем узле или кластере, это может привести к проблемам, которые будет очень трудно решить.

Эта процедура подразумевает перезапуск vRealize Automation в четко обозначенном порядке. Дополнительные сведения о том, как завершить работу и перезапустить vRealize Automation, см. в разделе [Запуск и остановка vRealize Automation](#).

1. С помощью следующей команды убедитесь, что узел или кластер vRealize Automation находится в работоспособном состоянии.

```
vracli service status
```

2. Если vRealize Automation работает, задайте альтернативный IP-адрес устройств (-a) узла или кластера с помощью следующей команды.

```
vracli network alternative-ip set --dns DNSIPAddress1,DNSIPAddress2 IPV4_address  
Gateway_IPV4_address
```

При работе с кластером задайте альтернативный IP-адрес каждого узла в кластере, на который распространяется процедура.

3. Завершите работу служб с помощью следующей команды.

```
/opt/scripts/deploy.sh -shutdown
```

4. При необходимости выполните аварийное переключение или миграцию vRealize Automation. Изучите информацию о [VMware Site Recovery Manager](#), а также внутренние процедуры вашей компании.

5. Измените IP-адрес vRealize Automation с помощью следующей команды.

```
vracli network alternative-ip swap
```

При использовании кластера vRealize Automation необходимо изменить IP-адрес каждого узла в кластере.

6. Перезагрузите службы vRealize Automation, выполнив следующую команду.

```
shutdown -r now
```

При использовании кластера vRealize Automation необходимо перезагрузить каждый узел в кластере.

7. Повторно разверните службы vRealize Automation, выполнив следующую команду.

```
/opt/scripts/deploy.sh
```

После перезагрузки vRealize Automation и запуска повторно развернутых служб vRealize Automation будут доступны по новому IP-адресу.

Включение синхронизации времени для vRealize Automation

Синхронизацию времени в развертывании vRealize Automation можно включить с помощью командной строки устройства vRealize Automation.

Синхронизацию времени можно настроить для автономного или кластерного развертывания vRealize Automation с помощью протокола NTP (Network Time Protocol). vRealize Automation поддерживает две взаимоисключающие конфигурации NTP.

Конфигурация NTP	Описание
ESXi	<p>Эту конфигурацию можно использовать, если сервер ESXi, на котором размещен vRealize Automation, синхронизируется с сервером NTP. В кластерном развертывании все узлы ESXi должны быть синхронизированы с сервером NTP. Дополнительные сведения о настройке NTP для ESXi см. в статье базы знаний 57147: настройка протокола NTP (Network Time Protocol) на узле ESXi с помощью vSphere Web Client.</p> <p>Примечание В случае переноса развертывания vRealize Automation на узел ESXi, который не синхронизирован с сервером NTP, может возникнуть рассинхронизация времени.</p>
systemd	<p>В этой конфигурации для синхронизации часов развертывания vRealize Automation используется управляющая программа systemd-timesyncd.</p> <p>Примечание По умолчанию управляющая программа systemd-timesyncd включена, но настроена без серверов NTP. Если устройство vRealize Automation имеет динамическую конфигурацию IP-адресов, оно может использовать любые серверы NTP, полученные протоколом DHCP.</p>

Процедура

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.

2. Включите NTP с ESXi.

- а) Выполните команду `vraccli ntp esxi`.
- б) (дополнительно) Чтобы подтвердить состояние конфигурации NTP, выполните команду `vraccli ntp status`.

Можно также восстановить конфигурацию NTP до состояния по умолчанию, выполнив команду `vraccli ntp reset`.

3. Включите NTP с systemd.

- а) Выполните команду `vraccli ntp systemd --set FQDN_or_IP_of_systemd_server`.

Примечание Можно добавить несколько серверов NTP systemd, разделяя их сетевые адреса запятыми. Каждый сетевой адрес должен быть заключен в одиночные кавычки. Например, `vraccli ntp systemd --set 'адрес_NTP_1','адрес_NTP_2'`

- б) (дополнительно) Чтобы подтвердить состояние конфигурации NTP, выполните команду `vraccli ntp status`.

Результаты

Синхронизация времени для развертывания устройства vRealize Automation включена.

Следующие шаги

Настройка NTP может завершиться сбоем, если разница во времени между сервером NTP и развертыванием vRealize Automation превышает 10 минут. Чтобы устранить эту проблему, перезагрузите устройство vRealize Automation.

Как сбросить пароль пользователя root для vRealize Automation

Утерянный или забытый пароль пользователя root vRealize Automation можно сбросить.

В этой процедуре для сброса пароля пользователя root vRealize Automation данной организации используется окно командной строки на устройстве vCenter узла.

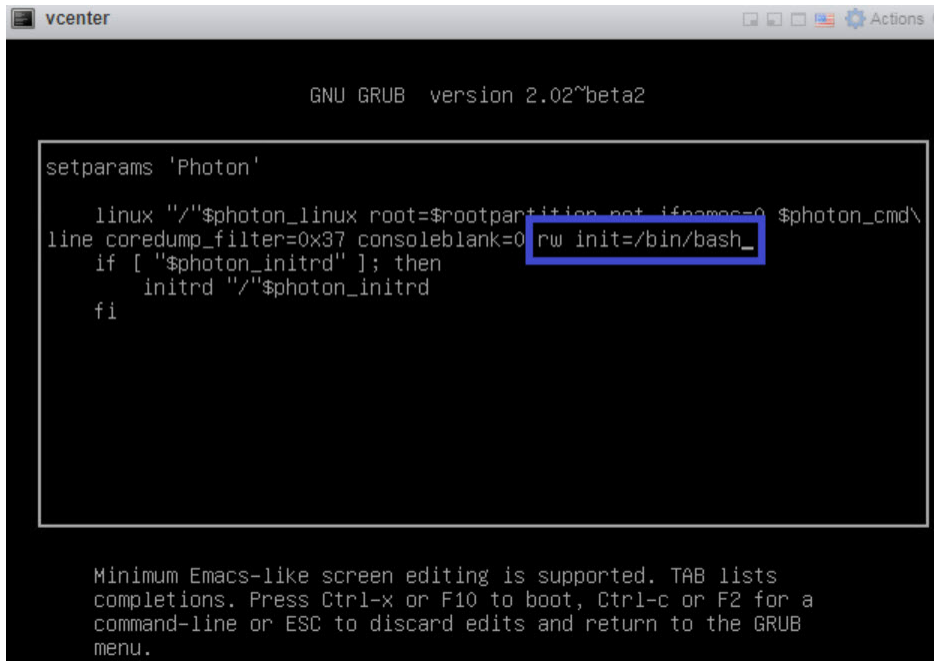
Необходимые условия

Этот процесс предназначен для администраторов vRealize Automation и требует ввода учетных данных, необходимых для доступа к устройству vCenter узла.

Процедура

1. Завершите работу и выполните запуск vRealize Automation с помощью процедуры, описанной в разделе [Запуск и остановка vRealize Automation](#).
2. Когда появится окно командной строки операционной системы Photon, введите `e` и нажмите клавишу **Ввод**, чтобы открыть редактор меню загрузки GNU GRUB.

- В редакторе GNU GRUB введите `rw init=/bin/bash` в конце строки, которая начинается с `linux "/"` `$photon_linux root=rootpartition`, как показано ниже.



- Нажмите клавишу **F10**, чтобы отправить изменения и перезапустить vRealize Automation.
- Дождитесь перезапуска vRealize Automation.
- В командной строке `root [/]#` введите `passwd` и нажмите клавишу **Ввод**.
- В командной строке `New password:` введите новый пароль и нажмите клавишу **Ввод**.
- В командной строке `Retype new password:` повторно введите новый пароль и нажмите клавишу **Ввод**.
- В командной строке `root [/]#` введите `reboot -f` и нажмите клавишу **Ввод**, чтобы завершить процесс сброса пароля пользователя `root`.

```

root [/]# passwd
New password:
Retype new password:
passwd: password updated successfully
root [/]# reboot -f_

```

Следующие шаги

Администратор vRealize Automation теперь может войти в vRealize Automation с новым паролем пользователя `root`.

Использование конфигураций vRealize Automation с несколькими арендаторами

4

vRealize Automation позволяет ИТ-поставщикам настроить несколько арендаторов (или организаций) в каждом развертывании. Поставщики могут настроить несколько организаций-арендаторов и выделить инфраструктуру в каждом развертывании. Поставщики также могут управлять пользователями для арендаторов. Каждый арендатор управляет собственными проектами, ресурсами и развертываниями.

В конфигурации vRealize Automation с несколькими арендаторами поставщики могут создать несколько организаций, причем каждая организация-арендатор будет использовать собственные проекты, ресурсы и развертывания. Хотя поставщики не могут управлять инфраструктурой арендаторов удаленно, они могут входить в систему арендаторов и управлять инфраструктурой из них.

Для множественной аренды требуется скоординировать и настроить три продукта VMware, как описано ниже.

- Workspace ONE Access обеспечивает поддержку инфраструктуры для множественной аренды и подключения к доменам Active Directory, которые позволяют управлять пользователями и группами в организациях-арендаторах.
- vRealize Suite Lifecycle Manager поддерживает создание и настройку арендаторов для поддерживаемых продуктов, таких как vRealize Automation. Кроме того, он предоставляет ряд возможностей управления сертификатами.
- vRealize Automation. Поставщики и пользователи заходят в vRealize Automation, чтобы получить доступ к арендаторам, в которых они создают развертывания и управляют ими.

Для настройки множественной аренды пользователям необходимо ознакомиться со всеми тремя этими продуктами и соответствующей документацией.

Дополнительные сведения о работе с vRealize Suite Lifecycle Manager и Workspace ONE Access см. в следующих разделах.

- vRealize Suite Lifecycle Manager — см. [документацию по системе Lifecycle Manager](#)
- Workspace ONE Access — см. [Управление пользователями с помощью VMware Identity Manager](#) и [Администрирование VMware Workspace ONE Access](#)

Администраторы с разрешениями vRealize Suite Lifecycle Manager создают арендаторов и управляют ими в Lifecycle Manager на странице «Арендаторы», расположенной в службе «Управление удостоверениями и арендаторами». Арендаторы создаются с помощью LDAP- или IWA-подключения к Active Directory и поддерживаются связанным экземпляром VMware Workspace ONE Access, необходимым для развертываний vRealize Automation. Дополнительные сведения об использовании Lifecycle Manager см. в сопутствующей документации.

Настройку множественной аренды необходимо начинать с основного, или главного, арендатора. Этот арендатор является арендатором по умолчанию, который создается при развертывании соответствующего приложения Workspace ONE Access. Другие арендаторы, или субарендаторы, могут быть созданы на основе главного арендатора. На данный момент vRealize Automation поддерживает до 20 организаций-арендаторов в рамках стандартного развертывания с тремя узлами.

Перед активацией vRealize Automation в режиме множественной аренды сначала необходимо установить приложение в конфигурации с одной организацией. Затем используйте Lifecycle Manager для создания конфигурации с несколькими организациями. Развертывание Workspace ONE Access поддерживает управление арендаторами и связанными подключениями к доменам Active Directory.

При первоначальной настройке множественной аренды администратор поставщика указывается в Lifecycle Manager. При необходимости это назначение можно изменить или добавить администраторов позже. В конфигурациях с несколькими организациями для управления пользователями и группами vRealize Automation в основном применяется Workspace ONE Access.

После создания организаций уполномоченные пользователи могут войти в свои приложения, чтобы создавать проекты и ресурсы или работать с ними, а также чтобы создавать развертывания. Администраторы могут управлять ролями пользователей в vRealize Automation.

Настройка для конфигурации с несколькими организациями

Включить развертывание с несколькими организациями можно после завершения установки vRealize Automation. При настройке конфигурации с несколькими организациями необходимо настроить внешний экземпляр Workspace ONE Access для использования множественной аренды, а затем использовать Lifecycle Manager для создания и настройки арендаторов. Это относится как к новым, так и к существующим развертываниям. На начальном этапе настройки арендаторов необходимо через Lifecycle Manager задать псевдоним для главного арендатора, который был создан по умолчанию в Workspace ONE Access. Субарендаторы, создаваемые на основе главного арендатора, наследуют конфигурации доменов Active Directory этого главного арендатора.

В Lifecycle Manager арендаторы присваиваются продукту, например vRealize Automation, и определенной среде. При настройке арендатора необходимо также назначить его администратора. По умолчанию функция множественной аренды включается на уровне имени узла арендатора. Пользователи могут выбрать ручную настройку имени арендатора по имени DNS. Во время этой процедуры необходимо установить несколько флажков для поддержки множественной аренды, а также настроить подсистему балансировки нагрузки.

При использовании кластерного экземпляра имени узлов Workspace ONE Access и vRealize Automation на основе арендаторов будут указывать на подсистему балансировки нагрузки.

Если кластерные подсистемы балансировки нагрузки vRealize Automation и Workspace ONE Access не используют сертификаты с подстановочными знаками, пользователям необходимо указать в сертификатах имена узлов арендаторов в виде записей SAN для каждого создаваемого арендатора.

В vRealize Automation и Lifecycle Manager нельзя удалить арендаторов. Если требуется добавить арендаторов в существующее развертывание с множественной арендой, это можно сделать с помощью Lifecycle Manager, при этом простой составит от трех до четырех часов.

Чтобы узнать больше о vRealize Suite Lifecycle Manager Workspace ONE Access, используйте ссылки на документы в начале этого раздела.

Имена узлов и множественная аренда

В предыдущих версиях vRealize Automation пользователи получали доступ к арендаторам с помощью URL-адресов, составленных на основе пути к каталогу. В текущей реализации множественной аренды пользователи получают доступ к арендаторам по имени узла.

Кроме того, формат имени узла для доступа пользователей vRealize Automation к арендаторам отличается от формата, который используется для доступа к арендаторам в Workspace ONE Access. Например, допустимым именем узла является `tenant1.example.eng.vmware.com`, а не `vidm-node1.eng.vmware.com`.

Множественная аренда и сертификаты

Необходимо создать сертификаты для всех компонентов, задействованных в конфигурации с несколькими организациями. Для Workspace ONE Access, Lifecycle Manager и vRealize Automation потребуется один сертификат или несколько, в зависимости от того, какая конфигурация используется — с одним узлом или кластерная.

При настройке сертификатов можно использовать подстановочные знаки с именами SAN или выделенные имена. Использование подстановочных знаков упрощает управление сертификатами, так как сертификаты должны обновляться при добавлении новых арендаторов. Если в подсистеме балансировки нагрузки vRealize Automation и Workspace ONE Access не используются сертификаты с подстановочными знаками, имена узлов должны быть добавлены в сертификаты как записи SAN для каждого нового создаваемого арендатора. Кроме того, при использовании SAN сертификаты необходимо обновлять вручную при добавлении и удалении узлов или изменении имен узлов. Кроме того, необходимо обновить записи DNS для арендаторов.

Обратите внимание, что Lifecycle Manager не создает отдельные сертификаты для каждого арендатора. Вместо этого создается единый сертификат с указанием имен всех узлов арендаторов. В базовых конфигурациях для CNAME арендатора используется следующий формат: `имя_арендатора.vrahostname.domain`. В конфигурациях с высокой доступностью для имени используется следующий формат: `имя_арендатора.vraLBhostname.domain`.

Если используется кластерная конфигурация Workspace ONE Access, Lifecycle Manager не сможет обновить сертификат подсистемы балансировки нагрузки, поэтому его необходимо обновить вручную. Кроме того, если необходимо повторно зарегистрировать продукты или службы, которые являются внешними по отношению к Lifecycle Manager, этот процесс выполняется вручную.

В эту главу входят следующие разделы:

- [Настройка среды vRealize Automation с несколькими арендаторами](#)
- [Вход в арендаторы и добавление пользователей в vRealize Automation](#)
- [Использование vRealize Orchestrator в развертываниях vRealize Automation с несколькими организациями](#)

Настройка среды vRealize Automation с несколькими арендаторами

Среду vRealize Automation с несколькими арендаторами можно настроить с помощью vRealize Suite Lifecycle Manager.

Ниже приведено высокоуровневое описание процедуры настройки множественной аренды для vRealize Automation, включая настройку DNS и сертификатов. Основное внимание в ней уделено развертыванию на одном узле, при этом есть примечания для кластерной конфигурации.

Дополнительные сведения и видеодемонстрация настройки конфигурации vRealize Automation с несколькими арендаторами см. в разделе <https://vmwarelab.org/2020/04/14/vrealize-automation-8-1-multi-tenancy-setup-with-vrealize-suite-lifecycle-manager-8-1/>.

Необходимые условия

- Установите и настройте Workspace ONE Access версии 3.3.4 или более поздней.
- Установите и настройте vRealize Suite Lifecycle Manager версии 8.5.

Процедура

1. Создайте необходимые записи DNS типов A и CNAME.
 - Для главного арендатора и субарендаторов необходимо создать и применить сертификат SAN.
 - Для развертываний с одним узлом полное доменное имя vRealize Automation указывает на устройство vRealize Automation, а полное доменное имя Workspace ONE Access указывает на устройство Workspace ONE Access.
 - Для кластерных развертываний полные доменные имена на основе арендаторов Workspace ONE Access и vRealize Automation должны указывать на соответствующие подсистемы балансировки нагрузки. Служба Workspace ONE Access настроена в режиме прерывания SSL, поэтому сертификат применяется как к кластеру, так и к подсистеме балансировки нагрузки Workspace ONE Access. Подсистема балансировки нагрузки vRealize Automation использует транзитный режим SSL, поэтому сертификат применяется только в кластере vRealize Automation.

Дополнительные сведения см. в разделах [Управление сертификатами и конфигурацией DNS в развертываниях с одним узлом и несколькими арендаторами](#) и [Управление сертификатами и конфигурацией DNS в кластерных развертываниях vRealize Automation](#).

2. Создайте или импортируйте необходимые сертификаты для нескольких доменов (SAN) для Workspace ONE Access и vRealize Automation.

Сертификаты можно создавать в Lifecycle Manager используя службу Locker, которая позволяет создавать лицензии, сертификаты и пароли. Кроме того, для создания сертификатов можно использовать сервер центра сертификации (CA) или другой механизм.

Если необходимо добавить или создать дополнительных арендаторов, необходимо повторно создать и применить арендаторов vRealize Automation и Workspace ONE Access.

После создания сертификатов их можно применить в Lifecycle Manager с помощью функции Lifecycle Operations (Операции жизненного цикла). Выберите среду и продукт, а затем в меню справа нажмите «Заменить сертификат». Далее можно выбрать продукт. При замене сертификата необходимо повторно настроить доверие для всех связанных продуктов в среде.

Перед тем как перейти к следующему шагу, необходимо дождаться применения сертификата и перезапуска всех служб.

Дополнительные сведения см. в разделах [Управление сертификатами и конфигурацией DNS в развертываниях с одним узлом и несколькими арендаторами](#) и [Управление сертификатами и конфигурацией DNS в кластерных развертываниях vRealize Automation](#).

3. Примените сертификат SAN Workspace ONE Access к экземпляру или кластеру Workspace ONE Access.
4. В vRealize Suite Lifecycle Manager запустите мастер включения аренды, чтобы включить множественную аренду и создать псевдоним для главного арендатора по умолчанию.

Для включения аренды требуется создать псевдоним главного арендатора или арендатора по умолчанию организации-поставщика. После включения аренды можно получить доступ к Workspace ONE Access через полное доменное имя главного арендатора.

Например, существующим полным доменным именем Workspace ONE Access является `idm.example.local`. Создается псевдоним для арендатора по умолчанию. После включения аренды полное доменное имя Workspace ONE Access меняется на `default-tenant.example.local`, а все клиенты, которые обмениваются данными с Workspace ONE Access, теперь будут делать это через `default-tenant.example.local`.

5. Примените сертификаты vRealize Automation SAN к экземпляру vRealize Automation или кластеру.

Сертификаты SAN можно применить с помощью службы Lifecycle Operations компонента Lifecycle Manager. Просмотрите сведения о среде, а затем в меню справа выберите «Заменить сертификаты». Перед добавлением арендаторов необходимо дождаться завершения задачи замены сертификатов. В процессе замены сертификатов службы vRealize Automation перезапускаются.

6. В Lifecycle Manager запустите мастер «Добавить арендаторов» для настройки нужных арендаторов.

Для добавления арендаторов используется страница Lifecycle Manager «Управление арендаторами», расположенная в разделе «Управление удостоверениями и арендаторами». Можно добавлять только тех арендаторов, для которых ранее были настроены сертификаты и параметры DNS.

При создании арендатора необходимо назначить администратора арендатора, а также выбрать подключения к Active Directory для этого арендатора. Доступные подключения зависят от подключений, настроенных для арендатора по умолчанию или главного арендатора. Также необходимо выбрать продукт или экземпляр продукта, с которым будет связан арендатор.

Следующие шаги

Когда арендаторы созданы, на странице Lifecycle Manager «Управление арендаторами», расположенной в разделе «Управление удостоверениями и арендаторами», можно изменить или добавить администраторов арендаторов, добавить каталоги Active Directory в арендатор и изменить связанные продукты для арендатора.

Кроме того, можно войти в экземпляр Workspace ONE Access для просмотра и проверки конфигурации арендатора.

Управление сертификатами и конфигурацией DNS в развертываниях с одним узлом и несколькими арендаторами

Конфигурации vRealize Automation с несколькими арендаторами строятся на основе согласованной конфигурации между несколькими продуктами. Убедитесь, что сертификаты и параметры DNS, необходимые для работы конфигурации с несколькими арендаторами, настроены правильно.

Данная конфигурация с несколькими арендаторами предполагает развертывания с одним узлом для следующих компонентов.

- Lifecycle Manager
- Workspace ONE Access Identity Manager
- vRealize Automation

Кроме того, она предполагает, что начать следует с арендатора по умолчанию, который представляет собой организацию поставщика, и затем создать два субарендатора с названиями tenant-1 и tenant-2.

Создать и применить сертификаты можно с помощью службы Locker в vRealize Suite Lifecycle Manager или с помощью другого механизма. Lifecycle Manager также позволяет заменять сертификаты или повторно настраивать для них доверие в vRealize Automation или Workspace ONE Access.

Требования к DNS

Для системных компонентов необходимо создать обе основные записи типа A и CNAME, как описано ниже.

- Создайте обе основные записи типа A для каждого системного компонента и каждого арендатора, которые будут созданы при включении нескольких арендаторов (многоарендности).

- Создайте записи многоарендности типа A для каждого из создаваемых арендаторов, а также для главного арендатора.
- Создайте записи многоарендности типа CNAME для каждого из создаваемых арендаторов, за исключением главного арендатора.

Требования к сертификатам для развертывания многоарендности с одним узлом

Необходимо создать два сертификата с альтернативным именем субъекта (SAN): один для Workspace ONE Access и второй для vRealize Automation.

- Сертификат vRealize Automation содержит имя узла сервера vRealize Automation и имена создаваемых арендаторов.
- Сертификат Workspace ONE Access содержит имя узла сервера Workspace ONE Access и имена создаваемых арендаторов.
- Если используются выделенные имена SAN, сертификаты необходимо обновлять вручную при добавлении и удалении узлов, а также при изменении имени узла. Кроме того, необходимо обновить записи DNS для арендаторов. Чтобы упростить конфигурацию, для сертификатов Workspace ONE Access и vRealize Automation можно использовать подстановочные знаки. Например, *.example.com и *.vra.example.com.

Примечание vRealize Automation 8.x поддерживает сертификаты с подстановочными знаками только для DNS-имен, которые соответствуют спецификациям в списке публичных суффиксов в <https://publicsuffix.org>. Например, *.myorg.com является допустимым именем, в то время как *.myorg.local — недопустимое имя.

Обратите внимание, что Lifecycle Manager не создает отдельные сертификаты для каждого арендатора. Вместо этого создается единый сертификат с указанием имен всех узлов арендаторов. В базовых конфигурациях для CNAME арендатора используется следующий формат: *имя_арендатора.vrahostname.domain*. В конфигурациях с высокой доступностью для имени используется следующий формат: *имя_арендатора.vraLBhostname.domain*.

Сводка

В следующей таблице приведены требования к DNS и сертификатам для развертывания Workspace ONE Access с одним узлом и vRealize Automation с одним узлом.

Требования к DNS	Требования к сертификатам SAN
Main A Type Records lcm.example.local WorkspaceOne.example.local vra.example.local	Workspace One Certificate Имя узла: WorkspaceOne.example.local, default-tenant.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local
Multi-tenancy A Type Records default-tenant.example.local tenant-1.example.local tenant-2.example.local	
Multi-Tenancy CNAME Type Records tenant-1.vra.example.local tenant-2.vra.example.local	vRealize Automation Certificate Имя узла: vra.example.local, tenant-1.vra.example.local, tenant-2.vra.example.local

Управление сертификатами и конфигурацией DNS в кластерных развертываниях vRealize Automation

Чтобы настроить кластерное развертывание vRealize Automation с несколькими организациями, необходимо согласовать сертификаты и конфигурацию DNS между всеми применимыми компонентами.

В типовой кластерной конфигурации содержится три устройства Workspace ONE Access, три устройства vRealize Automation и одно устройство Lifecycle Manager.

Данная конфигурация предполагает кластерные развертывания для следующих компонентов.

- Устройства Workspace ONE Access Identity Manager:

- idm1.example.local
- idm2.example.local
- idm3.example.local
- idm-lb.example.local

- Устройства vRealize Automation:

- vra-1.example.local
- vra-2.example.local
- vra-3.example.local
- vra-lb.example.local

- Устройство Lifecycle Manager

Требования к DNS

Создайте обе основные записи типа **A** для каждого компонента и для каждого арендатора, которые будут созданы при включении множественной аренды. Кроме того, создайте записи множественной аренды типа **CNAME** для каждого из создаваемых арендаторов, кроме главного арендатора. И наконец, создайте основные записи типа **A** для подсистем балансировки нагрузки Workspace ONE Access и vRealize Automation.

- Создайте записи типа **A** для трех устройств Workspace ONE Access и для устройств vRealize Automation, которые указывают на соответствующие полные доменные имена.
- Кроме того, создайте записи типа **A** для подсистем балансировки нагрузки Workspace ONE Access и vRealize Automation, указывающие на соответствующие полные доменные имена.
- Создайте записи множественной аренды типа **A** для арендатора по умолчанию и арендаторов tenant-1 и tenant-2, которые указывают на IP-адрес подсистемы балансировки нагрузки Workspace ONE Access.
- Создайте записи **CNAME** для арендаторов tenant-1 и tenant-2, которые указывают на IP-адрес подсистемы балансировки нагрузки vRealize Automation.

Требования к сертификату альтернативных имен субъекта (SAN)

Необходимо создать два сертификата Workspace ONE Access, один из которых применяется на устройствах кластера, а второй — в подсистеме балансировки нагрузки. Кроме того, создайте сертификат, который применяется к устройствам vRealize Automation, создаваемым арендаторам (кроме арендатора по умолчанию) и подсистеме балансировки нагрузки.

- Создайте сертификат для устройств Workspace ONE Access, в котором указаны полные доменные имена устройств Workspace ONE Access, а также арендатор по умолчанию и другие создаваемые арендаторы. Этот сертификат должен содержать IP-адреса устройств Workspace ONE Access.
- Рекомендуется настроить режим прерывания SSL в подсистеме балансировки нагрузки. Для этого создайте сертификат для подсистемы балансировки нагрузки Workspace ONE Access, в котором указано полное доменное имя подсистемы балансировки нагрузки Workspace ONE Access, а также арендатор по умолчанию и другие создаваемые арендаторы. Этот сертификат должен содержать IP-адрес подсистемы балансировки нагрузки.
- Создайте сертификат для vRealize Automation, в котором перечислены имена узлов трех устройств vRealize Automation, а также соответствующие подсистемы балансировки нагрузки и создаваемые арендаторы. Кроме того, в нем должны быть перечислены IP-адреса трех устройств vRealize Automation.

- Для упрощения конфигурации для сертификатов Workspace ONE Access и vRealize Automation можно использовать подстановочные знаки. Например, *.example.com, *.vra.example.com и *.vra-lb.example.com.

Примечание vRealize Automation 8.x поддерживает сертификаты с подстановочными знаками только для DNS-имен, которые соответствуют спецификациям в списке публичных суффиксов в <https://publicsuffix.org>. Например, *.myorg.com является допустимым именем, в то время как *.myorg.local — недопустимое имя.

Если используется кластерная конфигурация Workspace ONE Access, Lifecycle Manager не сможет обновить сертификаты подсистемы балансировки нагрузки, поэтому их необходимо обновить вручную. Кроме того, если необходимо повторно зарегистрировать продукты или службы, которые являются внешними по отношению к Lifecycle Manager, этот процесс выполняется вручную.

Сводка сертификатов и записей DNS для кластерной конфигурации с несколькими организациями

В следующих таблицах приведены основные записи типа A в DNS и записи «Тип имени C» и требования к сертификатам для кластерного развертывания Workspace ONE Access и кластерного развертывания vRealize Automation с несколькими организациями.

Требования к DNS	Требования к сертификатам SAN
<p>Main A Type Records</p> <ul style="list-style-type: none"> ■ lcm.example.local ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ WorkspaceOne-lb.example.local ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local 	<p>Workspace One Certificate</p> <p>Имя узла:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-1.example.local ■ WorkspaceOne-2.example.local ■ WorkspaceOne-3.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy A Type Records</p> <ul style="list-style-type: none"> ■ default-tenant.example.local ■ tenant-1.vra.example.local ■ tenant-2.vra.example.local <p>Примечание Все записи типа А с несколькими клиентами должны указывать на IP-адрес подсистемы балансировки нагрузки vIDM/WS1A.</p>	<p>Workspace One LB Certificate (LB Terminated)</p> <p>Имя узла:</p> <ul style="list-style-type: none"> ■ WorkspaceOne-lb.example.local ■ default-tenant.example.local ■ tenant-1.example.local ■ tenant-2.example.local
<p>Multi-Tenancy CNAME Type Records</p> <ul style="list-style-type: none"> ■ tenant-1.vra-lb.example.local - vra-lb.example.local ■ tenant-2.vra-lb.example.local - vra-lb.example.local 	<p>vRealize Automation Certificate</p> <p>Имя узла:</p> <ul style="list-style-type: none"> ■ vra-1.example.local ■ vra-2.example.local ■ vra-3.example.local ■ vra-lb.example.local ■ tenant-1.example.local ■ tenant-2.example.local <p>В подсистеме балансировки нагрузки vRealize Automation сертификат не требуется, так как используется транзитный режим SSL.</p>

Примечание Каждый дополнительный добавляемый клиент должен быть указан отдельно в сертификате vRealize Automation, записях CNAME с множественной арендой, записях типа А с множественной арендой, сертификате Workspace ONE и сертификате подсистемы балансировки нагрузки Workspace ONE.

Примечание Имена файлов *.local используются только в качестве примера. Они могут быть неприменимы в большинстве бизнес-сред.

Вход в арендаторы и добавление пользователей в vRealize Automation

После создания арендаторов для vRealize Automation в Lifecycle Manager можно войти в Workspace ONE Access для просмотра своих арендаторов и добавления пользователей.

Чтобы просмотреть сведения о клиентах, созданных для развертывания vRealize Automation, войдите в связанный экземпляр Workspace ONE Access. Используйте URL-адрес `https://имя_арендатора_по_умолчанию.domainname.local` или `https://idm.domainname.local` для некластерного развертывания, который отправляет к URL-адресу Workspace ONE Access арендатора по умолчанию.

Чтобы проверить отдельные арендаторы в Workspace ONE Access, используйте следующий URL-адрес: `https://tenant-1.domainname.local`. Этот URL-адрес открывает страницу, на которой отображаются пользователи указанного арендатора. Нажмите **Добавить пользователя**, чтобы создать дополнительных пользователей в индивидуальном порядке.

Авторизованные пользователи могут войти в главную организацию поставщика в vRealize Automation, используя URL-адрес `https://vra.domainname.local`. Это представление открывает доступ ко всем связанным службам vRealize Automation.

Авторизованные пользователи могут входить в соответствующие арендаторы в vRealize Automation, используя URL-адрес `https://имя_арендатора.vra.domainname.local`.

Дополнительные сведения об управлении пользователями в Workspace ONE Access см. в документе [Управление пользователями и группами](#).

Добавление локальных пользователей

Локальных пользователей можно добавить в развертывание с помощью связанного экземпляра Workspace ONE Access. Локальные пользователи — это пользователи, сведения о которых не хранятся в каком-либо внешнем поставщике удостоверений.

Использование vRealize Orchestrator в развертываниях vRealize Automation с несколькими организациями

vRealize Orchestrator можно использовать в развертываниях vRealize Automation с несколькими организациями.

Арендатор по умолчанию поддерживает интеграцию со встроенным vRealize Orchestrator. vRealize Orchestrator предварительно настроен на странице «Интеграции» арендатора по умолчанию.

Субарендаторы не имеют предварительно зарегистрированных интеграций vRealize Orchestrator. Для них предусмотрено несколько способов добавления интеграции vRealize Orchestrator.

- Субарендаторы могут добавить интеграцию со встроенным vRealize Orchestrator, перейдя в раздел **Инфраструктура > Подключения > Интеграции**.

Примечание Если встроенный vRealize Orchestrator добавлен в качестве интеграции нескольким арендаторам, все содержимое vRealize Orchestrator, в том числе иерархия подключаемого модуля, будет общим для этих арендаторов.

- Субарендаторы могут добавить внешний экземпляр vRealize Orchestrator, в котором используется vRealize Automation с несколькими организациями, в качестве поставщика проверки подлинности.

Любой экземпляр vRealize Orchestrator, использующий развертывание vRealize Automation с несколькими организациями в качестве поставщика проверки подлинности, можно зарегистрировать для любого из арендаторов, создав новую интеграцию и указав полное доменное имя vRealize Orchestrator без предоставления учетных данных.

Работа с журналами в vRealize Automation

5

Для создания и использования журналов в vRealize Automation можно использовать предоставляемую служебную программу командной строки `vracli`.

Журналы можно использовать непосредственно в vRealize Automation или пересылать их все в vRealize Log Insight.

В эту главу входят следующие разделы:

- [Работа с журналами и наборами журналов в vRealize Automation](#)
- [Настройка пересылки журналов в vRealize Log Insight в vRealize Automation](#)
- [Создание и обновление интеграции системного журнала в vRealize Automation](#)
- [Работа с контент-пакетами](#)

Работа с журналами и наборами журналов в vRealize Automation

Различные службы создают журналы автоматически. В vRealize Automation можно создавать наборы журналов. Кроме того, в среде можно настроить автоматическую отправку журналов в vRealize Log Insight.

Для получения сведений о служебной программе командной строки `vracli` используйте аргумент `--help` в командной строке `vracli` (например, `vracli log-bundle --help`).

Дополнительные сведения об использовании vRealize Log Insight см. в разделе [Настройка пересылки журналов в vRealize Log Insight в vRealize Automation](#).

Команды набора журналов

В наборе журналов можно объединить все журналы, которые создаются запущенными службами. Набор журналов содержит все журналы служб. Набор журналов можно использовать для устранения неполадок.

В кластерной среде (режим высокой доступности) команда `vracli log-bundle` выполняется только на одном узле. Журналы собираются со всех узлов в среде. Однако при наличии проблем с сетевым подключением или проблем в кластере журналы собираются только с доступных узлов. Например, если в кластере, состоящем из трех узлов, один узел недоступен, то журналы собираются только с двух работоспособных узлов. Выходные данные команды `vracli log-bundle` содержат сведения об обнаруженных проблемах и их устранении.

- Чтобы создать набор журналов, необходимо подключиться по протоколу SSH к любому узлу и выполнить следующую команду `vracli`:

```
vracli log-bundle
```

- Чтобы изменить время ожидания при получении журналов с каждого узла, выполните следующую команду `vracli`:

```
vracli log-bundle --collector-timeout $CUSTOM_TIMEOUT_IN_SECONDS
```

Например, в среде с большими файлами журналов, медленной сетью или интенсивным использованием ЦП, можно установить время ожидания, превышающее значение по умолчанию (1000 сек.).

- Чтобы определить дисковое пространство, используемое конкретным журналом службы, например `ebs` или `vro`, выполните следующую команду `vracli` и проанализируйте ее выходные данные.

```
vracli disk-mgr
```

- Чтобы настроить другие параметры, например время ожидания сборки и расположение буфера, используйте следующую команду справки `vracli`:

```
vracli log-bundle --help
```

Структура набора журналов

Набор журналов — это файл `tar` с отметками времени. Имя пакета формируется по шаблону `log-bundle-<дата>T<время>.tar`, например `log-bundle-20200629T131312.tar`. Типовой набор журналов содержит журналы со всех узлов среды. В случае ошибки он содержит максимально возможное количество журналов. Как минимум он содержит журналы с локального узла.

Набор журналов включает в себя следующее содержимое.

- Файл среды

Файл среды содержит выходные данные различных команд обслуживания Kubernetes. Он предоставляет информацию о текущем использовании ресурсов по узлам и по модулям. В нем также содержатся сведения о кластере и описания всех доступных сущностей Kubernetes.

- Журналы узлов и конфигурация

Конфигурация каждого узла (например, его каталога `/etc`) и связанные с узлом журналы (например, `journalld`) собираются в одном каталоге для каждого узла кластера. Имя каталога соответствует имени узла. Внутреннее содержимое каталога соответствует файловой системе узла. Количество каталогов соответствует количеству узлов кластера.

- Журналы служб

Журналы для служб Kubernetes находятся в следующей иерархии папок:

- `<hostname>/services-logs/<namespace>/<app-name>/file-logs/<container-name>.log`
- `<hostname>/services-logs/<namespace>/<app-name>/console-logs/<container-name>.log`

Пример имени файла: `my-host-01/services-logs/prelude/vco-app/file-logs/vco-server-app.log`.

- *hostname* — это имя узла, на котором выполняется или выполнялся контейнер приложения. Как правило, на каждом узле используется один экземпляр каждой службы. Например, 3 узла = 3 экземпляра.
- *namespace* — это пространство имен Kubernetes, в котором развернуто приложение. Для служб, связанных с пользователями, оно имеет значение `prelude`.
- *app-name* — это имя приложения Kubernetes, создавшего журналы (например, `provisioning-service-app`).
- *container-name* — это имя контейнера, в котором созданы журналы. Некоторые приложения состоят из нескольких контейнеров. Например, контейнер `vco-app` содержит контейнеры `vco-server-app` и `vco-controlcenter-app`.
- Журналы модулей (устарело)

До того, как в vRealize Automation 8.2 были внесены изменения в архитектуру ведения журналов, журналы служб находились в наборе журналов в каталоге каждого модуля. Хотя наборы журналов модулей можно по-прежнему создавать с помощью команды `vraccli log-bundle --include-legacy-pod-logs`, это не рекомендуется делать, поскольку все данные журналов уже находятся в журналах служб. Создание журналов модулей может привести к невынужденной потере времени и затратам памяти при создании набора журналов.

Уменьшение размера набора журналов

Чтобы создать набор журналов, имеющий меньший размер, используйте какую-либо из следующих команд `vraccli log-bundle`.

- `vraccli log-bundle --since-days n`

Эта команда используется для сбора только тех файлов журнала, которые были созданы за определенное количество прошедших дней. По умолчанию собираются и хранятся журналы за последние 2 дня. Например:

```
vraccli log-bundle --since-days 1
```

- `vraccli log-bundle --services service_A,service_B,service_C`

Эта команда используется для сбора журналов только для именованных предоставленных служб. Например:

```
vraccli log-bundle --services ebs-app,vco-app
```

- `vracli log-bundle --skip-heap-dumps`

Используйте эту команду, чтобы исключить дампы кучи из созданного набора журналов.

Отображение журналов

Для вывода журналов модуля или приложения службы можно использовать команду `vracli logs <pod_name>`.

Доступны следующие параметры команды.

- `--service`

Отображение объединенного журнала для всех узлов приложения вместо одного модуля.

Пример: `vracli logs --service abx-service-app`

- `--tail n`

Отображение последних *n* строк журнала. Значение *n* по умолчанию — 10.

Пример: `vracli logs --tail 20 abx-service-app-8598fcd4b4-tjwhk`

- `--file`

Отображение только указанного файла. Если имя файла не указано, отображаются все файлы.

Пример: `vracli logs --file abx-service-app.log abx-service-app-8598fcd4b4-tjwhk`

Основные сведения о ротации журналов

Что касается ротации журналов, необходимо учитывать следующие факторы, касающиеся журналов служб.

- Все службы создают журналы. Журналы служб хранятся на выделенном диске `/var/log/services-logs`.
- Все журналы регулярно проходят ротацию. Ротация происходит ежечасно или при достижении определенного ограничения размера.
- Ротация старых журналов со временем уплотняется.
- Квот на ротацию журналов для отдельных служб не устанавливается.
- Система сохраняет как можно больше журналов. Автоматизация регулярно проверяет дисковое пространство, занятое журналами. Если оно заполняется на 70 %, старые журналы удаляются, пока его объем не достигнет 60 %.
- Если требуется больше пространства, емкость диска для журналов можно изменить. См. раздел [Увеличение размера диска устройства vRealize Automation](#).

Чтобы проверить дисковое пространство для журналов, выполните следующие команды `vracli`.

Свободного места на диске `/dev/sdc (/var/log)` для каждого узла должно быть не менее 30 %.

```
# vracli cluster exec -- bash -c 'current_node; vracli disk-mgr; exit 0'
sc1-10-182-1-103.eng.vmware.com
/dev/sda4 (/):
    Total size: 47.80GiB
```

```

Free: 34.46GiB (72.1%)
Available (for non-superusers): 32.00GiB (66.9%)
SCSI ID: (0:0)
/dev/sdb(/data):
Total size: 140.68GiB
Free: 116.68GiB (82.9%)
Available (for non-superusers): 109.47GiB (77.8%)
SCSI ID: (0:1)
/dev/sdc(/var/log):
Total size: 21.48GiB
Free: 20.76GiB (96.6%)
Available (for non-superusers): 19.64GiB (91.4%)
SCSI ID: (0:2)
/dev/sdd(/home):
Total size: 29.36GiB
Free: 29.01GiB (98.8%)
Available (for non-superusers): 27.49GiB (93.7%)
SCSI ID: (0:3)

```

Настройка пересылки журналов в vRealize Log Insight в vRealize Automation

Чтобы воспользоваться преимуществами более надежного средства анализа журналов и создания отчетов, можно пересылать журналы из vRealize Automation в vRealize Log Insight.

vRealize Automation входит в пакет агента ведения журналов [на основе fluentd](#). Этот агент собирает и сохраняет журналы, чтобы их можно было включить в набор журналов и проверить позже. В агенте можно настроить пересылку копий журналов на сервер vRealize Log Insight через REST API vRealize Log Insight. Предоставленный API-интерфейс позволяет другим программам обмениваться данными с vRealize Log Insight.

Дополнительные сведения о vRealize Log Insight, в том числе документацию по REST API vRealize Log Insight, см. в [документации по vRealize Log Insight](#).

В агенте ведения журнала настройте непрерывную пересылку журналов vRealize Automation в vRealize Log Insight. Это можно сделать с помощью служебной программы командной строки `vraccli`.

Все строки журнала помечаются именем узла и тегом среды и могут быть просмотрены в vRealize Log Insight. В среде высокой доступности журналы помечаются разными именами узлов в зависимости от узла, на котором они были созданы. Тег среды настраивается с помощью параметра `--environment ENV`, как описано ниже в разделе *Настройка или обновление интеграции vRealize Log Insight*. В среде высокой доступности тег среды имеет одно значение для всех строк журнала, независимо от узла, на котором они были созданы.

Сведения о том, как пользоваться служебной программой командной строки `vraccli`, можно получить с помощью аргумента `--help` в командной строке `vraccli`. Например: `vraccli vrli --help`. Чтобы ответ был интуитивно понятным для пользователя, начните команду с `vraccli -j vrli`.

Примечание Можно настроить только одну удаленную интеграцию журнала. vRealize Log Insight имеет приоритет в том случае, если доступны как сервер vRealize Log Insight, так и сервер системного журнала.

Проверка существующей конфигурации vRealize Log Insight

Command

```
vracli vrli
```

Arguments

Аргументы командной строки отсутствуют.

Output

Текущая конфигурация для интеграции с vRealize Log Insight выводится в формате JSON.

Exit codes

Возможны следующие коды вывода.

- 0 — интеграция с vRealize Log Insight настроена.
- 1 — в ходе выполнения команды возникло исключение. Дополнительные сведения см. в сообщении об ошибке.
- 61 (ENODATA) — интеграция с vRealize Log Insight не настроена. Дополнительные сведения см. в сообщении об ошибке.

Example - check integration configuration

```
$ vracli vrli
No vRLI integration configured

$ vracli vrli
{
  "agentId": "0",
  "environment": "prod",
  "host": "my-vrli.local",
  "port": 9543,
  "scheme": "https",
  "sslVerify": false
}
```

Настройка или обновление интеграции vRealize Log Insight

Command

```
vracli vrli set [options] FQDN_OR_URL
```

Примечание После выполнения команды может пройти до 2 минут, прежде чем агент ведения журнала сможет применить указанную конфигурацию.

Arguments

- FQDN_OR_URL

Указывает полное доменное имя или URL-адрес сервера vRealize Log Insight, который будет использоваться для публикации журналов. По умолчанию используются порт 9543 и протокол https. Если какой-либо из этих параметров необходимо изменить, вместо него можно использовать URL-адрес.

```
vraccli vrli set <options> https://FQDN:9543
```

Примечание Для отправки журналов можно задать другой протокол (по умолчанию — https) и порт (по умолчанию для https — 9543, для http — 9000), как показано в следующих примерах:

```
vraccli vrli set https://HOSTNAME:9543
vraccli vrli set --insecure HOSTNAME
vraccli vrli set http://HOSTNAME:9000
```

Порт 9543 для https и порт 9000 для http используются REST API для сбора и обработки данных vRealize Log Insight, как описано в статье *Администрирование vRealize Log Insight* в разделе *Порты и внешние интерфейсы документации по vRealize Log Insight*.

■ OPTIONS

■ --agent-id SOME_ID

Устанавливает идентификатор агента ведения журнала для этого устройства. Значение по умолчанию — 0. Используется для идентификации агента при публикации журналов в vRealize Log Insight с помощью REST API vRealize Log Insight.

■ --environment ENV

Устанавливает идентификатор для текущей среды. Он будет присутствовать в журналах vRealize Log Insight в виде тега для каждой записи. Значение по умолчанию — prod.

■ --ca-file /path/to/server-ca.crt

Определяет файл, содержащий сертификат центра сертификации (ЦС), который использовался для подписания сертификата сервера vRealize Log Insight. В связи с этим агент ведения журнала должен доверять указанному центру сертификации и использовать его для проверки сертификата сервера vRealize Log Insight, если он подписан недоверенным центром сертификации. Файл может содержать всю цепочку сертификатов для проверки сертификата. В случае самозаверяющего сертификата требуется передавать сам сертификат.

■ --ca-cert CA_CERT

Определение совпадает с определением параметра --ca-file выше, но сертификат (цепочка сертификатов) передается в виде встроенной строки.

■ --insecure

Отключает проверку сертификата SSL сервера. В результате агент ведения журнала должен принимать любой сертификат SSL при публикации журналов.

■ Дополнительные параметры

■ --request-max-size BYTES

Несколько событий журнала регистрируются одним вызовом API-интерфейса. Этот аргумент определяет максимальный размер полезных данных в байтах для каждого запроса. Допустимые значения находятся в диапазоне от 4000 до 4 000 000. Значение по умолчанию — 256 000. Дополнительные сведения о допустимых значениях см. в разделе регистрации событий vRealize Log Insight в документации по REST API vRealize Log Insight. Слишком маленькое значение может привести к тому, что события, размер которых превышает допустимый размер журнала, будут игнорироваться.

- `--request-timeout SECONDS`

Вызов API-интерфейса может зависать по ряду причин, включая проблемы с удаленным подключением, сетью и т. д. Этот параметр определяет количество секунд, в течение которых ожидается завершение каждой операции, например открытие подключения, запись данных или ожидание ответа, перед тем как вызов будет признан несостоявшимся. Значение не может быть меньше 1 секунды. Значение по умолчанию — 30.

- `--request-immediate-retries RETRIES`

Прежде чем журналы будут отправлены в vRealize Log Insight, они записываются в объединенные блоки (см. ниже параметр `--buffer-flush-thread-count`). Если запрос API-интерфейса завершается сбоем, немедленно выполняется повторная попытка. По умолчанию количество немедленных попыток составляет 3. Если ни одна попытка не была успешной, производится откат всего блока журнала, и позже выполняется повторная попытка.

- `--request-http-compress`

Чтобы снизить объем сетевого трафика, к запросам, которые направляются на сервер vRealize Log Insight, можно применить сжатие gzip. Если этот параметр не указан, сжатие не применяется.

- `--buffer-flush-thread-count THREADS`

Чтобы повысить производительность и уменьшить объем сетевого трафика, перед очисткой журналов и отправкой их данных на сервер выполняется локальная поблочная буферизация журналов. В каждом блоке находятся журналы одной службы. В зависимости от среды блоки могут увеличиваться в размере и требовать много времени для очистки. Этот аргумент определяет количество блоков, которые можно очистить одновременно. Значение по умолчанию — 2.

Примечание Если при настройке интеграции по протоколу https на сервере vRealize Log Insight настроено использование недоверенного сертификата, например самозаверяющего сертификата или сертификата, подписанного недоверенным центром сертификации, необходимо использовать один из параметров `--ca-file`, `--ca-cert` или `--insecure`. В противном случае агент ведения журнала не сможет проверить подлинность сервера и не будет отправлять журналы. Если используется параметр `--ca-file` или `--ca-cert`, сертификат сервера vRealize Log Insight должен быть действительным для имени узла сервера. В любом случае следует проверить интеграцию: предоставить несколько минут на обработку и затем удостовериться, что служба vRealize Log Insight получила журналы.

Output

Выходные данные не ожидаются.

Exit codes

Возможны следующие коды вывода.

- 0 — конфигурация обновлена.
- 1 — в ходе выполнения возникло исключение. Дополнительные сведения см. в сообщении об ошибке.

Examples - Configure or update integration configuration

Примеры инструкций ниже отображаются в отдельных командных строках, однако аргументы можно объединить в одну командную строку. Например, можно включить несколько аргументов при использовании `vraccli vrli set {somehost}` или `vraccli vrli set --ca-file path/to/server-ca.crt` для изменения значений по умолчанию идентификатора агента или среды. Дополнительные сведения см. в онлайн-справке по командам: `vraccli vrli --help`.

```
$ vraccli vrli set my-vrli.local
$ vraccli vrli set 10.20.30.40
$ vraccli vrli set --ca-file /etc/ssl/certs/ca.crt 10.20.30.40
$ vraccli vrli set --ca-cert "$(cat /etc/ssl/certs/ca.crt)" 10.20.30.40
$ vraccli vrli set --insecure http://my-vrli.local:8080
$ vraccli vrli set --agent-id my-vrli-agent my-vrli.local
$ vraccli vrli set --request-http-compress
$ vraccli vrli set --environment staging my-vrli.local
$ vraccli vrli set --environment staging --request-max-size 10000 --request-timeout 120 --
request-immediate-retries 5 --buffer-flush-thread-count 4 my-vrli.local
```

Очистка интеграции vRealize Log Insight

Command

```
vraccli vrli unset
```

Примечание После выполнения команды может пройти до 2 минут, прежде чем агент ведения журнала сможет применить указанную конфигурацию.

Arguments

Аргументы командной строки отсутствуют.

Output

Подтверждение выводится в виде обычного текста.

Exit codes

Возможны следующие коды вывода.

- 0 — конфигурация была очищена или не существует.
- 1 — в ходе выполнения возникло исключение. Дополнительные сведения см. в сообщении об ошибке.

Examples - Clear integration

```
$ vracli vrli unset
Clearing vRLI integration configuration

$ vracli vrli unset
No vRLI integration configured
```

Создание и обновление интеграции системного журнала в vRealize Automation

В vRealize Automation можно настроить отправку данных журнала на удаленные серверы системного журнала.

Команда `vracli remote-syslog set` используется для создания интеграции системного журнала или перезаписи существующих интеграций.

Интеграция удаленного системного журнала vRealize Automation поддерживает следующие типы подключений.

- 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.

Примечание Можно настроить только одну удаленную интеграцию журнала. vRealize Log Insight имеет приоритет в том случае, если доступны как сервер vRealize Log Insight, так и сервер системного журнала.

Дополнительные сведения о настройке интеграции журналов с vRealize Log Insight см. в разделе [Настройка пересылки журналов в vRealize Log Insight в vRealize Automation](#).

Необходимые условия

Настройте удаленный сервер системного журнала.

Процедура

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.

2. Чтобы создать интеграцию с сервером системного журнала, выполните команду `vracli remote-syslog set`.

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

Примечание Если не указать порт в команде `vracli remote-syslog set`, 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, выполните команду `vracli remote-syslog set` и задайте для флага `-id` имя интеграции, которую требуется перезаписать.

Примечание По умолчанию при перезаписи интеграции системного журнала на устройстве vRealize Automation запрашивается подтверждение операции. Чтобы пропустить запрос подтверждения, добавьте флаг `-f` или `--force` в команду `vracli remote-syslog set`.

Следующие шаги

Чтобы просмотреть текущие интеграции системного журнала на устройстве, выполните команду `vracli remote-syslog`.

Удаление интеграции системного журнала для ведения журнала в vRealize Automation

Чтобы удалить интеграцию системного журнала с устройства vRealize Automation, выполните команду `vracli remote-syslog unset`.

Необходимые условия

Создайте одну интеграцию системного журнала или несколько на устройстве vRealize Automation. См. раздел [Создание и обновление интеграции системного журнала в vRealize Automation](#).

Процедура

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.
2. Удалите интеграции системного журнала с устройства vRealize Automation с помощью одного из следующих методов.
 - Чтобы удалить конкретную интеграцию системного журнала, выполните команду `vracli remote-syslog unset -id Integration_name`.

- Чтобы удалить все интеграции системного журнала с устройства vRealize Automation, выполните команду `vracli remote-syslog unset` без флага `-id`.

Примечание По умолчанию при удалении всех интеграций системного журнала с устройства vRealize Automation запрашивается подтверждение операции. Чтобы пропустить запрос подтверждения, добавьте флаг `-f` или `--force` в команду `vracli remote-syslog unset`.

Работа с контент-пакетами

Контент-пакеты размещаются в Log Insight и содержат панели управления, извлеченные поля, сохраненные запросы и оповещения, относящиеся к определенному продукту или набору журналов. Контент-пакеты, поддерживаемые сообществом, можно установить из VMware Sample Exchange, а остальные контент-пакеты — из магазина контент-пакетов.

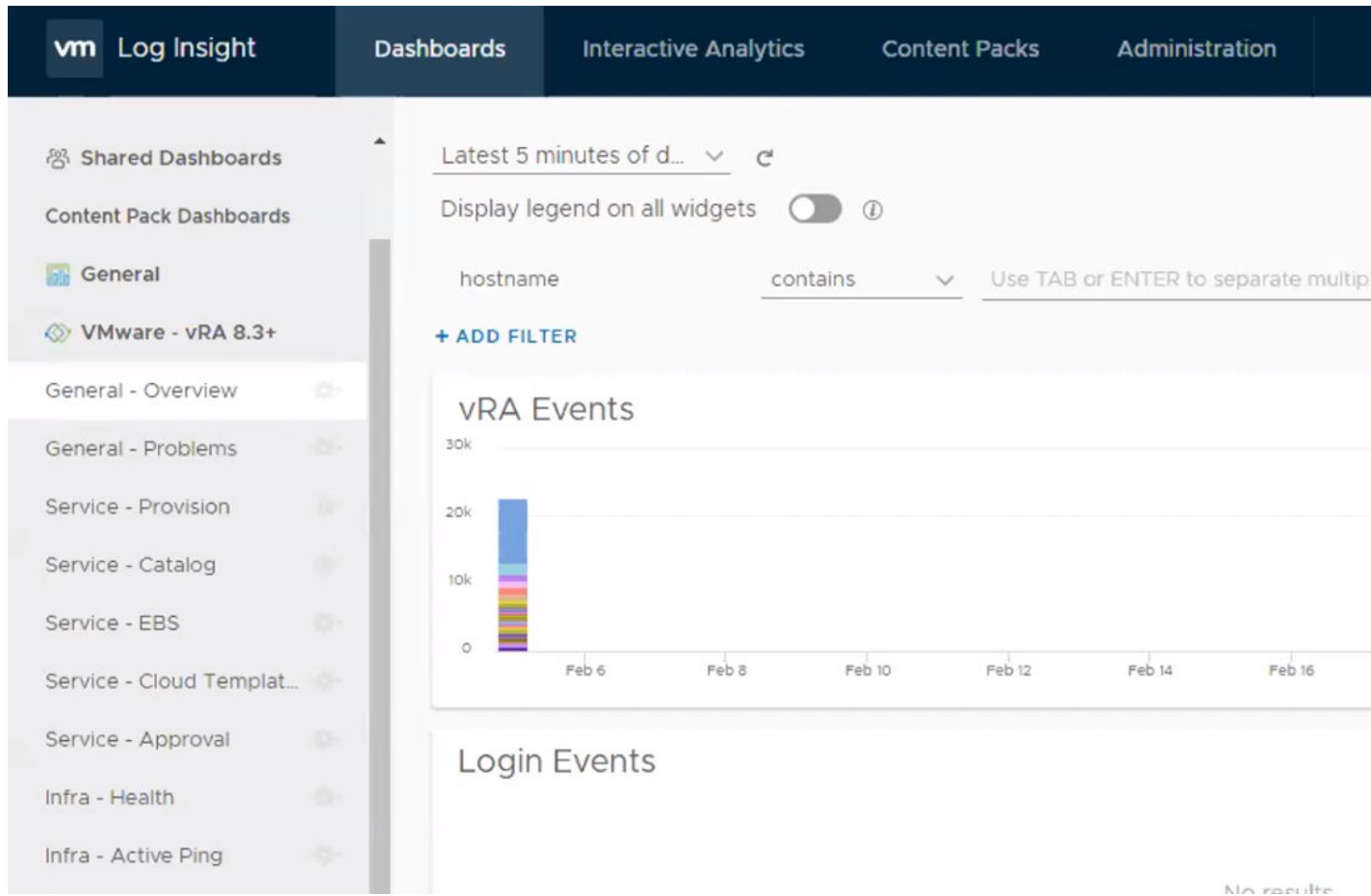
VMware vRealize Log Insight позволяет осуществлять автоматическое управление журналами посредством агрегирования, анализа и поиска, поддержки операционной аналитики и мониторинга всего предприятия в динамических гибридных облачных средах. Контент-пакеты представляют собой подключаемые модули VMware vRealize Log Insight, в которых содержатся предварительно сформированные данные о конкретных типах событий, таких как сообщения журнала.

Чтобы загрузить контент-пакет из Log Insight перейдите в **магазин > контент-пакетов**. Контент-пакеты также можно импортировать, нажав **+ «Импорт контент-пакета»**.

Контент-пакет vRA 8.x


Контент-пакет VMware vRealize Automation содержит общую сводку событий журнала для всех компонентов среды vRA. Он включает в себя несколько панелей управления с общим обзором, ключевыми сведениями об ошибках и операциях, а также данными о работоспособности экземпляра vRA в целом. Список этих панелей управления представлен на вкладке **Панели управления** вместе с другими панелями управления Log Insight. После загрузки панелей управления может потребоваться до 30 секунд для их заполнения показателями.

Примечание Обновить контент-пакет vRA 7.5+ до версии 8.3 невозможно. Необходимо отдельно установить контент-пакет vRA 8.3. После установки контент-пакеты версий 8.3 и 7.5 работают по отдельности.

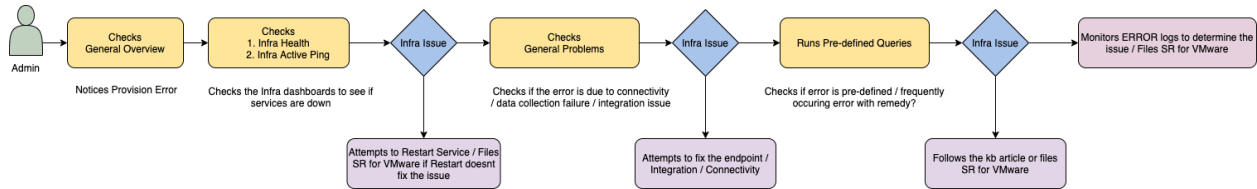


Контент-пакет vRealize Automation включает в себя следующие панели управления.

- Общие — обзор: сбор общих показателей для vRA.
- Общие — проблемы:
- Служба — предоставление: сбор сведений о проблемах, связанных со службой предоставления.
- Служба — каталог: сбор сведений о проблемах, связанных со службой каталогов.
- Служба — EBS: сбор сведений о проблемах, связанных со службой брокера событий.
- Служба — облачные шаблоны: сбор сведений об ошибках и показателях, связанных с облачными шаблонами Cloud Assembly, настраиваемыми ресурсами и действиями с ресурсами.
- Служба — утверждение: сбор сведений об ошибках и показателях, связанных с утверждениями.
- Инфраструктура — работоспособность: сбор сведений о перезапуске модулей за период времени. Эта панель управления необходима для обнаружения простоев из-за ограничений ресурсов.
- Инфраструктура — активная проверка связи (Active Ping): сбор сведений о URL-адресе, используемом для проверки работоспособности, за период времени.

В каждой панели управления есть отдельные мини-приложения, которые позволяют провести более детальный анализ. Чтобы узнать, какой тип анализа выполняется в мини-приложении, щелкните значок сведений ().

Администратор vRealize Automation может следить за рабочим процессом использования контент-пакета, чтобы выявлять ошибки и устранять неполадки.



Дополнительные сведения о контент-пакете vRealize Automation 8.3 см. в разделе [Контент-пакет vRealize Automation 8.3 Log Insight](#) и [Настройка пересылки журналов в vRealize Log Insight](#).

Участие в программе улучшения качества программного обеспечения vRealize Automation

6

Этот продукт участвует в программе улучшения качества программного обеспечения (CEIP) от компании VMware. Информация, получаемая через CEIP, позволяет компании VMware улучшать свои продукты и услуги, исправлять ошибки, а также давать рекомендации по эффективному развертыванию и использованию продуктов.

Сведения о собираемых в CEIP данных и целях, в которых они используются VMware, изложены в разделе на странице о [Программе улучшения качества программного обеспечения](#).

В эту главу входят следующие разделы:

- [Присоединение к программе улучшения качества программного обеспечения для vRealize Automation и выход из нее](#)
- [Настройка времени сбора данных для программы улучшения качества программного обеспечения для vRealize Automation](#)

Присоединение к программе улучшения качества программного обеспечения для vRealize Automation и выход из нее

Присоединиться к программе улучшения качества программного обеспечения (CEIP) или выйти из нее можно с помощью командной строки устройства vRealize Automation.

Присоединиться к программе CEIP можно при установке vRealize Automation и с помощью vRealize Lifecycle Manager (LCM). Кроме того, присоединиться к программе или выйти из нее можно с помощью параметров командной строки после установки.

Чтобы присоединиться к программе улучшения качества программного обеспечения с помощью параметров командной строки, выполните следующие действия.

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.
2. Выполните команду `vracli ceip on`.
3. Просмотрите сведения о программе улучшения качества программного обеспечения и выполните команду `vracli ceip on --acknowledge-ceip`.
4. Чтобы перезапустить службы vRealize Automation, выполните команду `/opt/scripts/deploy.sh`.

Чтобы выйти из программы улучшения качества программного обеспечения с помощью параметров командной строки, выполните следующие действия.

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.
2. Выполните команду `vracli ceip off`.
3. Чтобы перезапустить службы vRealize Automation, выполните команду `/opt/scripts/deploy.sh`.

Настройка времени сбора данных для программы улучшения качества программного обеспечения для vRealize Automation

Можно задать день и время, когда программа улучшения качества программного обеспечения (CEIP) будет отправлять данные VMware.

Процедура

1. Выполните вход в командную строку устройства vRealize Automation как пользователь **root**.
2. Откройте следующий файл в текстовом редакторе.

```
/etc/telemetry/telemetry-collector-vami.properties
```

3. Измените свойства «День недели» (dow) и «Время суток» (hod).

Свойство	Описание
<code>frequency.dow=<day-of-week></code>	День, в который выполняется сбор данных.
<code>frequency.hod=<hour-of-day></code>	Время суток (местное), когда выполняется сбор данных. Возможные значения: 0–23.

4. Сохраните и закройте `telemetry-collector-vami.properties`.
5. Для применения настроек введите указанную далее команду.

```
vcac-config telemetry-config-update --update-info
```

Изменения действуют для всех узлов в развертывании.

Включение формы отзыва в продукте в vRealize Automation

7

Пользователям можно разрешить оставлять отзывы для группы разработчиков vRealize Automation. Ваши отзывы очень важны для процесса разработки.

Что такое форма отзыва

Форма отзыва находится на панели поддержки на вкладке «Обратная связь». Чтобы открыть эту форму, нажмите кнопку **Справка**, а затем **Обратная связь**.

The screenshot shows the vRealize Automation user interface. At the top, there is a navigation bar with a key icon, a question mark icon (highlighted with a yellow box), and the user's name 'Fritz Arbeiter' with a dropdown arrow. Below the navigation bar, there are two tabs: 'SUPPORT' and 'FEEDBACK' (highlighted with a yellow box). The 'FEEDBACK' form contains the following elements:

- A message: "You can rate your experience and send us feedback about vRealize Automation."
- A question: "How satisfied are you with vRealize Automation?"
- A rating scale from 1 to 7, with 'Extremely Dissatisfied' at the left and 'Extremely Satisfied' at the right.
- A text area for additional feedback: "Do you have any other feedback about vRealize Automation? Let us know what's on your mind:"
- A dropdown menu for follow-up contact: "Your voice matters, and sometimes we want to hear more! Can we contact you for a follow-up conversation?" with 'Yes' selected.
- A field for the best way to reach the user: "If yes, what's the best way to reach you?" with a placeholder "Enter phone number or email address here".
- A disclaimer: "We will use any information that you share with us, in addition to information about your account, to fix problems, improve our products and services, and provide you with recommendations. If you choose to share your contact information, we will only use it to".

Как предоставить пользователям доступа к форме отзыва

Для формы отзыва требуется, чтобы узел vRealize Automation был подключен к Интернету, а следующие базовые URL-адреса добавлены в разрешенный список Интернета.

- <https://lumos.vmware.com/>

- <https://feedback.esp.vmware.com/>

Если у узла нет доступа к Интернету, на панели «Справка» эта форма будет недоступна.