

Управление vRealize Automation

21 июля 2021 г.

vRealize Automation 7.6

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

© 2015–2021 гг. VMware, Inc. Все права защищены. [Информация об авторских правах и товарных знаках.](#)

Содержание

1	Обслуживание и настройка компонентов и параметров vRealize Automation	5
	Широковещательная передача сообщения всем пользователям	5
	Создание разрешенного списка URL-адресов для панели сообщений	7
	Запуск и завершение работы vRealize Automation	8
	Запуск vRealize Automation	8
	Перезапуск vRealize Automation	9
	Завершение работы vRealize Automation	11
	Обновление сертификатов vRealize Automation	12
	Извлечение сертификатов и закрытых ключей	14
	Замена сертификатов в устройстве vRealize Automation	14
	Замена сертификата инфраструктуры как услуги	17
	Замена сертификата службы диспетчера инфраструктуры как услуги	19
	Включение во встроенном vRealize Orchestrator доверия к сертификатам vRealize Automation.	21
	Включение во внешнем vRealize Orchestrator доверия к сертификатам vRealize Automation.	24
	Обновление сертификата сайта управления устройством vRealize Automation	24
	Замена сертификата агента управления	29
	Изменение метода опроса для сертификатов	32
	Управление базой данных устройства Postgres vRealize Automation	32
	Настройка базы данных устройств	34
	Сценарии автоматического аварийного переключения базы данных устройства при сбое в работе трех узлов	36
	Сценарий: аварийное переключение базы данных устройств вручную	39
	Сценарий: выполнение тестового переключения баз данных	40
	Ручное восстановление базы данных устройства после катастрофического сбоя	42
	Резервное копирование и восстановление установок vRealize Automation	44
	Программа улучшения качества программного обеспечения	44
	Присоединение к программе улучшения качества программного обеспечения для vRealize Automation и выход из нее	44
	Настройка времени сбора данных	45
	Настройка параметров системы	45
	Изменение значка «Все службы» в каталоге служб	45
	Настройка параметров смены данных	47
	Настройка параметров в файле конфигурации службы диспетчера	49
	Мониторинг vRealize Automation	55
	Мониторинг рабочих процессов и просмотр журналов	55
	Мониторинг журналов событий и служб	56
	Ведение журнала аудита в vRealize Automation	58

Просмотр сведений об узле для кластеров в распределенных развертываниях	60
Мониторинг работоспособности vRealize Automation	62
Настройка системных тестов для vRealize Automation	63
Настройка тестов арендаторов для vRealize Automation	65
Настройка тестов vRealize Orchestrator	67
Пакет настраиваемых тестов	69
Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation	70
Устранение неполадок службы проверки работоспособности	71
Мониторинг ресурсов среды vRealize Automation с помощью протокола SNMP	72
Мониторинг и управление ресурсами	73
Выбор сценария мониторинга ресурсов	73
Терминология в области использования ресурсов	74
Подключение к облачному компьютеру	74
Уменьшение использования резервирования путем сокращения	77
Списание пути к хранилищу	78
Сбор данных	78
Общие сведения о проверке выделения vSwap для конечных точек vCenter Server	82
Удаление расположений центров обработки данных	83
Мониторинг контейнеров	83
Массовый импорт, обновление или перенос виртуальных машин	84
Импорт виртуальной машины в среду vRealize Automation	85
Обновление виртуальной машины в среде vRealize Automation	89
Перенос виртуальной машины в другую среду vRealize Automation	92

Обслуживание и настройка компонентов и параметров vRealize Automation

1

Вы можете управлять подготовленными компьютерами и другими аспектами развертывания vRealize Automation.

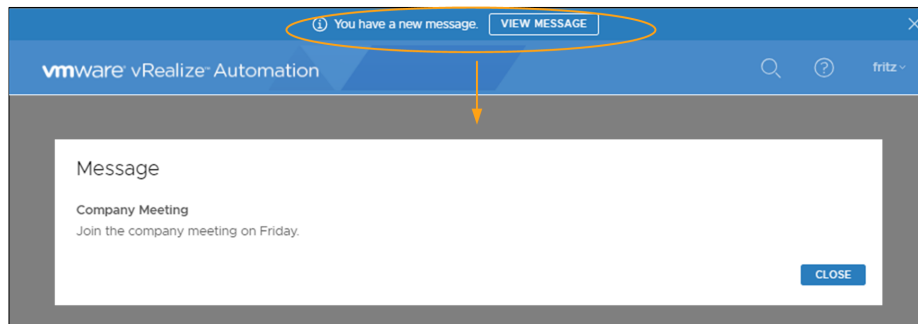
В эту главу входят следующие разделы:

- [Широковещательная передача сообщения всем пользователям](#)
- [Запуск и завершение работы vRealize Automation](#)
- [Обновление сертификатов vRealize Automation](#)
- [Управление базой данных устройства Postgres vRealize Automation](#)
- [Резервное копирование и восстановление установок vRealize Automation](#)
- [Программа улучшения качества программного обеспечения](#)
- [Настройка параметров системы](#)
- [Мониторинг vRealize Automation](#)
- [Мониторинг работоспособности vRealize Automation](#)
- [Мониторинг ресурсов среды vRealize Automation с помощью протокола SNMP](#)
- [Мониторинг и управление ресурсами](#)
- [Мониторинг контейнеров](#)
- [Массовый импорт, обновление или перенос виртуальных машин](#)

Широковещательная передача сообщения всем пользователям

Администратор арендатора может рассылать какое-либо сообщение всем пользователям. Уведомление об этом сообщении появляется в верхней части страницы браузера. Пользователи могут нажать это уведомление, чтобы просмотреть сообщение полностью.

Пользователь может открывать сообщение прямо из баннера или через раскрывающееся меню пользователя в заголовке.



Для широковещательной передачи текстового сообщения или веб-страницы используется панель сообщений. В зависимости от используемой веб-страницы пользователи могут перемещаться по разделам веб-сайта прямо на панели сообщений.

Панель сообщений имеет следующие ограничения.

Таблица 1-1. Ограничения панели сообщений

Параметр	Ограничения
Ограничения URL-сообщений	<ul style="list-style-type: none"> ■ Целевой URL-адрес необходимо включить в разрешенный список для панели сообщений. См. раздел Создание разрешенного списка URL-адресов для панели сообщений. ■ Можно публиковать только содержимое, размещенное на сайте https. ■ Нельзя использовать самозаверяющие сертификаты. Возможность принять такой сертификат не появляется на панели сообщений. ■ URL-адрес панели сообщений встроен в интернет-кадр. Некоторые веб-сайты не работают в интернет-кадре, что вызывает появление ошибки. Одной из причин такой ошибки могут быть значения параметра X-Frame-Options DENY или SAMEORIGIN в заголовке на целевом веб-сайте. Если целевым веб-сайтом является веб-сайт, которым управляет администратор, то можно задать для заголовка X-Frame-Options значение X-Frame-Options: ALLOW-FROM https://<vRealizeAutomationApplianceURL>. ■ У некоторых веб-сайтов настроено перенаправление на страницу верхнего уровня, что может привести к обновлению всей страницы vRealize Automation. Веб-сайт такого типа не сможет работать на панели сообщений. Обновление подавляется, и на панели сообщений появляется сообщение «Загрузка...». ■ Если отображается внутренняя страница HTML, узел vRealize Automation не может быть URL-адресом страницы.
Ограничение настраиваемых сообщений	<ul style="list-style-type: none"> ■ По соображениям безопасности в настраиваемых сообщениях можно использовать простую разметку, но код HTML не поддерживается. Например, нельзя использовать элемент <href> для организации перехода на другой веб-сайт. Для этих целей необходимо использовать функцию URL-сообщения.

Необходимые условия

Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Откройте вкладку **Администрирование**.
2. Выберите **Уведомления > Панель сообщений**
3. В раскрывающемся меню **Тип** выберите тип сообщения.

Параметр	Описание
Нет	Отменяет оповещение о сообщении.
Настраиваемое сообщение	Введите сообщение с простым текстом.
URL-адрес	<p>Введите URL-адрес страницы.</p> <p>Этот URL-адрес необходимо включить в разрешенный список для панели сообщений. См. раздел Создание разрешенного списка URL-адресов для панели сообщений.</p> <p>Чтобы пользователь мог войти на веб-сайт, например на ваш внутренний веб-сайт, с использованием своего идентификатора пользователя vRealize Automation, выберите режим Включить идентификатор пользователя. Пример URL-адреса, который передается на веб-сайт: <code>http://company.com/internal/message?userID=richard_dawson@company.com</code>. Этот метод позволяет вашему веб-сайту с помощью свойства JavaScript <code>window.location.search</code> передавать на этот веб-сайт идентификатор текущего пользователя.</p>

4. Нажмите кнопку **ОК**.

Результаты

Это сообщение рассылается в качестве баннера всем пользователям данного арендатора.

Чтобы изменить или удалить сообщение, необходимо войти в систему в качестве администратора арендатора. Чтобы изменить сообщение, повторите описанные выше шаги. Чтобы удалить это сообщение, выберите значение «Нет» для параметра «Тип» и нажмите **ОК**.

Создание разрешенного списка URL-адресов для панели сообщений

В качестве администратора безопасности настройте список разрешенных URL-адресов, которые могут использоваться на панели сообщений. Такой разрешенный список обеспечивает повышенный уровень безопасности.

Необходимые условия

Войдите в vRealize Automation как **администратор систем безопасности**.

Процедура

1. Выберите **Администрирование > Белый список для панели сообщений**.
2. Нажмите кнопку **Создать**.

3. Добавьте URL-адрес и нажмите **ОК.**

Записи URL-адресов могут включать следующие данные.

- IP-адрес или полное доменное имя веб-сайта. Например, <https://docs.vmware.com>.
- Включает в себя **https**.
- Может также включать разрешенные порты. Если порт не указан, разрешенными портами являются 80 и 443.

4. Эти действия выполняются для каждой записи.**Результаты**

Администратор арендатора не может добавить URL-адрес на панель сообщений, если адрес не входит в этот список.

Следующие шаги

Проверьте, можете ли вы добавить или разослать URL-адрес, входящий в разрешенный список, при помощи панели сообщений. См. раздел [Широковещательная передача сообщения всем пользователям](#).

Запуск и завершение работы vRealize Automation

Системный администратор производит контролируемое завершение работы или запуск vRealize Automation в целях обеспечения целостности системы и данных.

Также контролируемое завершение работы и запуск можно использовать при решении проблем производительности или неправильного функционирования продукта, которые могут являться следствием неправильного начального запуска. Используйте процедуру перезапуска только в случае сбоя отдельных компонентов развертывания.

Запуск vRealize Automation

При включении vRealize Automation после отключения в результате любого штатного или непредвиденного события необходимо запускать компоненты в указанном порядке.

Если вы управляете компонентами развертывания в vCenter Server, вы можете запускать в нем свои гостевые операционные системы.

Необходимые условия

Убедитесь, что используемые развертыванием подсистемы балансировки нагрузки запущены.

Процедура

- 1.** Если используется автономная устаревшая база данных PostgreSQL, запустите этот сервер.
- 2.** Запустите автономные серверы vRealize Automation MS SQL в любом порядке.
- 3.** Если в развертывании используются подсистемы балансировки нагрузки с проверками работоспособности, деактивируйте все проверки работоспособности, кроме проверок связи (ping).

4. Запустите основное устройство vRealize Automation.
5. В интерфейсе управления основным устройством vRealize Automation на вкладке **Кластер** проверьте, в каком режиме работает система (синхронном или асинхронном). Развертывание с одним устройством всегда выполняется в асинхронном режиме.
 - Если развертывание работает в синхронном режиме, запустите оставшиеся устройства vRealize Automation.
 - Если развертывание работает в асинхронном режиме, перейдите в интерфейс управления основным устройством vRealize Automation и дождитесь запуска и РЕГИСТРАЦИИ службы лицензирования.

После этого запустите все оставшиеся устройства vRealize Automation.

6. После запуска всех устройств зайдите в их интерфейсы управления и убедитесь, что службы запущены и ЗАРЕГИСТРИРОВАННЫ.

На запуск устройств может уйти 15 минут или больше.

7. Запустите все веб-узлы Инфраструктура как услуга и подождите 5 минут.
8. Запустите основной узел службы диспетчера и подождите 2–5 минут.
9. В распределенном развертывании с несколькими узлами службы диспетчера запустите дополнительные узлы службы диспетчера и подождите 2–5 минут.

Не запускайте и не выполняйте службу Windows на вторичных компьютерах, если у вас не настроено автоматическое аварийное переключение службы диспетчера.

10. Запустите диспетчер DEM Orchestrator, рабочие процессы DEM Worker и все прокси-агенты vRealize Automation в любом порядке.

Не нужно ждать завершения запуска одного компонента, прежде чем запустить другой.

11. Если проверки работоспособности подсистемы балансировки нагрузки деактивированы, снова активируйте их.
12. Убедитесь, что запущенные службы работают и ЗАРЕГИСТРИРОВАННЫ.

- а) В браузере войдите в интерфейс управления основного устройства vRealize Automation.
<https://vrealize-automation-appliance-FQDN:5480>
- б) Откройте вкладку **Службы**.
- в) Проследите за ходом запуска службы, нажимая кнопку **Обновить**.

Результаты

После того как все службы будут ЗАРЕГИСТРИРОВАННЫ, развертывание готово к использованию.

Перезапуск vRealize Automation

Перезапуск компонентов vRealize Automation может помочь устранить возникшие проблемы. Необходимо перезапускать компоненты в определенном порядке.

Если управление компонентами развертывания осуществляется в vCenter Server, можно перезапустить их гостевые операционные системы в этой среде.

Если не удастся выполнить перезапуск, попробуйте выполнить инструкции в [Завершение работы vRealize Automation](#) и [Запуск vRealize Automation](#).

Необходимые условия

- Убедитесь, что запущены все подсистемы балансировки нагрузки, задействованные в развертывании.

Процедура

1. Убедитесь, что база данных устройства vRealize Automation работает в асинхронном режиме. При необходимости используйте интерфейс управления, чтобы перевести ее в асинхронный режим.

Вы можете вернуться в синхронный режим после завершения всей процедуры. Дополнительные сведения см. в разделе [Управление базой данных устройства Postgres vRealize Automation](#).
2. Перезапустите основное устройство vRealize Automation и дождитесь окончания запуска.
3. Откройте интерфейс управления основного устройства vRealize Automation и убедитесь, что служба лицензирования работает и ЗАРЕГИСТРИРОВАНА.
4. Перезапустите остальные устройства vRealize Automation одновременно.
5. Дождитесь перезапуска устройств, откройте их интерфейсы управления и убедитесь, что службы запущены и ЗАРЕГИСТРИРОВАНЫ.

На перезапуск устройств может уйти 15 минут или более.

6. Перезапустите основной веб-узел и дождитесь окончания процесса загрузки.
7. В распределенном развертывании с несколькими веб-узлами перезапустите все вторичные веб-узлы и дождитесь окончания процесса загрузки.
8. Перезапустите узлы службы диспетчера и дождитесь окончания процесса загрузки.

Если используется автоматическое аварийное переключение службы диспетчера и требуется оставить активные и пассивные узлы без изменений, произведите перезапуск в следующем порядке.

- а) Остановите пассивные узлы службы диспетчера, не перезапуская их.
 - б) Полностью перезапустите активный узел службы диспетчера.
 - в) Запустите пассивные узлы службы диспетчера.
9. Перезапустите диспетчер DEM Orchestrator, рабочие процессы DEM Worker и все прокси-агенты vRealize Automation в любом порядке. Дождитесь завершения запуска.

Не нужно ждать завершения перезапуска каждого компонента, прежде чем запустить другой.

10. Убедитесь, что перезапущенные службы выполняются и ЗАРЕГИСТРИРОВАНЫ.

- а) В браузере войдите в интерфейс управления основного устройства vRealize Automation.
<https://vrealize-automation-appliance-FQDN:5480>
- б) Откройте вкладку **Службы**.
- в) Проследите за ходом запуска службы, нажимая кнопку **Обновить**.

Результаты

После того как все службы будут ЗАРЕГИСТРИРОВАНЫ, развертывание готово к использованию.

Завершение работы vRealize Automation

Чтобы сохранить целостность данных, необходимо завершить работу vRealize Automation в определенном порядке.

Если управление компонентами развертывания выполняется в vCenter Server, можно завершить работу гостевых операционных систем в этом интерфейсе.

Процедура

- 1.** Завершите работу диспетчера DEM Orchestrator, рабочих процессов DEM Worker и всех прокси-агентов vRealize Automation в любом порядке. Дождитесь завершения работы.
- 2.** Завершите работу узлов службы диспетчера и дождитесь завершения всех процессов.
- 3.** В распределенных развертываниях с несколькими веб-узлами завершите работу дополнительных веб-узлов и дождитесь завершения процессов.
- 4.** Завершите работу основного веб-узла и дождитесь завершения процесса.
- 5.** В распределенных развертываниях с несколькими устройствами vRealize Automation, работающими в синхронном режиме, перейдите в асинхронный режим в интерфейсе управления устройством vRealize Automation.
- 6.** В распределенных развертываниях с несколькими устройствами vRealize Automation выключите дополнительные устройства и дождитесь завершения всех процессов.
- 7.** Завершите работу основного устройства vRealize Automation и дождитесь завершения процесса.

Основное устройство vRealize Automation — это устройство, которое содержит основную (т. е. доступную для записи) базу данных устройств. Запишите, какое устройство является основным, чтобы можно было начать резервное копирование в нужном порядке.
- 8.** Завершите работу всех автономных серверов vRealize Automation MS SQL в любом порядке и дождитесь завершения процессов.
- 9.** Если используется автономная устаревшая база данных PostgreSQL, завершите работу сервера.

Обновление сертификатов vRealize Automation

Системный администратор может обновлять или заменять сертификаты для компонентов vRealize Automation.

vRealize Automation содержит три основных компонента, которые используют сертификаты SSL, чтобы упростить безопасное соединение друг с другом.

- Устройство vRealize Automation
- компонент веб-сайта инфраструктуры как услуги
- Компонент службы диспетчера инфраструктуры как услуги

Кроме того, в развертывании могут быть сертификаты для веб-сайта с интерфейсом управления Устройство vRealize Automation. Помимо этого, на каждом компьютере Инфраструктура как услуга работает агент управления, в котором используется сертификат.

Примечание vRealize Automation использует несколько сторонних продуктов, например Rabbit MQ, чтобы обеспечивать поддержку различных функций. Некоторые из этих продуктов используют собственные самозаверяющие сертификаты, которые сохраняются, даже если заменить основные сертификаты vRealize Automation на сертификаты, предоставленные центром сертификации. Из-за этого пользователи не могут полностью контролировать использование сертификатов на отдельных портах, например 5671, который используется RabbitMQ для внутреннего взаимодействия.

Изменения в компонентах поздних версий в этом списке не влияют на компоненты ранних версий, но есть одно исключение. Оно состоит в том, что обновленный сертификат для компонентов Инфраструктура как услуга нужно зарегистрировать на устройстве vRealize Automation.

Как правило, создаются самозаверяющие сертификаты и применяются к этим компонентам во время установки продукта. Возможно, потребуется заменить сертификат, чтобы перейти от использования самозаверяющих сертификатов на сертификаты, предоставленные центром сертификации, или по истечении срока действия сертификата. При замене сертификата для компонента vRealize Automation доверие с другими компонентами vRealize Automation обновляется автоматически.

Например, если в распределенной системе с несколькими экземплярами Устройство vRealize Automation обновить сертификат для одного продукта Устройство vRealize Automation, все другие связанные сертификаты обновятся автоматически.

Примечание vRealize Automation поддерживает сертификаты SHA2. В самозаверяющих сертификатах, созданных в системе, используется SHA-56 с шифрованием RSA. Возможно, потребуется выполнить обновление до сертификатов SHA2 в соответствии с требованиями операционной системы или браузера.

В интерфейсе управления устройством vRealize Automation доступны функции обновления или замены сертификатов.

В кластерном развертывании изменения необходимо инициировать из интерфейса основного узла.

- **Создать сертификат** — vRealize Automation создаст самозаверяющий сертификат.
- **Импортировать сертификат** — использование собственного сертификата.

- **Предоставить отпечаток сертификата** — предоставление отпечатка сертификата для использования сертификата, который уже находится в хранилище сертификатов на серверах Инфраструктура как услуга под управлением Windows.

При использовании этого параметра сертификат не будет передаваться от устройства vRealize Automation на Windows-серверы инфраструктуры как услуги. Этот параметр позволяет развертывать существующие сертификаты на Windows-серверах инфраструктуры как услуги без отправки сертификатов через интерфейс управления устройством vRealize Automation.

- **Сохранить существующий** — продолжить использование текущего сертификата.

Сертификаты для веб-сайтов с интерфейсом управления vRealize Automation не требуют регистрации.

Примечание Если в сертификате для шифрования используется парольная фраза, но ее не удалось правильно ввести при замене сертификата на устройстве, то произойдет сбой замены сертификата и отобразится сообщение `Unable to load private key`.

Шаблоны виртуальной машины

После изменения сертификатов устройства vRealize Automation или Windows-сервера инфраструктуры как услуги необходимо обновить гостевые и программные агенты vRealize Automation в шаблонах виртуальных машин, чтобы эти шаблоны снова работали в vRealize Automation. Если не обновить агенты, то запросы на развертывание, связанные с программными компонентами, завершатся ошибкой, как показано в следующем примере.

```
The following component requests failed: Linux. Request failed: Machine VM-001:
InstallSoftwareWorkflow. Install software work item timeout.
```

vRealize Orchestrator

После замены сертификатов vRealize Automation необходимо обновить vRealize Orchestrator, чтобы включить доверие к новым сертификатам.

Компонент vRealize Orchestrator, связанный с развертыванием vRealize Automation, имеет собственные сертификаты и также должен доверять сертификатам vRealize Automation. По умолчанию компонент vRealize Orchestrator встроен в vRealize Automation, хотя некоторые пользователи предпочитают использовать внешний vRealize Orchestrator. В любом случае информацию об обновлении сертификатов vRealize Orchestrator можно найти в документации по vRealize Orchestrator.

Если используется развертывание vRealize Orchestrator с несколькими узлами в подсистеме балансировки нагрузки, все узлы vRealize Orchestrator должны использовать один и тот же сертификат.

Дополнительная информация

Дополнительную информацию об устранении неполадок, поддержке и требованиях к доверию см. в [статье 2106583 из базы знаний VMware](#).

Извлечение сертификатов и закрытых ключей

Сертификаты, используемые с виртуальными устройствами, должны храниться в PEM-файлах.

В примерах в следующей таблице использованы команды `Gnu openssl` для извлечения сведений о сертификате, необходимых для настройки виртуальных устройств.

Таблица 1-2. Примеры команд (`openssl`) и значений сертификата

Материалы, предоставляемые центром сертификации	Команда	Записи виртуального устройства
Закрытый ключ RSA	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -nocerts -out key.pem</code>	Закрытый ключ RSA
PEM-файл	<code>openssl pkcs12 -in <i>path_to_.pfx</i> <i>certificate_file</i> -clcerts -nokeys -out cert.pem</code>	Цепочка сертификатов
Парольная фраза (необязательно)	н/д	Парольная фраза

Замена сертификатов в устройстве vRealize Automation

Системный администратор может обновить или заменить самозаверяющий сертификат доверенным сертификатом, выданным центром сертификации. Можно использовать сертификаты с альтернативным именем субъекта, групповые сертификаты или любой другой метод многократной сертификации, который подходит для данной среды, при условии, что он удовлетворяет требованиям к доверию.

При обновлении или замене сертификата устройства vRealize Automation доверие в отношении других связанных компонентов автоматически иницируется повторно. Дополнительные сведения об обновлении сертификатов см. в разделе [Обновление сертификатов vRealize Automation](#).

Процедура

1. Выполните вход в интерфейс управления устройства vRealize Automation как пользователь `root`.
`https://vrealize-automation-appliance-FQDN:5480`
2. Выберите **vRA > Сертификаты**.
3. Выберите компонент vRealize Automation, для которого нужно обновить сертификат.
4. Выберите нужное действие в меню **Действие с сертификатом**.

Если используется сертификат в кодировке PEM, например для распределенной среды, выберите **Импорт**.

Импортируемые сертификаты должны быть доверенными. Убедитесь, что их можно применить ко всем экземплярам устройства vRealize Automation и любой подсистеме балансировки нагрузки при помощи сертификатов с альтернативным именем субъекта (Subject Alternative Name, SAN).

Если необходимо создать запрос CSR на новый сертификат, который можно будет отправить в центр сертификации, выберите **Создать запрос подписи**. CSR позволит вашему центру сертификации создать сертификат с правильными значениями, который затем будет можно импортировать.

Примечание Если используются цепочки сертификатов, укажите сертификаты в следующем порядке:

- а) сертификат клиента или сервера, подписанный промежуточным сертификатом центра сертификации;
- б) промежуточные сертификаты (один или несколько);
- в) корневой сертификат центра сертификации.

Параметр	Действие
Сохранить существующую	Сохраните текущую конфигурацию SSL. Выберите этот параметр, чтобы отменить изменения.
Создать сертификат	<ul style="list-style-type: none"> а) Значение, отображаемое в текстовом поле Обычное имя, является именем узла, которое отображается в верхней части страницы. Если существуют дополнительные экземпляры устройства vRealize Automation, их полные доменные имена включаются в атрибут SAN сертификата. б) В текстовом поле Организация введите название организации, например название своей компании. в) В текстовом поле Организационная единица введите организационную единицу, например название отдела или расположение. г) В текстовом поле Страна введите двухбуквенный код страны ISO 3166, например RU.

Параметр	Действие
Создать запрос подписи	<ul style="list-style-type: none"> а) Выберите Создать запрос подписи. б) Проверьте значения в текстовых полях Организации, Организационная единица, Код страны и Обычное имя. Эти значения подставляются из существующего сертификата. При необходимости эти значения можно изменить. в) Щелкните Создать CSR для создания запроса на подпись сертификата, а затем щелкните ссылку Загрузить созданный CSR здесь, чтобы открыть диалоговое окно, с помощью которого CSR можно будет сохранить в расположении для отправки в центр сертификации. г) При получении подготовленного сертификата щелкните Импортировать и выполните процедуру импорта сертификата в vRealize Automation.
Импорт	<ul style="list-style-type: none"> а) Скопируйте значения сертификата, начиная с заголовка BEGIN PRIVATE KEY до нижнего колонтитула END PRIVATE KEY включительно, и вставьте их в текстовое поле Закрытый ключ RSA. б) Скопируйте значения сертификата, начиная с заголовка BEGIN CERTIFICATE до нижнего колонтитула END CERTIFICATE включительно, и вставьте их в текстовое поле Цепочка сертификатов. Для нескольких значений сертификатов добавьте заголовок BEGIN PRIVATE KEY и нижний колонтитул END PRIVATE KEY в каждый сертификат. <hr/> <p>Примечание В цепочках сертификатов могут быть доступны дополнительные атрибуты.</p> <hr/> <ul style="list-style-type: none"> в) (Необязательно.) Если сертификат использует парольную фразу для шифрования ключа, скопируйте ее и вставьте в текстовое поле Парольная фраза.

5. Нажмите кнопку **Сохранить настройки**.

Для обновления сертификата устройства vRealize Automation требуется, чтобы службы vRealize Automation были надлежащим образом перезапущены. Перезапуск может занять от 15 минут до часа в зависимости от количества устройств vRealize Automation в рабочей среде.

После перезапуска на странице отобразятся сведения о сертификате для всех соответствующих экземпляров устройства vRealize Automation.

6. Если это требуется для вашей сети или подсистемы балансировки нагрузки, скопируйте импортированный или новый созданный сертификат в подсистему балансировки нагрузки виртуального устройства.

Может потребоваться включить доступ с правами root по протоколу SSH, чтобы экспортировать сертификат.

- а) Если вы еще не вошли в систему, выполните вход в консоль управления устройства vRealize Automation как в качестве пользователя с правами root.
- б) Откройте вкладку **Администратор**.
- в) Щелкните подменю **Admin**.
- г) Установите флажок **Служба SSH включена**.

По окончании процедуры снимите флажок, чтобы деактивировать протокол SSH.

- д) Установите флажок **Вход администратора по протоколу SSH**.

По окончании процедуры снимите флажок, чтобы деактивировать протокол SSH.

- е) Нажмите кнопку **Сохранить настройки**.

7. Убедитесь, что можете войти в консоль vRealize Automation.

- а) Откройте браузер и перейдите по адресу `https://vcac-hostname.domain.name/vcac`.

В случае использования подсистемы балансировки нагрузки имя узла должно быть полным доменным именем подсистемы балансировки нагрузки.

- б) Пройгнорируйте предупреждения сертификата, если они будут появляться.

- в) Войдите, используя имя **administrator@vsphere.local** и пароль, указанный при настройке управления каталогами.

Консоль откроется на странице **Арендаторы** на вкладке **Администрирование**. В списке появится один арендатор с именем `vsphere.local`.

8. При использовании подсистемы балансировки нагрузки стоит настроить и включить применимые проверки работоспособности.

Результаты

Теперь сертификат обновлен.

Замена сертификата инфраструктуры как услуги

Чтобы обеспечить безопасность в среде распределенного развертывания, системный администратор может заменить сертификат, срок действия которого истек, либо самозаверяющий сертификат сертификатом, выданным центром сертификации.

Сертификат с альтернативным именем субъекта можно использовать на нескольких компьютерах. Сертификаты, используемые для компонентов инфраструктуры как услуги (служба диспетчера и веб-сайта), должны быть выданы со значениями SAN, включая полные доменные имена всех узлов Windows, на которых установлен соответствующий компонент, а также полное доменное имя подсистемы балансировки нагрузки для того же компонента.

Процедура

1. Выполните вход в интерфейс управления устройством vRealize Automation как пользователь `root`.
`https://vrealize-automation-appliance-FQDN:5480`
2. Выберите **vRA > Сертификаты**.
3. Выберите пункт **Веб-инфраструктура как услуга** в меню **Тип компонента**.
4. Перейдите на панель **Сертификат веб-инфраструктуры как услуги**.
5. Выберите параметр замены сертификата в меню **Действие с сертификатом**.

Если используется сертификат в кодировке PEM, например для распределенной среды, выберите **Импорт**.

Импортируемые сертификаты должны быть доверенными. Убедитесь, что их можно применить ко всем экземплярам устройства vRealize Automation и любой подсистеме балансировки нагрузки при помощи сертификатов с альтернативным именем субъекта (Subject Alternative Name, SAN).

Примечание Если используются цепочки сертификатов, укажите сертификаты в следующем порядке:

- а) сертификат клиента или сервера, подписанный промежуточным сертификатом центра сертификации;
- б) промежуточные сертификаты (один или несколько);
- в) корневой сертификат центра сертификации.

Параметр	Описание
Сохранить существующую	Сохраните текущую конфигурацию SSL. Выберите этот параметр, чтобы отменить изменения.
Создать сертификат	<ul style="list-style-type: none"> а) Значение, отображаемое в текстовом поле Обычное имя, является именем узла, которое отображается в верхней части страницы. Если существуют дополнительные экземпляры устройства vRealize Automation, их полные доменные имена включаются в атрибут SAN сертификата. б) В текстовом поле Организация введите название организации, например название своей компании. в) В текстовом поле Организационная единица введите организационную единицу, например название отдела или расположение. г) В текстовом поле Страна введите двухбуквенный код страны ISO 3166, например RU.
Импорт	<ul style="list-style-type: none"> а) Скопируйте значения сертификата, начиная с заголовка BEGIN PRIVATE KEY до нижнего колонтитула END PRIVATE KEY включительно, и вставьте их в текстовое поле Закрытый ключ RSA. б) Скопируйте значения сертификата, начиная с заголовка BEGIN CERTIFICATE до нижнего колонтитула END CERTIFICATE включительно, и вставьте их в текстовое поле Цепочка сертификатов. Для нескольких значений сертификатов добавьте заголовок BEGIN PRIVATE KEY и нижний колонтитул END PRIVATE KEY в каждый сертификат. <p>Примечание В цепочках сертификатов могут быть доступны дополнительные атрибуты.</p> <ul style="list-style-type: none"> в) (Необязательно.) Если сертификат использует парольную фразу для шифрования ключа, скопируйте ее и вставьте в текстовое поле Парольная фраза.
Предоставить отпечаток сертификата	Используйте этот параметр, если необходимо предоставить отпечаток сертификата для использования сертификата, который уже развернут в хранилище сертификатов на серверах инфраструктуры как услуги. При использовании этого параметра сертификат не будет передаваться от виртуального устройства на серверы инфраструктуры как услуги. Это позволяет пользователям развертывать в интерфейсе управления существующие сертификаты на серверах инфраструктуры как услуги без отправки их.

6. Нажмите кнопку **Сохранить настройки**.

Для обновления сертификата Windows-сервера инфраструктуры как услуги требуется, чтобы службы vRealize Automation были надлежащим образом перезапущены. Перезапуск может занять от 15 минут до часа в зависимости от количества устройств vRealize Automation в рабочей среде.

После перезапуска на странице появятся сведения о сертификате.

Замена сертификата службы диспетчера инфраструктуры как услуги

Чтобы обеспечить безопасность в среде распределенного развертывания, системный администратор может заменить сертификат, срок действия которого истек, либо самозаверяющий сертификат сертификатом, выданным центром сертификации.

Сертификат с альтернативным именем субъекта можно использовать на нескольких компьютерах. Сертификаты, используемые для компонентов инфраструктуры как услуги (служба диспетчера и веб-сайта), должны быть выданы со значениями SAN, включая полные доменные имена всех узлов Windows, на которых установлен соответствующий компонент, а также полное доменное имя подсистемы балансировки нагрузки для того же компонента.

В службе диспетчера инфраструктуры как услуги и веб-службе инфраструктуры как услуги используется один сертификат.

Процедура

1. Откройте URL-адрес интерфейса управления устройством vRealize Automation в веб-браузере.
2. Войдите, используя имя пользователя **root** и пароль, указанный при развертывании Устройство vRealize Automation.
3. Выберите **vRA > Сертификаты**.
4. Выберите **Служба диспетчера** в меню **Тип компонента**.
5. Выберите тип сертификата в меню **Действие с сертификатом**.

Если используется сертификат в кодировке PEM, например для распределенной среды, выберите **Импорт**.

Импортируемые сертификаты должны быть доверенными. Убедитесь, что их можно применить ко всем экземплярам устройства vRealize Automation и любой подсистеме балансировки нагрузки при помощи сертификатов с альтернативным именем субъекта (Subject Alternative Name, SAN).

Примечание Если используются цепочки сертификатов, укажите сертификаты в следующем порядке:

- а) сертификат клиента или сервера, подписанный промежуточным сертификатом центра сертификации;
- б) промежуточные сертификаты (один или несколько);
- в) корневой сертификат центра сертификации.

Параметр	Описание
Сохранить существующую	Сохраните текущую конфигурацию SSL. Выберите этот параметр, чтобы отменить изменения.
Создать сертификат	<ul style="list-style-type: none"> а) Значение, отображаемое в текстовом поле Обычное имя, является именем узла, которое отображается в верхней части страницы. Если существуют дополнительные экземпляры устройства vRealize Automation, их полные доменные имена включаются в атрибут SAN сертификата. б) В текстовом поле Организация введите название организации, например название своей компании. в) В текстовом поле Организационная единица введите организационную единицу, например название отдела или расположение. г) В текстовом поле Страна введите двухбуквенный код страны ISO 3166, например RU.
Импорт	<ul style="list-style-type: none"> а) Скопируйте значения сертификата, начиная с заголовка BEGIN PRIVATE KEY до нижнего колонтитула END PRIVATE KEY включительно, и вставьте их в текстовое поле Закрытый ключ RSA. б) Скопируйте значения сертификата, начиная с заголовка BEGIN CERTIFICATE до нижнего колонтитула END CERTIFICATE включительно, и вставьте их в текстовое поле Цепочка сертификатов. Для нескольких значений сертификатов добавьте заголовок BEGIN PRIVATE KEY и нижний колонтитул END PRIVATE KEY в каждый сертификат. <p>Примечание В цепочках сертификатов могут быть доступны дополнительные атрибуты.</p> <ul style="list-style-type: none"> в) (Необязательно.) Если сертификат использует парольную фразу для шифрования ключа, скопируйте ее и вставьте в текстовое поле Парольная фраза.
Предоставить отпечаток сертификата	Используйте этот параметр, если необходимо предоставить отпечаток сертификата для использования сертификата, который уже развернут в хранилище сертификатов на серверах инфраструктуры как услуги. При использовании этого параметра сертификат не будет передаваться от виртуального устройства на серверы инфраструктуры как услуги. Это позволяет пользователям развертывать в интерфейсе управления существующие сертификаты на серверах инфраструктуры как услуги без отправки их.

6. Нажмите кнопку **Сохранить настройки**.

Через несколько минут на странице появятся сведения о сертификате.

7. Если это требуется для вашей сети или подсистемы балансировки нагрузки, скопируйте импортированный или новый созданный сертификат в подсистему балансировки нагрузки.
8. Откройте браузер и перейдите по адресу <https://managerServiceAddress/vmpsProvision/> с сервера, на котором запущен рабочий процесс или агент DEM.

В случае использования подсистемы балансировки нагрузки имя узла должно быть полным доменным именем подсистемы балансировки нагрузки.

9. Пройгнорируйте предупреждения сертификата, если они будут появляться.
10. Проверьте, что новый сертификат предоставлен и является доверенным.
11. При использовании подсистемы балансировки нагрузки стоит настроить и включить применимые проверки работоспособности.

Включение во встроенном vRealize Orchestrator доверия к сертификатам vRealize Automation.

При обновлении или изменении Устройство vRealize Automation или сертификатов инфраструктуры как услуги необходимо настроить в vRealize Orchestrator доверие к новым или обновленным сертификатам.

Данная процедура относится ко всем развертываниям vRealize Automation, в которых используется встроенная копия vRealize Orchestrator. При использовании внешнего экземпляра vRealize Orchestrator см. раздел [Включение во внешнем vRealize Orchestrator доверия к сертификатам vRealize Automation.](#)

Примечание Эта процедура сбрасывает настройки аутентификации арендатора и группы пользователей к значениям по умолчанию. Если вы проводили индивидуальную настройку аутентификации, сохраните информацию об имеющихся настройках, чтобы после завершения процедуры можно было настроить аутентификацию заново.

Сведения об обновлении и замене сертификатов vRealize Orchestrator см. в документации vRealize Orchestrator.

В кластерной конфигурации необходимо выполнить эту процедуру на основном узле устройства vRealize Automation, а затем выполнить команду `join-cluster` для основного узла на каждом узле-реплике устройства vRealize Automation.

Примечание В кластере необходимо остановить службу `vco-configurator` на всех узлах-репликах вплоть до завершения процедуры, чтобы избежать нежелательной автоматической синхронизации центра управления.

При замене или обновлении сертификатов vRealize Automation без выполнения этой процедуры центр управления vRealize Orchestrator может оказаться недоступен и в файлах журнала `vco-server` и `vco-configurator` могут появиться ошибки.

Кроме того, ошибки при обновлении сертификатов могут появиться, если vRealize Orchestrator настроен на аутентификацию для иного арендатора и группы пользователей, нежели vRealize Automation. Дополнительные сведения см. в статье базы знаний VMware [об исключении цепочки недоверенных сертификатов после замены сертификатов vRA \(2147612\)](#).

Описанный здесь синтаксис команды настройки доверия приведен для примера и не является исчерпывающим. Несмотря на то что такой синтаксис подходит для большинства типичных развертываний, в отдельных случаях может потребоваться поэкспериментировать с различными вариациями команд.

- Если задан параметр `--certificate`, необходимо указать путь к допустимому файлу сертификата в формате PEM.
- Если задан параметр `--uri`, необходимо указать URI, от которого команда может получить доверенный сертификат.
- Если задан параметр `--registry-certificate`, необходимо указать, что запрашиваемый сертификат должен обрабатываться как сертификат для реестра компонентов, а доверенный сертификат добавляется в доверенное хранилище под псевдонимом, который используется сертификатом реестра компонента.

Также можно управлять сертификатами с помощью рабочих процессов диспетчера доверия SSL в vRealize Orchestrator. Информацию см. в разделе *Управление сертификатами Orchestrator* в [документации по vRealize Orchestrator](#).

Процедура

1. Остановите сервер vRealize Orchestrator и службы центра управления.

```
service vco-server stop
service vco-configurator stop
```

2. Сбросьте поставщика проверки подлинности vRealize Orchestrator, выполнив следующую команду.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
ls -l /etc/vco/app-server/
mv /etc/vco/app-server/vco-registration-id /etc/vco/app-server/vco-registration-id.old
vcac-vami vco-service-reconfigure
```

3. Проверьте доверенный сертификат для доверенного хранилища vRealize Orchestrator с помощью программы интерфейса командной строки, которая находится в папке `/var/lib/vco/tools/configuration-cli/bin`, выполнив следующую команду.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

- Проверьте сертификат с помощью следующего псевдонима: `vco.cafe.component-registry.ssl.certificate`. Это должен быть сертификат vRealize Automation, который используется экземпляром vRealize Orchestrator в качестве поставщика проверки подлинности.

- Этот сертификат должен совпадать с только что настроенным сертификатом vRealize Automation. Если он не совпадает, его можно изменить следующим образом.
1. Скопируйте PEM-файл сертификата устройства, подписанный vRealize Automation, в папку /tmp на устройстве.
 2. Выполните следующую команду, добавив соответствующий путь сертификата.

```
./vro-configure.sh trust --certificate path-to-the-certificate-file-in-PEM-format--registry-certificate
```

См. приведенный ниже пример команды.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --certificate /var/tmp/test.pem --registry-certificate
```

4. Возможно, потребуется выполнить следующие команды, чтобы сделать сертификат доверенным.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --uri https://vra.domain.com  
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh trust --registry-certificate --uri https://vra.domain.com
```

5. Убедитесь, что сертификат vRealize Automation теперь вставляется в доверенное хранилище vRealize Orchestrator, выполнив следующую команду.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh list-trust
```

6. Запуск сервера vRealize Orchestrator и служб центра управления.

```
service vco-server start  
service vco-configurator start
```

Следующие шаги

Можно проверить, обновлены ли отношения доверия в кластерной системе.

1. Выполните вход в интерфейс управления виртуальным устройством с учетными данными пользователя root.
2. Перейдите на страницу «Службы» (Services).
3. Убедитесь, что в списке нет дублирующихся служб vCO.

Если в списке есть дублирующиеся службы vCO, выберите **Отменить регистрацию**, чтобы удалить службы, которым не назначено состояние Registered.
4. Убедитесь, что служба vco-configurator запущена на всех узлах виртуального устройства.
5. Войдите в центр управления vRealize Orchestrator и перейдите на страницу «Проверка конфигурации» (Validate Configuration), чтобы проверить конфигурацию.
6. Перейдите на страницу «Поставщик проверки подлинности» (Authentication Provider) и убедитесь в том, что параметры проверки подлинности заданы правильно.

На этой странице также можно протестировать учетные данные для входа.

Включение во внешнем vRealize Orchestrator доверия к сертификатам vRealize Automation.

При обновлении или изменении Устройство vRealize Automation или сертификатов инфраструктуры как услуги необходимо настроить в vRealize Orchestrator доверие к новым или обновленным сертификатам.

Данная процедура относится к тем развертываниям vRealize Automation, в которых используется внешняя копия vRealize Orchestrator.

Примечание Эта процедура сбрасывает настройки аутентификации арендатора и группы пользователей к значениям по умолчанию. Если вы проводили индивидуальную настройку аутентификации, сохраните информацию об имеющихся настройках, чтобы после завершения процедуры можно было настроить аутентификацию заново.

Сведения об обновлении и замене сертификатов vRealize Orchestrator см. в документации vRealize Orchestrator.

При замене или обновлении сертификатов vRealize Automation без выполнения данной процедуры центр управления vRealize Orchestrator может оказаться недоступен. Также могут возникнуть ошибки в файлах журнала vco-server и vco-configurator.

Кроме того, ошибки при обновлении сертификатов могут появиться, если vRealize Orchestrator настроен на аутентификацию для иного арендатора и группы пользователей, нежели vRealize Automation. См. [статью базы знаний 2147612](#).

Процедура

1. Остановите сервер vRealize Orchestrator и службы центра управления.

```
service vco-configurator stop
```

2. Произведите сброс поставщика аутентификации vRealize Orchestrator.

```
/var/lib/vco/tools/configuration-cli/bin/vro-configure.sh reset-authentication
```

3. Запустите службу центра управления vRealize Orchestrator.

```
service vco-configurator start
```

4. Войдите в центр управления, используя учетные данные пользователя root интерфейса управления виртуальными устройствами.

5. Отмените регистрацию поставщика аутентификации и произведите ее повторно.

Обновление сертификата сайта управления устройством vRealize Automation

Системный администратор может заменить сертификат SSL службы управления средой или заменить самозаверяющий сертификат на подписанный центром сертификации. Необходимо обеспечить безопасность службы сайта управления с использованием порта 5480.

Устройство vRealize Automation использует сервер `lighttpd` для работы собственного сайта управления. После замены сертификата среды управления необходимо настроить все агенты управления, чтобы они распознавали новый сертификат.

При распределенном развертывании агенты управления можно обновить автоматически или вручную. При минимальном развертывании необходимо обновить агент управления вручную.

Дополнительные сведения см. в разделе [Обновление агента управления в ручном режиме для распознавания сертификата](#).

Процедура

1. Поиск идентификатора агента управления

Идентификатор агента управления используется при создании и регистрации нового сертификата сервера сайта управления.

2. Замена сертификата сайта управления устройством vRealize Automation

Если срок действия сертификата SSL для службы сайта управления истекает или работа начата с использованием самозаверяющего сертификата, а для политик сайта требуется другой сертификат, можно заменить сертификат.

3. Обновление агента управления для распознавания сертификата

После того как сертификат для среды управления устройствами vRealize Automation будет заменен, потребуется обновить все агенты управления, чтобы обеспечить распознавание нового сертификата и восстановить доверие между средой управления виртуальными устройствами и агентами управления на узлах Инфраструктура как услуга.

Поиск идентификатора агента управления

Идентификатор агента управления используется при создании и регистрации нового сертификата сервера сайта управления.

Процедура

1. Откройте файл конфигурации агента управления, который находится в папке `<vra-installation-dir>\Management Agent\VMware.IaaS.Management.Agent.exe.config`.

2. Запишите значение атрибута `id` для элемента `agentConfiguration`.

```
<agentConfiguration id="0E22046B-9D71-4A2B-BB5D-70817F901B27">
```

Замена сертификата сайта управления устройством vRealize Automation

Если срок действия сертификата SSL для службы сайта управления истекает или работа начата с использованием самозаверяющего сертификата, а для политик сайта требуется другой сертификат, можно заменить сертификат.

Разрешено повторно воспользоваться сертификатом, используемым службой vRealize Automation на порте 443, или использовать другой сертификат. Если запрашивается новый сертификат, выданный центром сертификации, чтобы обновить существующий сертификат, рекомендуется повторно использовать общее имя из существующего сертификата.

Примечание Устройство vRealize Automation использует сервер `lighttpd` для работы собственного сайта управления. Необходимо обеспечить безопасность службы сайта управления с использованием порта 5480.

Необходимые условия

- У файлов сертификатов должен быть формат PEM.
- В одном файле сертификата должны содержаться следующие данные.
 - а) Закрытый ключ RSA
 - б) Цепочка сертификатов
- Закрытый ключ невозможно зашифровать.
- Имя файла и расположение по умолчанию: `/opt/vmware/etc/lighttpd/server.pem`.

Дополнительные сведения об экспорте сертификата и закрытого ключа из хранилища ключей Java в PEM-файл см. в разделе [Извлечение сертификатов и закрытых ключей](#).

Процедура

1. Войдите в систему, используя консоль устройства или протокол SSH.
2. Сделайте резервную копию текущего файла сертификата.

```
cp /opt/vmware/etc/lighttpd/server.pem /opt/vmware/etc/lighttpd/server.pem-bak
```

3. Скопируйте созданный сертификат для своего устройства, заменив содержимое файла `/opt/vmware/etc/lighttpd/server.pem` предоставленными сведениями о новых сертификатах.
4. Чтобы перезапустить сервер `lighttpd`, выполните следующую команду.


```
service vami-lighttp restart
```
5. Чтобы перезапустить службу `haproxy`, выполните следующую команду.


```
service haproxy restart
```
6. Войдите в консоль управления и проверьте, заменен ли сертификат. Возможно потребуется перезапустить браузер.

Следующие шаги

Обновите все агенты управления для распознавания нового сертификата.

При распределенном развертывании агенты управления можно обновить вручную или автоматически. В случае минимальных установок необходимо обновить агенты вручную.

- Дополнительные сведения об автоматическом обновлении см. в разделе [Автоматическое обновление агентов управления в распределенной среде для распознавания сертификата среды управления устройства vRealize Automation](#)
- Дополнительные сведения об автоматическом обновлении см. в разделе [Обновление агента управления в ручном режиме для распознавания сертификата](#).

Обновление агента управления для распознавания сертификата

После того как сертификат для среды управления устройствами vRealize Automation будет заменен, потребуется обновить все агенты управления, чтобы обеспечить распознавание нового сертификата и восстановить доверие между средой управления виртуальными устройствами и агентами управления на узлах Инфраструктура как услуга.

На каждом узле Инфраструктура как услуга работает агент управления, поэтому необходимо обновить каждый агент. Минимальные развертывания необходимо обновлять вручную, в то время как распределенные развертывания можно обновлять вручную или с помощью автоматизированного процесса.

■ Обновление агента управления в ручном режиме для распознавания сертификата

После того как сертификат для среды управления устройствами vRealize Automation будет заменен, потребуется обновить агенты управления вручную, чтобы обеспечить распознавание нового сертификата и восстановить доверие между средой управления виртуальными устройствами и агентами управления на узлах Инфраструктура как услуга.

■ Автоматическое обновление агентов управления в распределенной среде для распознавания сертификата среды управления устройства vRealize Automation

После обновления сертификата среды управления в развертывании с высоким уровнем доступности необходимо также обновить конфигурацию агента управления, чтобы выполнить распознавание нового сертификата и восстановить надежную передачу данных.

Обновление агента управления в ручном режиме для распознавания сертификата

После того как сертификат для среды управления устройствами vRealize Automation будет заменен, потребуется обновить агенты управления вручную, чтобы обеспечить распознавание нового сертификата и восстановить доверие между средой управления виртуальными устройствами и агентами управления на узлах Инфраструктура как услуга.

После того как сертификат для среды управления устройствами vRealize Automation будет заменен, выполните следующие шаги для каждого агента управления в развертывании.

При распределенном развертывании агенты управления можно обновить вручную или автоматически. Дополнительные сведения об автоматическом обновлении см. в разделе [Автоматическое обновление агентов управления в распределенной среде для распознавания сертификата среды управления устройства vRealize Automation](#)

Необходимые условия

Получите отпечатки SHA1 нового сертификата для среды управления устройствами vRealize Automation.

Процедура

1. Остановите работу службы агента управления VMware vCloud Automation Center.
2. Перейдите к файлу конфигурации агента управления с таким расположением:
`[vcac_installation_folder]\Management Agent\VMware.IaaS.Management.Agent.exe.Config`. Обычно он расположен по такому пути:
`C:\Program Files (x86)\VMware\VCAC\Management Agent\VMware.IaaS.Management.Agent.exe.Config`.
3. Откройте файл, чтобы редактировать его, и найдите параметр конфигурации конечной точки прежнего сертификата среды управления. Его можно определить по адресу конечной точки.

Пример:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="D1542471C30A9CE694A512C5F0F19E45E6FA32E6" />
  </managementEndpoints>
</agentConfiguration>
```

4. Замените отпечаток на отпечаток SHA1 нового сертификата.

Пример:

```
<agentConfiguration id="C816CFBC-4830-4FD2-8951-C17429CEA291" pollingInterval="00:03:00">
  <managementEndpoints>
    <endpoint address="https://vra-va.local:5480"
thumbprint="8598B073359BAE7597F04D988AD2F083259F1201" />
  </managementEndpoints>
</agentConfiguration>
```

5. Запустите службу агента управления VMware vCloud Automation Center.
6. Войдите в среду управления виртуальным устройством и откройте вкладку **Кластер**.
7. Просмотрите таблицу «Сведения о распределенном развертывании», чтобы убедиться, что сервер Инфраструктура как услуга недавно обменивался данными с виртуальным устройством. Факт обмена подтверждает успешное обновление.

Автоматическое обновление агентов управления в распределенной среде для распознавания сертификата среды управления устройства vRealize Automation

После обновления сертификата среды управления в развертывании с высоким уровнем доступности необходимо также обновить конфигурацию агента управления, чтобы выполнить распознавание нового сертификата и восстановить надежную передачу данных.

Обновить сведения о сертификате среды управления устройства vRealize Automation для распределенных систем можно как вручную, так и автоматически. Дополнительные сведения об обновлении агентов управления вручную см. в разделе [Обновление агента управления в ручном режиме для распознавания сертификата](#).

Выполните эти действия, чтобы обеспечить автоматическое обновление сведений о сертификате.

Процедура

1. Во время использования агентов управления необходимо заменить сертификат в одной среде управления устройства vRealize Automation в развертывании.
2. Подождите пятнадцать минут, пока не завершится синхронизация сертификата агента управления с новым сертификатом среды управления устройства vRealize Automation.
3. Замените сертификаты в других средах управления устройства vRealize Automation в развертывании.

Параметры сертификата будут автоматически обновлены в агентах управления.

Замена сертификата агента управления

Системный администратор может заменить сертификат агента управления по истечении срока действия или заменить самозаверяющий сертификат на сертификат, выданный центром сертификаций.

Каждый узел инфраструктуры как услуги использует свой агент управления. Выполните эту процедуру для каждого узла инфраструктуры как услуги, агент управления которого нужно обновить.

Необходимые условия

- Прежде чем удалить запись, скопируйте идентификатор агента управления, указанный в столбце «Идентификатор узла». Этот идентификатор можно использовать при создании нового сертификата агента управления, а также при его регистрации.
- Запрашивая новый сертификат, убедитесь, что в поле субъекта нового сертификата атрибут обычного имени (CN) введен в таком формате:

```
VMware Management Agent 00000000-0000-0000-0000-000000000000
```

Введите строку, которая начинается с VMware Management Agent, после чего следует пробел и идентификатор GUID агента управления в числовом формате, как показано выше.

Процедура

1. Остановите работу службы агента управления из оснастки «Службы Windows».
 - а) На компьютере Windows щелкните меню **Пуск**.
 - б) В поле поиска, расположенном в меню «Пуск» системы Windows, введите команду **services.msc** и нажмите клавишу ВВОД.
 - в) Щелкните правой кнопкой мыши службу **Агент управления VMware vCloud Automation Center**, а затем выберите **Остановить**, чтобы остановить работу службы.

2. Удалите текущий сертификат на компьютере. Дополнительные сведения об управлении сертификатами в Windows Server 2008 R2 см. в статье базы знаний Майкрософт по адресу <http://technet.microsoft.com/en-us/library/cc772354.aspx> или вики-статье Майкрософт по адресу <http://social.technet.microsoft.com/wiki/contents/articles/2167.how-to-use-the-certificates-console.aspx>.
 - а) Введите команду **mmc.exe**, чтобы открыть консоль управления Microsoft.
 - б) Нажмите Ctrl+M, чтобы добавить новую оснастку в консоль, или выберите соответствующий пункт из раскрывающегося меню «Файл».
 - в) Выберите пункт **Сертификаты** и нажмите кнопку **Добавить**.
 - г) Выберите **Учетная запись компьютера** и нажмите **Далее**.
 - д) Выберите **Локальный компьютер: (компьютер, на котором запущена данная консоль)**.
 - е) Нажмите кнопку **ОК**.
 - ж) Разверните узел **Сертификаты (локальный компьютер)** в левой части консоли.
 - з) Разверните узел **Личные** и выберите папку «Сертификаты».
 - и) Выберите текущий сертификат агента управления и нажмите кнопку **Удалить**.
 - к) Нажмите кнопку **Да**, чтобы подтвердить удаление.
3. Импортируйте недавно созданный сертификат в локальное хранилище `computer.personal` или не импортируйте ничего, если необходимо, чтобы система автоматически создавала новый самоподписанный сертификат.

4. Зарегистрируйте сертификат агента управления на сайте управления для устройства vRealize Automation.

- а) Откройте командную строку в качестве администратора и перейдите к каталогу Cafe, расположенному на компьютере, на котором установлен агент управления:
<каталог_установки_vra>\Management Agent\Tools\Cafe, как правило, C:\Program Files (x86)\VMware\VCAC\Management Agent\Tools\Cafe.
- б) Введите команду Vcac-Config.exe RegisterNode с параметрами для регистрации идентификатора агента управления и сертификата за один шаг. Введите записанный ранее идентификатор агента управления в качестве значения параметра -nd.

Таблица 1-3. Требуемые параметры и аргументы для Vcas-Config.exe RegisterNode

Параметр	Аргумент	Примечания
-vamih	" <i>имя_узла_виртуального_устройства_vra.домен.имя:5480</i> "	URL-адрес узла сайта управления со спецификацией порта.
-cu	"root"	Имя пользователя, который должен быть пользователем root.
-cp	" <i>пароль</i> "	Пароль пользователя root в кавычках.
-hn	" <i>имя_узла_компьютера.домен.имя</i> "	Имя компьютера узла агента управления со сведениями о домене. Это значение должно совпадать с именем узла, с которым зарегистрирован текущий узел в Устройство vRealize Automation. Его можно увидеть, задав указанный выше параметр 1 для идентификатора узла или в VAMI, таблице сведений о распределенном развертывании. Если это значение не совпадает, то при выполнении команды будет выведено сообщение об ошибке: «Ошибка: невозможно добавить повторяющийся идентификатор узла 00000000-0000-0000-0000-00000000».
-nd	" <i>00000000-0000-0000-0000-000000000000</i> "	Идентификатор агента управления.
-tp	" <i>00</i> "	Отпечаток пальца сертификата SSL узла сайта управления, как определено в параметре -vamih.

В следующем примере показан формат команды:

```
Vcac-Config.exe RegisterNode -v -vamih "vra-vr-hostname.domain.name:5480"  
-cu "root" -cp "password" -hn "machine-hostname.domain.name"  
-nd "00000000-0000-0000-0000-000000000000"  
-tp "00000000000000000000000000000000000000000000000000"
```

5. Перезапустите агент управления.

Пример. Команда для регистрации сертификата агента управления

```
Vcac-Config.exe RegisterNode -v -vamih "vra-va.eng.mycompany:5480" -cu "root" -cp "secret" -hn "iaas.eng.mycompany" -nd "C816CFBX-4830-4FD2-8951-C17429CEA291" -tp "70928851D5B72B206E4B1CF9F6ED953EE1103DED"
```

Изменение метода опроса для сертификатов

Если в разделе ОУ («организационная единица») сертификата инфраструктуры как услуги есть запятые, в файлах журнала службы диспетчера могут возникнуть ошибки STOMP WebSocket. Кроме того, возможны сбои при предоставлении виртуальных машин. В этом случае можно удалить запятые или изменить метод опроса WebSocket на HTTP.

Чтобы изменить метод опроса, выполните следующие действия.

Процедура

1. Откройте следующий файл в текстовом редакторе.

C:\Program Files (x86)\VMware\vCAC\Server\Manager Service.exe.config.

2. Добавьте следующие строки в раздел <appSettings>.

```
<add key="Extensibility.Client.RetrievalMethod" value="Polling"/>
<add key="Extensibility.Client.PollingInterval" value="2000"/>
<add key="Extensibility.Client.PollingMaxEvents" value="128"/>
```

3. Сохраните и закройте файл Manager Service.exe.config.

4. Перезапустите службу диспетчера.

Результаты

Дополнительные сведения о службе диспетчера см. в разделе *Установка vRealize Automation*.

Управление базой данных устройства Postgres vRealize Automation

Для работы системы vRealize Automation требуется использование базы данных устройства. Базой данных устройства можно управлять с помощью интерфейса управления виртуальными устройствами vRealize Automation.

Примечание Данная информация относится только к развертываниям, в которых используется встроенная база данных устройств. Она не относится к развертываниям, в которых используется внешняя база данных Postgres.

Базу данных можно настроить в качестве одиночного узла или системы с несколькими узлами, чтобы обеспечить высокую доступность при аварийном переключении. Программа установки vRealize Automation содержит узел базы данных в каждой установке Устройство vRealize Automation. Таким образом, при установке трех экземпляров Устройство vRealize Automation получают три узла базы данных. Автоматическое аварийное переключение внедрено в соответствующих развертываниях. Обслуживание базы данных устройств требуется только в случае изменения конфигурации компьютера или при повышении другого узла до уровня основного при использовании кластерной конфигурации.

Примечание Кластерная конфигурация базы данных настраивается автоматически во время присоединения виртуального устройства к кластеру с использованием операции «Присоединить к кластеру». Кластер базы данных не зависит непосредственно от кластера виртуальных устройств. Например, виртуальная машина, присоединенная к кластеру, может работать нормально, даже если встроенная база данных устройств не запущена или в ней случился сбой.

Для обеспечения высокой доступности в vRealize Automation используется модель основной реплики PostgreSQL, обеспечивающая репликацию данных. Это означает, что все узлы базы данных работают в кластере с одним ведущим узлом, называемым основным, и несколькими реплицирующими узлами, называемыми репликами. Основной узел обрабатывает все запросы к базе данных, а узлы-реплики выполняют потоковую передачу и воспроизводят основного узла локально.

Кластерная конфигурация содержит один основной узел и один или несколько узлов-реплик. Основной узел — это узел устройства vRealize Automation, где находится основная база данных, поддерживающая работу системных функций. На узлах-репликах содержатся копии базы данных, которые можно использовать, если на основном узле произойдет сбой.

Существует несколько вариантов базы данных устройств с высокой доступностью. При настройке базы данных очень важной является операция выбора режима репликации. Режим репликации влияет на целостность данных развертывания vRealize Automation и определяет способ аварийного переключения для конфигурации высокой доступности при сбое основного узла. Существует два режима репликации: синхронный и асинхронный.

Оба режима поддерживают аварийное переключение базы данных, но у каждого из них есть свои преимущества и недостатки. Для поддержки аварийного переключения базы данных с высокой доступностью в асинхронном режиме требуются два узла, а в синхронном режиме — три. Синхронный режим также вызывает автоматическое аварийное переключение.

Режим репликации	Преимущества	Недостатки
Синхронный	<ul style="list-style-type: none"> ■ Минимизирует риск потери данных. ■ Вызывает автоматическое переключение. 	<ul style="list-style-type: none"> ■ Может повлиять на производительность системы. ■ Требуются три узла.
Асинхронный	<ul style="list-style-type: none"> ■ Требуется всего два узла. ■ Оказывает меньшее влияние на производительность системы, чем синхронный режим. 	<ul style="list-style-type: none"> ■ Не такой надежный в предотвращении потери данных, как синхронный режим.

vRealize Automation поддерживает оба режима, но по умолчанию работает в асинхронном режиме и обеспечивает высокую доступность только при наличии по крайней мере двух узлов базы данных устройства. На вкладке **Кластер** в интерфейсе управления виртуальным устройством можно переключать режимы синхронизации и добавлять узлы базы данных по необходимости.

Во время работы в синхронном режиме vRealize Automation вызывает операцию автоматического восстановления после отказа.

Если сначала используются один узел и конфигурация невысокой доступности, позже при необходимости увеличения доступности можно добавить больше узлов. При наличии соответствующего оборудования и необходимости максимально предотвратить потерю данных лучше выбрать синхронный режим развертывания.

Аварийное переключение базы данных устройства

В конфигурации высокой доступности основной узел в потоковом режиме передает транзакции на серверы-реплики. При сбое в работе основного узла активная и работающая реплика готова продолжить работу с запросами «только для чтения». Когда назначается новый основной узел (вручную или автоматически), все предстоящие запросы перемещаются на него.

Настройка базы данных устройств

Для мониторинга или обновления конфигурации базы данных устройств можно использовать страницу «База данных интерфейса управления виртуальными устройствами». Кроме того, на данной странице можно изменять назначение основного узла и режим синхронизации, используемый базой данных.

Установка и настройка базы данных устройств выполняется во время установки и настройки системы vRealize Automation, но контролировать и изменять конфигурацию можно на вкладке **База данных** в интерфейсе управления виртуальными устройствами.

В текстовом поле **Состояние подключения** указывается, подключена ли база данных к системе vRealize Automation и правильно ли она функционирует.

Если ваша база данных устройств использует несколько узлов для поддержки аварийного переключения, в таблице в нижней части страницы указываются узлы, их состояние, а также основной узел. В текстовом поле **Режим репликации** указывается текущий настроенный режим работы для системы (синхронный или асинхронный). На этой странице можно обновлять конфигурацию базы данных устройств.

В столбце «Состояние синхронизации*» в таблице узлов базы данных указывается метод синхронизации для кластера. Этот столбец вместе со столбцом «Состояние» позволяет показать состояние кластерных узлов. Потенциальное (potential) состояние может быть разным в зависимости от того, используется ли для кластера асинхронная или синхронная репликация.

Таблица 1-4. Состояние синхронизации для режимов репликации базы данных устройств

Режим	Сообщение о состоянии синхронизации
Синхронная репликация	Основной узел — состояние не указано Узел реплики — синхронизация Другие узлы — потенциальное
Асинхронная репликация	Основной узел — состояние не указано Другие узлы — потенциальное

В столбце «Допустимый» указывается, синхронизированы ли реплики с основным узлом. Основной узел всегда является допустимым.

В столбце «Приоритет» указывается положение узлов-реplik относительно основного узла. Основной узел не имеет значения приоритета. При повышении статуса реплики до основного узла выберите узел с наименьшим приоритетом.

Во время работы в синхронном режиме vRealize Automation вызывает операцию автоматического восстановления после отказа. В случае отказа основного узла новым основным узлом автоматически становится следующий доступный узел-реплика. В стандартном развертывании vRealize Automation операция восстановления после отказа занимает от 10 до 30 секунд.

Необходимые условия

- Установите и настройте vRealize Automation, следуя соответствующим инструкциям в разделе *Установка vRealize Automation*.
- Войдите в интерфейс управления устройства vRealize Automation в качестве **пользователя root** с помощью пароля, введенного вами при развертывании устройства vRealize Automation.
- Настройте соответствующий кластер встроенной базы данных устройства Postgres как часть своего развертывания vRealize Automation.

Процедура

1. В интерфейсе управления виртуальными устройствами последовательно выберите **Настройки vRA > База данных**.
2. Если ваша база данных использует несколько узлов, просмотрите таблицу в нижней части страницы и убедитесь, что система функционирует надлежащим образом.
 - Убедитесь, что перечислены все узлы.
 - Убедитесь, что соответствующий узел указан как основной.

Примечание Не нажимайте кнопку **Режим синхронизации** для изменения режима синхронизации базы данных, если вы не уверены в безопасности своих данных. Изменение режима синхронизации без подготовки может привести к потере данных.

3. Чтобы сделать основным один из узлов, щелкните **Повысить** в соответствующем столбце.
4. Щелкните **Сохранить настройки** для сохранения конфигурации, если были внесены изменения.

Сценарии автоматического аварийного переключения базы данных устройства при сбое в работе трех узлов

Есть несколько сценариев аварийного переключения базы данных устройства для обеспечения высокой доступности. В каждом из них поведение vRealize Automation зависит от конфигурации базы данных устройства и количества узлов, в работе которых происходит сбой.

Сценарии, в которых отказ затрагивает один узел

Если в работе одного из трех узлов происходит сбой, vRealize Automation инициирует автоматическое аварийное переключение. Дополнительные операции автоматического аварийного переключения не могут выполняться, пока не восстановлены все три узла.

В следующей таблице описаны поведение и действия, связанные со сбоем в работе основного узла в развертывании с высокой доступностью.

Таблица 1-5. Сбой основного узла

Ожидаемое поведение	<ul style="list-style-type: none"> ■ Настроенный синхронный узел-реплика становится основным и автоматически берет на себя выполнение функций базы данных устройства. ■ Потенциальная синхронная реплика становится синхронным резервным узлом. ■ Развертывание vRealize Automation работает в режиме «только чтение» до завершения автоматического аварийного переключения.
Дальнейшие действия	<ul style="list-style-type: none"> ■ После восстановления узла, бывшего раньше основным, логика восстановления агента аварийного переключения автоматически сбросит состояние этого узла и сделает его репликой. Вручную ничего не нужно делать. ■ Если предыдущий основной узел не подлежит восстановлению, вручную переведите базу данных устройства в асинхронный режим.

В следующей таблице описаны поведение и действия, связанные со сбоем в работе синхронного узла-реплики в развертывании с высокой доступностью.

Таблица 1-6. Сбой синхронного узла-реплики

Ожидаемое поведение	<ul style="list-style-type: none"> ■ Развертывание vRealize Automation не простаивает. До того как потенциальная реплика станет новой синхронной репликой, для выполнения запросов базы данных потребуется небольшая задержка. База данных устройства автоматически выполняет это действие.
Дальнейшие действия	<ul style="list-style-type: none"> ■ Когда бывшая синхронная реплика возвращается в рабочее состояние, она автоматически становится потенциальной репликой. Вручную ничего не нужно делать. ■ Если бывшая синхронная реплика не подлежит восстановлению, вручную переведите базу данных устройства в асинхронный режим.

В следующей таблице описаны поведение и действия, связанные со сбоем в работе основного узла в развертывании с высокой доступностью.

Таблица 1-7. Сбой потенциальной реплики

Ожидаемое поведение	Развертывание не простаивает.
Дальнейшие действия	<ul style="list-style-type: none"> ■ Когда бывшая потенциальная реплика возвращается в рабочее состояние, она автоматически становится потенциальной репликой. Вручную ничего не нужно делать. ■ Если бывшая потенциальная реплика не подлежит восстановлению, переведите базу данных устройства в асинхронный режим.

Сценарии, в которых сбой затрагивает два узла

Если сбой одновременно происходит в работе двух из трех узлов, vRealize Automation переходит в режим «только чтение», в котором находится до тех пор, пока узлы не будут восстановлены вручную.

В следующей таблице описаны поведение и действия, связанные со сбоем в работе основного узла и потенциального узла-реплики в развертывании с высокой доступностью.

Таблица 1-8. Сбой основного узла и потенциального узла-реплики

Ожидаемое поведение	<ul style="list-style-type: none"> ■ Уровень синхронной реплики не повышается автоматически до уровня основного узла. vRealize Automation работает в режиме «только чтение», поскольку позволяет обрабатывать транзакции со свойством «только чтение» до тех пор, пока уровень не будет повышен вручную.
Дальнейшие действия	<ul style="list-style-type: none"> ■ Нужно вручную повысить уровень. Переведите базу данных устройства в асинхронный режим. ■ После восстановления основного узла и потенциального узла-реплики переведите их вручную в режим синхронизации с новым основным узлом. На этом этапе vRealize Automation можно вернуть в синхронный режим. ■ Если два из трех узлов отключатся одновременно, vRealize Automation переходит в режим «только чтение», в котором находится до тех пор, пока узлы не будут восстановлены вручную. Если доступен только один узел базы данных, переведите развертывание в асинхронный режим.

В следующей таблице описаны поведение и действия, связанные со сбоем в работе синхронного и потенциального узлов в развертывании с высокой доступностью.

Таблица 1-9. Сбой синхронной и потенциальной реплик

Ожидаемое поведение	<ul style="list-style-type: none"> ■ vRealize Automation работает в режиме «только чтение», поскольку позволяет обрабатывать транзакции со свойством «только чтение» до тех пор, пока не будет выполнено восстановление вручную.
Дальнейшие действия	<ul style="list-style-type: none"> ■ Нужно вручную повысить уровень. Переведите базу данных устройства в асинхронный режим. ■ После восстановления синхронной и потенциальной реплик их нужно сбросить вручную, чтобы они синхронизировались с основным узлом. На этом этапе vRealize Automation можно вернуть в синхронный режим. ■ Если два из трех узлов отключатся одновременно, vRealize Automation переходит в режим «только чтение», в котором находится до тех пор, пока узлы не будут восстановлены вручную. Если доступен только один узел базы данных, переведите развертывание в асинхронный режим.

Сбой связи между узлами

Если в связи между узлами из распределенного развертывания происходит сбой, агент автоматического аварийного переключения пытается восстановить конфигурацию.

В следующей таблице описаны поведение и действия, связанные со сбоем связи между двумя площадками в развертывании высокой доступности с заданной конфигурацией, когда все узлы остаются в работоспособном состоянии.

Площадка А: основной узел и потенциальная реплика

Площадка Б: синхронный узел-реплика

Таблица 1-10. Сбой связи между двумя площадками при сохранении работоспособности всех узлов

Ожидаемое поведение	Развертывание vRealize Automation не простаивает. Потенциальная реплика автоматически становится синхронной.
Дальнейшие действия	Вручную ничего не нужно делать.

В следующей таблице описаны поведение и действия, связанные со сбоем связи между двумя площадками в развертывании высокой доступности с заданной конфигурацией, когда все узлы остаются в работоспособном состоянии.

Площадка А: основной узел

Площадка Б: синхронный и потенциальный узлы-реплики

Таблица 1-11. Сбой связи между двумя площадками при сохранении работоспособности всех узлов: альтернативная конфигурация

Ожидаемое поведение	Синхронный узел-реплика становится основным и автоматически берет на себя выполнение функций базы данных устройства. Агент автоматического аварийного переключения повышает уровень потенциального узла-реплики, делая этот узел новым синхронным узлом-репликой. Пока это повышение не завершается, развертывание vRealize Automation работает в режиме «только чтение».
Дальнейшие действия	Вручную ничего не нужно делать. Когда связь восстанавливается, агент автоматического аварийного переключения сбрасывает предыдущий основной узел и делает его узлом-репликой.

Сценарий: аварийное переключение базы данных устройств vRealize Automation вручную

При возникновении проблем с базой данных Postgres устройства vRealize Automation необходимо вручную выполнить аварийное переключение на узел устройства vRealize Automation реплики в кластере.

Выполните эти действия, если на основном узле устройства vRealize Automation произойдет сбой или остановка базы данных Postgres.

Примечание После того как узел выйдет из строя, не используйте его интерфейс управления виртуальным устройством ни для каких процессов, в том числе для аварийного переключения.

Необходимые условия

- Настройте кластер узлов устройства vRealize Automation. На каждом узле размещена копия встроенной базы данных устройств Postgres.

Процедура

1. Удалите IP-адрес основного узла из внешней подсистемы балансировки нагрузки.
2. Выполните вход в интерфейс управления устройства vRealize Automation как пользователь root.
<https://vrealize-automation-appliance-FQDN:5480>
3. Выберите **Кластер**.
4. В списке узлов базы данных найдите узел реплики с наименьшим приоритетом.
Узлы реплик отображаются в порядке возрастания приоритета.
5. Нажмите кнопку **Повысить** и подождите завершения операции.
После завершения операции узел-реплика будет указан в списке как основной.
6. Исправьте ошибки, которые возникли на предыдущем основном узле, и снова добавьте его в кластер.
 - а) Изолируйте предыдущий основной узел.

Отключите узел от его текущей сети, которая проводит соединение с оставшимися узлами устройства vRealize Automation. Выберите другой сетевой адаптер для управления или управляйте им непосредственно с консоли управления виртуальными машинами.

- б) Восстановите предыдущий основной узел.

Включите узел или другим способом устраните проблему. Например, можно сбросить виртуальную машину, если она не отвечает.

- в) Из сеанса консоли как пользователь root остановите службу vpostgres.

```
service vpostgres stop
```

- г) Добавьте основной узел обратно в исходную сеть, которая обеспечивает маршрутизацию на другие узлы устройств vRealize Automation.

- д) Из сеанса консоли как пользователь root перезапустите службу haproxy.

```
service haproxy restart
```

- е) Войдите в интерфейс управления нового основного узла устройства vRealize Automation как пользователь root.

- ж) Выберите **Кластер**.

- з) Найдите предыдущий основной узел и нажмите кнопку **Сбросить**.

- и) После успешного сброса перезапустите предыдущий основной узел.

- к) После включения предыдущего основного узла убедитесь, что работают следующие службы.

```
haproxy horizon-workspace rabbitmq-server vami-lighttpd vcac-server vco-server
```

- л) Снова добавьте предыдущий основной узел во внешнюю подсистему балансировки нагрузки.

Примечание Если основной узел, уровень которого был понижен до реплики, все еще отображается как «основной», возможно, нужно будет вручную повторно добавить его в кластер, чтобы исправить ошибку.

Сценарий: выполнение тестового переключения баз данных

Системный администратор vRealize Automation должен принять меры по обслуживанию и выполнить аварийное переключение базы данных устройства.

В этом сценарии предполагается, что текущий основной узел запущен и работает нормально.

Техобслуживание при аварийном переключении базы данных предусматривает два этапа: обслуживание главного узла и обслуживание узла-реплики. После замены основной узел становится репликой, поэтому нужно выполнить соответствующие действия по обслуживанию, чтобы при необходимости узел можно было снова назначить основным.

Примечание Не останавливайте и не перезапускайте службу HAProxy на соответствующем хост-компьютере, пока выполняется обслуживание при аварийном переключении.

Необходимые условия

- Установка и настройка vRealize Automation в соответствии с инструкциями в руководстве по установке *Установка vRealize Automation*.
- Войдите в интерфейс управления устройства vRealize Automation в качестве **пользователя root** с помощью пароля, введенного вами при развертывании устройства vRealize Automation.
- Установите и настройте соответствующий кластер встроенной базы данных устройств Postgres.
- Если для базы данных используется режим синхронной репликации, в кластере должно быть три активных узла.

Процедура

1. Удалите IP-адрес основного узла из внешней подсистемы балансировки нагрузки.
2. Изолируйте основной узел.

Отключите узел от текущей сети. Это должна быть сеть, выполняющая маршрутизацию в остальные узлы Устройство vRealize Automation.
3. Выберите другой сетевой адаптер для управления или управляйте им непосредственно из интерфейса управления виртуальным устройством.
4. Выберите **Кластер** в интерфейсе управления виртуальными устройствами.
5. Выберите узел-реплику с наименьшим приоритетом для повышения до уровня основного и щелкните **Повысить**.

Узлы реплик отображаются в порядке возрастания приоритета.

Уровень предыдущего основного узла понижен до реплики, а уровень реплики повышен.
6. Выполните соответствующее обслуживание реплики.
7. После завершения обслуживания убедитесь, что виртуальное устройство работает и использует сетевое подключение, а также что работает его служба HAProxy.
 - а) Войдите в консоль управления vRealize Automation в качестве **привилегированного пользователя**.
 - б) Убедитесь, что с узлом реплики удастся проверить связь, что он разрешается по имени и что его актуальное состояние отображается на вкладке **Кластер** в интерфейсе управления виртуальными устройствами.
8. Выберите команду **Сброс** для реплики узла.

Эта операция позволяет сбросить базу данных, чтобы она была настроена для репликации ее данных на основной узел, и повторно синхронизировать конфигурацию узла-реплики с последней конфигурацией HAProxy основного узла.
9. После успешного сброса занесите IP-адрес узла виртуального устройства реплики обратно в пул IP-адресов системы балансировки нагрузки внешнего виртуального устройства.

10. Убедитесь, что данный узел реплики отображается как работоспособный в таблице этой базы данных, что с ним удастся проверить связь и что он разрешается по имени.

Следующие шаги

Исправьте ошибки, которые возникли на предыдущем основном узле, и снова добавьте его в кластер.

Ручное восстановление базы данных устройства после катастрофического сбоя

Если произошел сбой базы данных устройства, после которого не работает ни один ее узел, или после сбоя основного узла нарушена синхронизация всех узлов-реплик, попробуйте восстановить базу данных с помощью следующей процедуры.

Данная процедура подходит для ситуаций, когда в кластере, работающем в несинхронном режиме, нет работоспособных узлов базы данных. В этом случае при попытке загрузить или обновить страницу интерфейса управления виртуальными устройствами обычно возникают ошибки, аналогичные следующим:

```
Error initializing the database service: Could not open JDBC Connection for transaction; nested exception is org.postgresql.util.PSQLException: The connection attempt failed.
```

Процедура

1. Попробуйте восстановить базу данных, используя интерфейс управления виртуальными устройствами с одного из узлов базы данных.
 - а) Если возможно, откройте страницу **Кластер** в интерфейсе управления виртуальными устройствами для узла с наиболее актуальным состоянием. Обычно это узел, который был основным до сбоя базы данных.
 - б) Если не удастся открыть интерфейс управления виртуальными устройствами для основного узла, попробуйте открыть интерфейс для узлов-реплик.
 - в) Если имеется узел базы данных с работоспособным интерфейсом управления виртуальными устройствами, попробуйте восстановить его, выполнив аварийное переключение вручную.
См. раздел [Сценарий: аварийное переключение базы данных устройств vRealize Automation вручную](#).
2. Если не удалось выполнить процедуру, описанную в шаге 1, запустите сеанс оболочки и попробуйте найти узел с самым последним состоянием. Запустите сеанс оболочки для всех доступных узлов кластера и попробуйте запустить базы данных с помощью следующей команды: `service vpostgres start`

3. Используйте следующую процедуру для каждого узла, на котором работает локальная база данных, чтобы определить узел с самым последним состоянием.

- а) Запустите следующую команду, чтобы определить узел с самым последним состоянием: Если при выполнении команды возвращается результат `f`, то это узел с самым последним состоянием, и можно переходить к шагу 4.

```
su - postgres
psql vcac
vcac=# select pg_is_in_recovery();
pg_is_in_recovery
```

- Если при выполнении команды возвращается результат `f`, то это узел с самым последним состоянием.
- Если узел возвращает результат `t`, запустите на этом узле следующую команду:

```
SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location() as
replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
```

Эта команда должна вернуть результат, аналогичный приведенному ниже.

```
vcac=# SELECT pg_last_xlog_receive_location() as receive_loc, pg_last_xlog_replay_location()
as replay_loc, extract(epoch from pg_last_xact_replay_timestamp()) as replay_timestamp;
receive_loc | replay_loc | replay_timestamp
-----+-----+-----
0/200000000 | 0/203228A0 | 1491577215.68858
(1 row)
```

4. Сравните результаты для каждого узла и определите, какой из них находится в самом последнем состоянии.

Выберите узел с наибольшим значением в столбце `receive_loc`. Если значения в этом столбце равны у всех узлов, выберите узел с наибольшим значением в столбце `replay_loc`. Если эти значения также равны для всех узлов, выберите узел с наибольшим значением в столбце `replay_timestamp`.

5. Запустите следующую команду на узле с самым последним состоянием: `vcac-vami psql-promote-master -force`
6. Откройте файл `/etc/haproxy/conf.d/10-psql.cfg` в текстовом редакторе и измените следующую строку,

```
server masterserver sc-rdops-vm06-dhcp-170-156.eng.vmware.com:5432 check on-marked-up shutdown-
backup-sessions
```

указав полное доменное имя текущего узла. Строка должна выглядеть так:

```
server masterserver current-node-fqdn:5432 check on-marked-up shutdown-backup-sessions
```

7. Сохраните файл.
8. Выполните команду `service haproxy restart`.

9. Откройте страницу **Кластер** в интерфейсе управления виртуальными устройствами для узла с наиболее актуальным состоянием.

Этот узел должен отображаться как основной, а остальные узлы — как недопустимые реплики. Для этих реплик также доступна кнопка **Сброс**.

10. Нажимайте **Сброс** поочередно для каждой реплики до тех пор, пока кластер не будет восстановлен.

Резервное копирование и восстановление установок vRealize Automation

Чтобы свести к минимуму время простоя системы и потери данных в случае сбоев, администраторы регулярно создают резервную копию всей установки vRealize Automation. Если в системе происходит сбой, можно использовать для восстановления последнюю известную рабочую резервную копию и переустановить некоторые компоненты.

Сведения о резервном копировании и восстановлении vRealize Automation см. в следующих разделах [документации по vRealize Suite](#):

- Подготовка vRealize Automation к резервному копированию
- vRealize Automation Восстановление системы

Программа улучшения качества программного обеспечения

Этот продукт участвует в программе улучшения качества программного обеспечения (CEIP) от компании VMware. Программа CEIP предоставляет компании VMware сведения, позволяющие улучшить ее продукты и службы VMware, устранить проблемы, а также предоставить рекомендации по наиболее подходящему развертыванию и использованию продуктов. К программе CEIP для vRealize Automation можно присоединиться в любое время. Выйти из нее также можно в любой момент.

Сведения о собранных в CEIP данных и целях их использования в VMware изложены в разделе Trust & Assurance Center на странице <http://www.vmware.com/trustvmware/ceip.html>.

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

К программе улучшения качества программного обеспечения (CEIP) для vRealize Automation можно присоединиться в любое время. Также из нее можно выйти в любой момент.

В vRealize Automation при первоначальной установке и настройке продукта предоставляется возможность присоединиться к программе улучшения качества программного обеспечения (CEIP). После установки можно присоединиться к программе CEIP или выйти из нее. Для этого нужно выполнить описанные ниже действия.

Процедура

1. Войдите в интерфейс управления устройства vRealize Automation как пользователь root.

<https://vrealize-automation-appliance-FQDN:5480>

2. Перейдите на вкладку **Телеметрия**.
3. Установите флажок напротив параметра **Присоединиться к программе улучшения качества программного обеспечения VMware** или снимите его.

Если этот флажок установлен, программа активируется и на адрес <https://vmware.com> отправляются данные.

4. Нажмите кнопку **Сохранить настройки**.

Настройка времени сбора данных

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

Процедура

1. Запустите сеанс консоли устройства vRealize Automation в качестве пользователя 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.

Настройка параметров системы

Системный администратор может настроить ведение журнала и шаблоны сообщений электронной почты инфраструктуры как услуги. Кроме того, можно управлять параметрами, которые отображаются как значения по умолчанию для каждого арендатора, например почтовые серверы для обработки уведомлений. Администраторы арендатора могут переопределить эти значения по умолчанию в соответствии с требованиями арендатора.

Изменение значка «Все службы» в каталоге служб

Можно изменить значок по умолчанию в каталоге служб, чтобы отобразить настраиваемое изображение. Изменения значка отражаются для всех арендаторов, В каталоге нельзя настроить значок для конкретного арендатора.

Команды предназначены для Linux, Mac и Windows, так что можно запускать команды cURL на любой из этих операционных систем.

Необходимые условия

- Преобразуйте образ в зашифрованную строку base64.
- Необходимо установить cURL на компьютере, где запускаются команды.
- Должны использоваться учетные данные для пользователя vRealize Automation с ролью системного администратора.

Процедура

1. Установите переменную VCAC в терминальном сеансе для команд cURL.

Операционная система	Команда
Linux/Mac	<code>export VCAC=<VA URL></code>
Windows	<code>set VCAC=<VA URL></code>

2. Получите маркер проверки подлинности для системного администратора.

Операционная система	Команда
Linux/Mac	<code>curl https://\$VCAC/identity/api/tokens --insecure -H "Accept: application/json" -H 'Content-Type: application/json' --data '{"username": "<Catalog Administrator User>", "password": "<password>", "tenant": "vsphere.local"}'</code>
Windows	<code>curl https://%VCAC%/identity/api/tokens --insecure -H "Accept:application/json" -H "Content-Type:application/json" --data "{\"username\":\"<Catalog Administrator User>\", \"password\":\"<password>\", \"tenant\":\"vsphere.local\"}"</code>

Создан маркер проверки подлинности.

3. Установите переменную маркера проверки подлинности, заменив <Auth Token> на строку маркера, созданного на предыдущем шаге.

Операционная система	Команда
Linux/Mac	<code>export AUTH="Bearer <Auth Token>"</code>
Windows	<code>set AUTH=Bearer <Auth Token></code>

4. Добавьте в образ зашифрованную строку base64.

Операционная система	Команда
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons --insecure -H "Accept: application/json" -H 'Content-Type: application/json' -H "Authorization: \$AUTH" --data '{"id":"cafe_default_icon_genericAllServices","fileName":"<filename>","contentType":"image/png","image":"<IMAGE DATA as base64 string>"}'</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons --insecure -H "Accept: application/json" -H "Content-Type: application/json" -H "Authorization: %AUTH%" --data "{\"id\":\"cafe_default_icon_genericAllServices\", \"fileName\":\"<filename>\", \"contentType\":\"image/png\", \"image\":\"<IMAGE DATA as base64 string>\"}"</pre>

Результаты

Новый значок служб появится в каталоге служб примерно через пять минут.

Если необходимо вернуться к значку по умолчанию, после выполнения шагов 1–3 можно запустить следующую команду.

Операционная система	Команда
Linux/Mac	<pre>curl https://\$VCAC/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: \$AUTH" --request DELETE</pre>
Windows	<pre>curl https://%VCAC%/catalog-service/api/icons/cafe_default_icon_genericAllServices --insecure -H "Authorization: %AUTH%" --request DELETE</pre>

Настройка параметров смены данных

Благодаря настройке параметров смены данных vRealize Automation можно управлять хранением, архивацией и удалением устаревших данных.

Функция смены данных позволяет установить для vRealize Automation максимальное количество дней хранения данных в базе данных SQL Server. Инфраструктура как услуга, прежде чем они будут архивированы или удалены, а также управлять другими параметрами смены данных.

По умолчанию функция смены данных деактивирована.

Параметры смены данных можно настроить в vRealize Automation на странице **Глобальные параметры**. Активированная функция обеспечивает отправку запросов и удаление данных из следующих таблиц баз данных SQL Server.

- UserLog;
- Аудит
- CategoryLog;
- VirtualMachineHistory;
- VirtualMachineHistoryProp;

- AuditLogItems;
- AuditLogItemsProperties;
- TrackingLogItems;
- WorkflowHistoryInstances;
- WorkflowHistoryResults.

Если для параметра `DataRolloverIsArchiveEnabled` установить значение `True`, в схеме `dbo` будут создаваться архивные версии таблиц. Например, архивной версией `UserLog` будет `UserLogArchive`, а архивной версией `VirtualMachineHistory` — `VirtualMachineHistoryArchive`.

Если функция смены данных включена, она запускается один раз в день в заранее определенное время (3:00) в соответствии с установленным часовым поясом для устройства vRealize Automation. Параметр `DataRollover MaximumAgeInDays` позволяет установить максимальное количество дней хранения данных. Обратите внимание, что этот процесс, как правило, выполняется достаточно быстро и занимает от нескольких минут до одного часа. Тем не менее при первом включении этой функции процесс может занять намного больше времени, так как нужно будет обработать большой объем данных для их архивации или удаления. Данный процесс будет выполняться до тех пор, пока не будет полностью завершен. Он выполняется постепенно в формате небольших и быстро обрабатываемых транзакционных пакетов, чтобы избежать проблем при параллельной обработке. Обратите внимание, что этот процесс можно безопасно остановить, как описано ниже.

Примечание Для остановки процесса смены данных установите для параметра `DataRollover Status` значение «Disabled» или «Enabled» вместо «Running». Это позволит безопасно остановить текущий выполняемый процесс. Никакие данные потеряны не будут. Будут сохранены все данные, архивированные или удаленные до момента остановки процесса.

Если для параметра `DataRollover IsArchiveEnabled` установлено значение `True`, данные, которые хранятся дольше, чем указано для параметра `DataRollover MaximumAgeInDays`, будут перемещены в архивные таблицы. Если для параметра `DataRollover IsArchiveEnabled` установлено значение `False`, данные не будут заархивированы и будут безвозвратно удалены. Удаленные данные нельзя восстановить.

Процедура

1. Войдите в консоль vRealize Automation в качестве **системного администратора**.
2. Выберите **Инфраструктура > Администрирование > Глобальные параметры**.

3. На странице **Глобальные параметры** найдите раздел таблицы **Смена данных**, а затем просмотрите параметры и настройте их.

Параметр	Описание
DataRollover BatchSize	Значение по умолчанию — 2000. Скорее всего, его не нужно будет изменять. Тем не менее, если существуют проблемы с производительностью, возможно, будет иметь смысл уменьшить значение для BatchSize. Более высокое значение для BatchSize может обеспечить более быстрое выполнение задания, но это приведет к росту нагрузки по параллельной обработке. Диапазон допустимых значений: 100–20 000.
DataRollover IsArchiveEnabled	Указывает, следует ли перемещать сменяемые данные в архивные таблицы по прошествии максимального количества дней. По умолчанию для этого параметра установлено значение True. Если установить значение False, все данные, которые хранятся дольше, чем указано в параметре DataRollover MaximumAgeInDays, будут безвозвратно удалены.
DataRollover MaximumAgeInDays	Указывает максимальное количество дней хранения данных в базе данных, прежде чем они будут перемещены в архив или безвозвратно удалены. По умолчанию значение этого параметра — 90 дней.
DataRollover Status	Указывает, следует ли включить смену данных. По умолчанию для этого параметра установлено значение «Отключено». Чтобы включить смену данных, установите значение «Включить».
DataRollover VirtualMachineHistory BatchSize	Указывает размер пакета в таблице VirtualMachineHistory в диапазоне от 1 до 5 записей. Значение по умолчанию — 1.
DataRollover UpdateStatistics	Параметр UpdateStatistics отключен по умолчанию. Его настоятельно рекомендуется включить (установить значение 1), так как обновленная статистика необходима для эффективной обработки запросов. Это приведет к тому, что хранимая процедура [dbo].[usp_DataRollover] выполнит команду обновления статистики в таблицах после запуска процесса архивации.

4. В первом столбце таблицы щелкните значок **Изменить** () , чтобы изменить параметр.

Область **Значение** соответствующего параметра станет доступна для изменения.

5. В первом столбце таблицы щелкните значок **Сохранить** () , чтобы сохранить изменения.

Настройка параметров в файле конфигурации службы диспетчера

С помощью файла конфигурации службы диспетчера (managerService.exe.config) можно настроить общие параметры для развертывания компьютера.

Файл `managerService.exe.config`, как правило, расположен в каталоге `%System-Drive%\Program Files x86\VMware\vCAC\Server`. Прежде чем изменять файл, следует сделать его копию.

Приведенные ниже параметры файла `managerService.exe.config` позволяют управлять различными аспектами развертывания компьютера. Здесь приведены значения по умолчанию.

- `<add key="ProcessLeaseWorkflowTimerCallbackIntervalMilliseconds" value="3600000"/>`
- `<add key="BulkRequestWorkflowTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineRequestTimerCallbackMilliseconds" value="10000"/>`
- `<add key="MachineWorkflowCreationTimerCallbackMilliseconds" value="10000"/>`
- `<add key="RepositoryConnectionMaxRetryCount" value="100"/>`
- `<add key="MachineCatalogRegistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUnregistrationRetryTimerCallbackMilliseconds" value="120000"/>`
- `<add key="MachineCatalogUpdateMaxRetryCount" value="15"/>`

Установка ограничений для ресурсоемкого параллельного выполнения

Для экономии ресурсов vRealize Automation ограничивает количество одновременно выполняемых экземпляров подготовки компьютера и сбора данных. Эти ограничения можно изменить.

Настройка параллельной подготовки компьютеров

Несколько параллельных запросов на подготовку компьютеров могут негативно повлиять на производительность vRealize Automation. Чтобы изменить производительность, можно изменить ограничения, налагаемые на прокси-агенты и активности рабочего процесса.

В зависимости от потребностей владельцев компьютеров на вашем участке, сервер vRealize Automation может получить несколько параллельных запросов на подготовку компьютеров. Это может случиться в следующих обстоятельствах:

- один пользователь отправляет запрос на несколько компьютеров;
- много пользователей запрашивают компьютеры одновременно;
- диспетчеры групп (один или несколько) подтверждают несколько ожидающих запросов на компьютеры за короткий промежуток времени.

Чем больше количество параллельных запросов, тем больше времени нужно решению vRealize Automation для подготовки компьютера. Увеличение времени на подготовку зависит от трех важных факторов:

- влияние, которое оказывают на производительность ресурсоемкие активности рабочего процесса vRealize Automation, в том числе активность `SetupOS` (для компьютеров, созданных в платформе виртуализации, как при подготовке на основе WIM) и активность `Clone` (для компьютеров, клонированных в платформе виртуализации);

- настраиваемый для vRealize Automation лимит ресурсоемких (и обычно длительных) активностей подготовки, которые могут выполняться параллельно. По умолчанию заданы восемь таких активностей. Если активностей больше восьми, они помещаются в очередь.
- любой лимит в рамках платформы виртуализации или учетной записи на количество рабочих элементов vRealize Automation (независимо от того, ресурсоемкие они или нет), которые можно выполнить параллельно. Например, в vCenter Server по умолчанию задан лимит 4, а элементы, превышающие этот лимит, помещаются в очередь.

По умолчанию в решении vRealize Automation задано не более восьми параллельных активностей по подготовке виртуальных машин для гипервизоров, использующих прокси-агенты, на каждую конечную точку. Благодаря этому платформа виртуализации, управляемая тем или иным агентом, никогда не получает такое количество ресурсоемких рабочих элементов, которое предотвращает выполнение других элементов. Прежде чем изменять лимит, тщательно проверяйте последствия его изменения. Чтобы определить оптимальный лимит для вашей среды, может потребоваться проанализировать, как выполняются рабочие элементы на платформе виртуализации и активности рабочих процессов в vRealize Automation.

Если увеличить настраиваемый лимит vRealize Automation на агента, то, возможно, понадобится внести дополнительные изменения конфигурации в vRealize Automation. Они приведены ниже.

- Заданные по умолчанию интервалы времени ожидания выполнения для активностей рабочих процессов SetupOS и Clone — 2 часа. Если превышает время на выполнение одного из этих действий, то действие отменяется, а подготовка заканчивается неудачей. Чтобы избежать такого результата, увеличьте один или оба интервала времени ожидания выполнения.
- Заданный по умолчанию интервал времени ожидания выполнения для операций каждого из рабочих процессов SetupOS и Clone — 20 часов. Если одна из этих активностей запущена, то, если соответствующий компьютер не подготовлен в течение 20 часов, активность отменяется и подготовка завершается неудачей. Поэтому, если при увеличенном вами лимите такое иногда случается, рекомендуется увеличить один или оба интервала времени ожидания доставки.

Настройка параллельных процессов сбора данных

По умолчанию решение vRealize Automation ограничивает параллельные действия по сбору данных. Изменяя это ограничение, можно избежать ненужного времени ожидания. Для этого нужно изменить заданные по умолчанию интервалы времени ожидания для разных типов сбора данных.

Решение vRealize Automation регулярно собирает данные из известных вычислительных ресурсов виртуализации через прокси-агенты, а из учетных записей облачных и физических компьютеров — через представляющие их конечные точки. Частота выполнения параллельных операций по сбору данных может зависеть от числа вычислительных ресурсов виртуализации, агентов и конечных точек в среде.

Время выполнения сбора данных зависит от количества объектов на конечных точках, в том числе виртуальных машин, хранилищ данных, шаблонов и вычислительных ресурсов. При совпадении некоторых условий процесс сбора данных может продолжаться очень долго. Как и при подготовке компьютеров, если процессы протекают параллельно, увеличивается время на сбор данных.

По умолчанию в агенте разрешено максимум два параллельных процесса сбора данных. Процессы, превышающие этот лимит, помещаются в очередь. Благодаря этому процессы сбора данных протекают сравнительно быстро и их параллельность почти не влияет на производительность IaaS.

В зависимости от ресурсов и обстоятельств на вашем участке иногда возможно увеличить заданный лимит, сохраняя при этом достаточно быструю производительность. Таким образом можно эффективно использовать параллельность при сборе данных в прокси-агентах. Хотя при увеличении лимита может увеличиться время, в течение которого выполняется процесс сбора данных, это компенсируется тем, что появляется возможность собирать больше информации с большего количества вычислительных ресурсов и компьютеров одновременно.

Если увеличить лимит на одного агента, то, возможно, понадобится изменить заданные по умолчанию интервалы времени ожидания выполнения для разных типов сбора данных, в которых используется прокси-агент (для сбора данных о иерархии, производительности, состоянии и WMI). Если превышает заданный интервал времени ожидания на выполнение одного из этих действий, то действие отменяется и перезапускается. Чтобы избежать отмены действия, увеличьте интервалы времени ожидания выполнения.

Настройка пределов параллельного выполнения и интервалов времени ожидания

Для каждого агента можно изменить заданные по умолчанию пределы для параллельной подготовки, операций сбора данных и интервалов времени ожидания.

При вводе значения времени для этих переменных используйте формат чч:мм:сс (чч — часы, мм — минуты, а сс — секунды).

Необходимые условия

Войдите в качестве администратора на сервер, где размещена служба диспетчера инфраструктуры как услуги. Для распределенных установок это сервер, на котором была установлена служба диспетчера.

Процедура

1. Откройте файл `ManagerService.exe.config` в редакторе. Данный файл находится в каталоге установки сервера vRealize Automation. Как правило это `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
2. Найдите раздел под названием `workflowTimeoutConfigurationSection`.
3. Обновите следующие переменные соответствующим образом.

Параметр	Описание
<code>MaxOutstandingResourceIntensive WorkItems</code>	Предел одновременной подготовки (по умолчанию восемь)
<code>CloneExecutionTimeout</code>	Интервал времени ожидания выполнения для виртуальной подготовки
<code>SetupOSExecutionTimeout</code>	Интервал времени ожидания выполнения для виртуальной подготовки
<code>CloneTimeout</code>	Интервал времени ожидания доставки клона для виртуальной подготовки
<code>SetupOSTimeout</code>	Интервал времени ожидания доставки ОС для настройки для виртуальной подготовки
<code>CloudInitializeProvisioning</code>	Интервал времени ожидания инициализации для облачной подготовки

Параметр	Описание
MaxOutstandingDataCollectionWorkItems	Предел параллельного сбора данных
InventoryTimeout	Интервал времени ожидания выполнения для сбора данных иерархии
PerformanceTimeout	Интервал времени ожидания выполнения для сбора данных о быстродействии
StateTimeout	Интервал времени ожидания выполнения для сбора данных о состоянии

4. Сохраните файл и закройте его.
5. Выберите **Пуск > Администрирование > Службы**.
6. Остановите и перезапустите службу vRealize Automation.
7. (дополнительно) Если vRealize Automation работает в режиме высокой доступности, при необходимости изменить что-либо в файле `ManagerService.exe.config` после установки все изменения нужно вносить как на основном, так и на резервном сервере.

Настройка частоты выполнения обратных вызовов компьютером

Частоту нескольких процедур обратного вызова, в том числе частоту выполнения процедуры обратного вызова vRealize Automation при изменении аренд компьютеров, можно изменить.

В vRealize Automation для запуска различных процедур обратного вызова в службе диспетчера моделей используется настроенный промежуток времени. Такой промежуток, например, используется для процедуры `ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds`, которая ищет компьютеры с измененной арендой. Этот промежуток времени можно изменить, чтобы проверки выполнялись реже или чаще.

При вводе значения времени для этих переменных введите значение в миллисекундах. Например, 10 000 миллисекунд = 10 секунд и 3 600 000 миллисекунд = 60 минут = 1 час.

Необходимые условия

Войдите в качестве администратора на сервер, где размещена служба диспетчера инфраструктуры как услуги. Для распределенных установок это сервер, на котором была установлена служба диспетчера.

Процедура

1. Откройте файл `ManagerService.exe.config` в редакторе. Данный файл находится в каталоге установки сервера vRealize Automation. Как правило это `%SystemDrive%\Program Files x86\VMware\VCAC\Server`.
2. Обновите следующие переменные необходимым образом.

Параметр	Описание
RepositoryWorkflowTimerCallbackMiliSeconds	Проверьте, активна ли служба репозитория или веб-служба диспетчера модели. Значение по умолчанию — 10 000.
ProcessLeaseWorkflowTimerCallbackIntervalMiliSeconds	Проверка просроченных аренд компьютеров. Значение по умолчанию — 3600000.

Параметр	Описание
<i>BulkRequestWorkflowTimerCallbackMiliSeconds</i>	Проверка массовых запросов. Значение по умолчанию — 10 000.
<i>MachineRequestTimerCallbackMiliSeconds</i>	Проверка запросов компьютеров. Значение по умолчанию — 10 000.
<i>MachineWorkflowCreationTimerCallbackMiliSeconds</i>	Проверка новых компьютеров. Значение по умолчанию — 10 000.

3. Сохраните файл и закройте его.
4. Выберите **Пуск > Администрирование > Службы**.
5. Остановите службу vCloud Automation Center, а затем запустите ее снова.
6. (дополнительно) Если vRealize Automation работает в режиме высокой доступности, при необходимости изменить что-либо в файле `ManagerService.exe.config` после установки все изменения нужно вносить как на основном, так и на резервном сервере.

Настройка параметров журналов инфраструктуры как услуги

Систему vRealize Automation можно настроить так, чтобы она фиксировала только те сведения, которые вы хотите видеть в журнале службы диспетчера.

Если решение vRealize Automation запущено в режиме высокой доступности и вы вносите изменения в файл `ManagerService.exe.config` после установки, нужно внести изменения в основной сервер и сервер отработки отказа vRealize Automation.

Процедура

1. Войдите в сервер vRealize Automation, используя учетные данные, обладающие правами администратора.
2. Измените файл `ManagerService.exe.config` в каталоге `%SystemDrive%\Program Files x86\VMware\VCAC\Server` или, если он находится в другом расположении, в каталоге установки сервера vRealize Automation.

- Отредактируйте ключи RepositoryLogSeverity и RepositoryLogCategory для выбора типов событий, которые будут записываться в файлах журнала.

Параметр	Описание
RepositoryLogSeverity	<p>Указывает уровень серьезности, чтобы игнорировать события с более низким уровнем серьезности.</p> <ul style="list-style-type: none"> ■ <i>Ошибка</i>: в журнале регистрируются только исправляемые ошибки и события более высокого уровня серьезности. ■ <i>Предупреждение</i>: регистрируются некритические предупреждения и события более высокого уровня серьезности. ■ <i>Сведения</i>: регистрируются все информативные сообщения и события более высокого уровня серьезности ■ <i>Подробный</i>: регистрируются результаты трассировки отладки; данный режим может ухудшить производительность. <p>Например, <code><add key="RepositoryLogSeverity" value="Warning" /></code>.</p>
RepositoryLogCategory	<p>Укажите категорию для регистрации в журнале всех событий для данной категории, независимо от уровня серьезности. Например, <code><add key="RepositoryLogCategory" value="MissingMachines,UnregisteredMachines,AcceptMachineRequest,RejectMachineRequest" /></code> регистрирует все события отсутствующих компьютеров или компьютеров с отмененной регистрацией, а также каждый принятый или отклоненный запрос компьютера.</p>

- Сохраните файл и закройте его.
- Выберите **Пуск > Администрирование > Службы** и перезапустите службу vCloud Automation Center.

Результаты

Чтобы увидеть, как внесенные изменения влияют на запись данных в журнале, используйте файл журнала службы диспетчера, расположенный в папке %SystemDrive%\Program Files (x86)\VMware\VCAC\Server\Logs на компьютере, где установлена служба диспетчера, или в каталоге установки сервера vRealize Automation, если вы установили его в другом месте.

Мониторинг vRealize Automation

В зависимости от роли можно выполнять мониторинг рабочих процессов или служб, просматривать журналы событий или аудита, а также собирать данные журналов всех узлов в распределенном развертывании.

Мониторинг рабочих процессов и просмотр журналов

В зависимости от роли можно выполнять мониторинг рабочих процессов и просматривать журналы действий.

Таблица 1-12. Возможности мониторинга и отображения журналов

Цель	Роль	Последовательность выбора пунктов меню и описание
Отображение сведений о выполненных действиях, например тип действия, дата и время его выполнения и т. д.	администратор инфраструктуры как услуги	Просматривайте сведения журнала по умолчанию или управляйте отображаемым содержимым с использованием столбцов и параметров фильтрации. Выберите Инфраструктура > Мониторинг > Журнал аудита . В журнале аудита содержатся подробные сведения о состоянии управляемых виртуальных машин и действиях, выполненных с ними во время перенастройки. Журнал включает в себя сведения о подготовке компьютеров, NSX, реорганизации, а также перенастройке действий.
Просмотр состояния запланированных и доступных рабочих процессов Distributed Execution Manager и других рабочих процессов.	администратор инфраструктуры как услуги	Просматривайте состояние рабочего процесса и при необходимости сведения об определенном рабочем процессе (для этого его нужно открыть). Последовательно выберите Инфраструктура > Мониторинг > Состояние DEM .
Просмотр и при необходимости экспорт данных журнала.	администратор инфраструктуры как услуги	Просматривайте сведения журнала по умолчанию или управляйте отображаемым содержимым с использованием столбцов и параметров фильтрации. Выберите Инфраструктура > Мониторинг > Журнал .
Просмотр состояния и журнала выполненных рабочих процессов Distributed Execution Manager и других рабочих процессов.	администратор инфраструктуры как услуги	Открывайте журнал рабочих процессов и при необходимости просматривайте сведения об определенном рабочем процессе (для этого его нужно открыть). Выберите Инфраструктура > Мониторинг > Журнал рабочих процессов .
Отображение списка событий, в том числе типа события, времени его выполнения, идентификатора пользователя и т. п. При необходимости отображение страницы сведений о событии.	Системный администратор	Просматривайте список событий и связанные атрибуты, такие как время выполнения, описание события, имя арендатора, тип и идентификатор цели, а также другие характеристики. Выберите Администрирование > События > Журналы событий .
Мониторинг состояния запросов и просмотр сведений о запросах.	Администратор арендатора или диспетчер бизнес-групп	Отображайте состояния запросов, за которые несете ответственность или которыми владеете. Щелкните Запросы .
Просмотрите сведения о последних событиях.	Администратор инфраструктуры как услуги или администратор арендатора	Отобразите последние события для текущего пользователя. Выберите Инфраструктура > Последние события

Мониторинг журналов событий и служб

Мониторинг журналов событий и служб позволяет определять текущее и историческое состояние vRealize Automation.

По умолчанию период хранения журналов событий составляет 90 дней. Этот период можно изменить в файле `/etc/vcac/vcac.properties`.

Дополнительные сведения об очистке журналов с помощью настройки параметров смены данных см. в главе *Настройка vRealize Automation*.

Службы vRealize Automation

Системный администратор может просматривать состояние служб vRealize Automation из журнала событий в консоли системного администратора.

Для запуска отдельных компонентов продукта нужны подмножества служб. Например, для настройки арендатора требуются службы идентификации и базовые службы интерфейса пользователя.

В следующих таблицах сопоставлены службы и соответствующие функциональные компоненты vRealize Automation.

Таблица 1-13. Группа служб идентификации

Служба	Описание
management-service	Группа служб идентификации
sts-service	Устройство единого входа
authorization	Служба авторизации
проверка подлинности	Проверка подлинности
eventlog-service	служба журнала событий
licensing-service	Служба лицензирования

Таблица 1-14. Базовые службы интерфейса пользователя

Служба	Описание
shel-ui-app	Служба оболочки
branding-service	Служба фирменной символики
plugin-service	Служба расширенных возможностей (подключаемого модуля)
portal-service	Служба портала

Все перечисленные ниже службы необходимы для запуска компонента инфраструктуры как услуги.

Таблица 1-15. Группа каталога служб (службы управления)

Служба	Описание
notification-service	Служба уведомлений
workitem-service	Служба рабочих элементов

Таблица 1-15. Группа каталога служб (службы управления) (продолжение)

Служба	Описание
approval-service	Служба подтверждения
catalog-service	Каталог служб

Таблица 1-16. Группа служб инфраструктуры как услуги

Служба	Описание
iaas-proxy-provider	Прокси-служба инфраструктуры как услуги
iaas-server	компьютер инфраструктуры как услуги Windows

Таблица 1-17. Все как услуга

Служба	Описание
VCO	vRealize Orchestrator
advanced-designer-service	Схемы элементов и действия ресурсов Все как услуга

Ведение журнала аудита в vRealize Automation

vRealize Automation имеет функцию ведения журнала аудита, которая поддерживает сбор и хранение важных системных событий.

В настоящий момент vRealize Automation поддерживает ведение журнала аудита в качестве дополнительной функции ведения журнала событий. Эта возможность позволяет получить только основные данные аудита, а настройки сохранения можно изменить только с помощью соответствующих вызовов службы брокера событий REST API vRealize Automation. В настоящее время ведение журнала аудита доступно только администраторам арендатора и системным администраторам, которые могут войти в систему от имени арендатора. Эта функция позволяет использовать поиск и фильтр по событиям.

По умолчанию vRealize Automation поддерживает ведение журнала аудита для подписки на рабочий процесс и событий создания, обновления и удаления конечных точек и групп пользователей фабрики. Также vRealize Automation поддерживает настройку ведения журнала аудита для различных событий инфраструктуры как услуги.

Ведение журнала аудита для vRealize Automation по умолчанию деактивировано. Чтобы его включить или выключить, установите флажок **Включено** в разделе интеграции журнала аудита на странице **vRA > Журналы** в интерфейсе управления виртуальными устройствами.

Данные журнала аудита появляются на стандартной странице журналов событий. Если вы являетесь администратором арендатора, выберите **Администрирование > Журналы событий**, чтобы просмотреть эту страницу. События аудита можно найти в таблице журнала событий по назначению «Аудит» в поле «Тип события». Каждая запись отображает для каждого события такие данные, как описание события, арендатора, время, пользователя и имя службы, связанной с событием.

Чтобы включить ведение журнала аудита для других событий инфраструктуры как услуги, необходимо воспользоваться пользовательским файлом конфигурации и запустить соответствующие команды на компьютере узла инфраструктуры как услуги. Если вам потребуется помощь, обратитесь в службу профессиональных услуг VMware.

Можно настроить vRealize Automation так, чтобы события экспортировались на внешний сервер системного журнала, а именно на VMware Log Insight.

Настройка vRealize Automation для ведения журнала аудита Log Insight

В vRealize Automation можно настроить экспорт событий аудита в VMware Log Insight для более удобного просмотра.

Ведение журнала аудита по умолчанию деактивировано, и для генерации и просмотра событий аудита его необходимо включить.

При использовании протокол SSL настраивается на Устройство vRealize Automation, где размещен агент Log Insight, и относится к подключению к серверу системного журнала Log Insight. Если требуется использовать протокол SSL, необходимо настроить соответствующие сертификаты и возможность подключения между vRealize Automation и сервером Log Insight, установленным в развертывании.

Необходимые условия

В vRealize Automation для чтения записей журнала, которые будут просматриваться в Log Insight, используется агент Log Insight, который по умолчанию установлен в развертывании vRealize Automation.

Процедура

1. Выполните вход в интерфейс управления виртуальными устройствами как системный администратор.
2. Выберите **vRA > Журналы**.
3. Убедитесь, что выбран флажок **Включено** для журнала аудита в разделе «Интеграция журнала аудита».
4. Введите имя компьютера **узла** для сервера Log Insight в разделе «Конфигурация агента Log Insight».
 - а) Введите имя компьютера **узла** для агента Log Insight.
 - б) Введите **порт**, который будет использоваться для связи с агентом Log Insight.
 - в) Выберите нужный протокол связи.
 - г) Установите флажок **Протокол SSL включен**, если для связи между агентом Log Insight и сервером необходимо использовать протокол SSL.

Если протокол SSL не будет использоваться, остальные параметры на этой странице можно игнорировать. Если используется протокол SSL, необходимо настроить эти параметры.

5. Если протокол SSL используется, задайте соответствующие настройки в разделе «Доверенны корневые сертификаты SSL».

По умолчанию в Устройство vRealize Automation используется самозаверяющий сертификат. Если необходимо использовать доверенный корневой сертификат, его следует импортировать.

- а) Чтобы использовать новый либо существующий сертификат, установите соответствующий флажок.

Дополнительные сведения см. на странице настройки ведения журналов vRealize Automation в интерфейсе управления виртуальными устройствами.

6. Нажмите кнопку **Сохранить настройки**.
7. Задайте соответствующие настройки в разделе «SSL-сертификаты сервера».
8. Работа агента с файлами журналов настраивается в разделе «Настройка поведения агента».

Результаты

События журнала аудита vRealize Automation отображаются в интерфейсе Log Insight.

Просмотр сведений об узле для кластеров в распределенных развертываниях

В консоли управления устройством vRealize Automation можно собрать журналы для всех кластерных узлов в распределенном развертывании.

Можно также просмотреть сведения о каждом узле в развертывании. В консоли управления vRealize Automation на вкладке **Кластер** находится таблица «Сведения о распределенном развертывании», в которой отображаются следующие данные:

- Список всех узлов в развертывании.
- Имя узла для узла. Имя узла задается в виде полного доменного имени.
- Время, прошедшее с момента получения последнего ответа узла на запрос консоли управления. Узлы компонентов Инфраструктура как услуга сообщают о доступности каждые три минуты, а узлы виртуальных устройств — каждые девять минут.
- Тип компонента vRealize Automation. Определяет, чем является узел — виртуальным устройством или сервером Инфраструктура как услуга.

Рис. 1-1. таблица «Сведения о распределенном развертывании»

	Host / Node Name	Version	Last Connected	Type	State*	Valid*
▶	cava-n-80-175.eng.vmware.com	7.5.0.378	7 minutes ago	MASTER	Up	<button>Delete</button>
▶	cava-n-85-043.eng.vmware.com	7.5.0.14528	14 seconds ago	IAAS		<button>Delete</button>

Эту таблицу можно использовать для мониторинга процессов в развертывании. Например, если в столбце «Последнее подключение» указано, что подключение с узлом давно не устанавливалось, это может указывать на проблемы с сервером.

Сбор журналов

Можно создать zip-файл, содержащий файлы журналов всех узлов в развертывании с помощью кнопки «Создать пакет поддержки» на странице **vRA > Журналы**. Дополнительные сведения см. в разделе [Сбор журналов для кластеров и распределенных развертываний](#).

Удаление узлов из таблицы

При удалении узла из развертывания удалите соответствующий узел из таблицы «Сведения о распределенном развертывании», чтобы сократить время сбора журналов. Чтобы удалить узел из таблицы, нажмите кнопку **Удалить**.

Сбор журналов для кластеров и распределенных развертываний

Чтобы обеспечить устранение неполадок и сохранение журналов, можно создать zip-файл, содержащий файлы журналов всех серверов в данном развертывании.

Таблица сведений о распределенном развертывании на вкладке «Кластер» в интерфейсе управления виртуальным устройством содержит список узлов, для которых создаются файлы журналов. При необходимости можно удалять узлы из этой таблицы.

Дополнительные сведения о настройке развертывания устройства vRealize Automation см. в разделе *Установка vRealize Automation*.

Процедура

1. Выполните вход в интерфейс управления виртуальными устройствами как системный администратор.
2. Выберите **vRA > Журналы**.
3. Щелкните **Создать пакет поддержки**.

Файлы журналов для каждого узла собираются и копируются в ZIP-файл.

Удаление узла из таблицы «Сведения о распределенном развертывании»

Операция удаления узла требуется, когда нужно удалить узел из кластера развертывания или когда нужно заменить сертификат агента управления.

Таблица сведений о распределенном развертывании на вкладке «Кластер» (Cluster) в интерфейсе управления виртуальным устройством содержит список узлов для соответствующего кластера. Чтобы удалить нужный узел из кластера, можно в этой таблице нажать кнопку **Удалить** для этого узла, или можно использовать следующую процедуру.

Процедура

1. Войдите в устройство vRealize Automation, используя имя пользователя **root** и пароль, указанный при развертывании устройства.

2. Перейдите на вкладку Кластер.

В таблице с информацией о распределенном развертывании отображается список узлов для распределенного развертывания.

3. Найдите идентификатор удаляемого узла, открыв командную строку и выполнив следующую команду:

```
/usr/sbin/vcac-config cluster-config-node --action list
```

4. Найдите идентификатор узла, например `cafe.node.46686239.17144`, в выходных данных JSON.**5. Откройте командную строку и введите команду в следующем формате, используя идентификатор узла, полученный на предыдущем шаге.**

```
/usr/sbin/vcac-config cluster-config-node  
--action delete --id node-UID
```

Например, введите следующую команду для идентификатора узла в качестве примера `cafe.node.46686239.17144`:

```
/usr/sbin/vcac-config cluster-config-node --action delete --id cafe.node.46686239.17144
```

6. Нажмите кнопку Обновить.

Узел больше не отображается.

Мониторинг работоспособности vRealize Automation

Служба проверки работоспособности vRealize Automation оценивает работоспособность среды vRealize Automation.

Администраторы инфраструктуры как услуги настраивают в службе проверки работоспособности выполнение наборов тестов, которые определяют, зарегистрированы ли соответствующие компоненты и доступны ли необходимые ресурсы. В этой таблице представлены наборы тестов, доступные в службе проверки подлинности, и примеры тестов из каждого набора.

Наборы тестов в службе проверки работоспособности	Примеры тестов
Системные тесты для vRealize Automation	<ul style="list-style-type: none"> ■ Тест службы единого входа/подключения к VA удостоверений ■ vRealize Automation Проверка лицензии — истек срок действия лицензии? ■ Проверка пароля пользователя root на виртуальном устройстве vRealize Automation — срок действия пароля заканчивается?
Тесты арендаторов для vRealize Automation	<ul style="list-style-type: none"> ■ Проверка путей к хранилищу резервирования vSphere ■ Проверка политики резервирования для назначений резервирования ■ Проверка состояния службы портала
Тесты для vRealize Orchestrator	<ul style="list-style-type: none"> ■ Проверка количества активных узлов vRO ■ Проверка использования динамической памяти Java в узлах vRO ■ Проверка состояния службы vRO-сервера в узлах vRO

После выполнения набора тестов на виртуальной машине служба проверки работоспособности выдает информацию о количестве тестов, которые завершились успешно или со сбоем. Для каждого теста, который завершен со сбоем, служба проверки работоспособности предоставляет следующие ссылки.

Ссылка	Содержимое
Причина	Объяснение причины сбоя теста.
Исправление	Сведения, которые можно использовать для устранения проблемы.

Службу проверки работоспособности можно настроить на выполнение тестов по расписанию или только по запросу.

Можно также использовать Python для создания настраиваемых тестов. См. *Руководство по расширяемости службы проверки работоспособности vRealize Automation*.

Администраторы арендаторов с ролью «Потребитель службы проверки работоспособности» (Health Consumer) могут просматривать результаты тестирования для своих арендаторов, но не могут настраивать тесты или выполнять их.

Настройка системных тестов для vRealize Automation

Администратор инфраструктуры как услуги настраивает параметры службы проверки работоспособности для выполнения системных тестов на выбранном виртуальном устройстве vRealize Automation. Эти тесты определяют, зарегистрированы ли компоненты, например лицензия vRealize Automation, и имеются ли на виртуальном устройстве необходимые ресурсы, например память. После настройки службы тесты отображаются на странице «Работоспособность» в виде карточки тестов.

Чтобы настроить выполнение системных тестов для vRealize Automation в службе проверки работоспособности, выполните следующие действия.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Администрирование > Работоспособность**.
2. Щелкните **Новая конфигурация**.
3. На странице «Сведения о конфигурации» введите запрашиваемую информацию.

Параметр	Описание
Имя	Название этой конфигурации. Это название будет отображаться на карточке тестов.
Описание	Описание пакета тестов.
Продукт	Выберите vRealize Automation.
Расписание	Выберите частоту выполнения пакета тестов.

4. Нажмите кнопку **Далее**.
5. На странице «Выбор наборов тестов» выберите **Системные тесты для vRealize Automation**.
6. Нажмите кнопку **Далее**.
7. На странице «Настройка параметров» введите запрашиваемую информацию.

Таблица 1-18. Виртуальное устройство vRealize Automation

Параметр	Описание
Общедоступный адрес веб-сервера	<ul style="list-style-type: none"> ■ Для минимального развертывания базовый URL-адрес узла устройства vRealize Automation. Например, <code>https://va-host.domain/</code>. ■ Для развертывания высокой доступности базовый URL-адрес подсистемы балансировки нагрузки vRealize Automation. Например, <code>https://load-balancer-host.domain/</code>.
Адрес консоли SSH	Полное доменное имя устройства vRealize Automation. Например, <code>va-host.domain</code> .
Пользователь консоли SSH	root
Пароль консоли SSH	Пароль пользователя root.

Таблица 1-19. Арендатор системы vRealize Automation

Параметр	Описание
Администратор арендатора системы	администратор
Пароль арендатора системы	Пароль администратора.

Таблица 1-20. Мониторинг дискового пространства vRealize Automation

Параметр	Описание
Пороговый процент предупреждения	Допустимый процент используемой дискового пространства виртуального устройства, при превышении которого предупредительный тест завершается сбоем.
Критический пороговый процент	Допустимый процент используемого дискового пространства виртуального устройства, при превышении которого критический тест завершается сбоем.

8. Нажмите кнопку **Далее**.
9. Ознакомьтесь с информацией на странице «Сводка».
10. Щелкните элемент **Готово**.

Тесты выполняются в соответствии с выбранным расписанием.

Следующие шаги

[Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation](#)

Настройка тестов арендаторов для vRealize Automation

Администратор инфраструктуры как услуги настраивает службу проверки работоспособности для выполнения тестов арендаторов на выбранном виртуальном устройстве vRealize Automation. Эти тесты определяют, зарегистрированы ли связанные с арендаторами компоненты, например software-service, и имеются ли на виртуальном устройстве необходимые ресурсы, например виртуальные машины vSphere. После настройки службы тесты отображаются на странице «Работоспособность» в виде карточки тестов.

Чтобы настроить выполнение тестов арендаторов для vRealize Automation в службе проверки работоспособности, выполните следующие действия.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Администрирование > Работоспособность**.
2. Щелкните **Новая конфигурация**.
3. На странице «Сведения о конфигурации» введите запрашиваемую информацию.

Параметр	Описание
Имя	Название этой конфигурации. Это название будет отображаться на карточке тестов.
Описание	Описание тестов.

Параметр	Описание
Продукт	Выберите vRealize Automation.
Расписание	Укажите, как часто должны выполняться тесты.

- Нажмите кнопку **Далее**.
- На странице «Выбор наборов тестов» выберите **Тесты арендаторов для vRealize Automation**.
- Нажмите кнопку **Далее**.
- На странице «Настройка параметров» введите запрашиваемую информацию.

Таблица 1-21. Виртуальное устройство vRealize Automation

Параметр	Описание
Веб-адрес vRealize Automation	<ul style="list-style-type: none"> ■ Для минимального развертывания базовый URL-адрес узла устройства vRealize Automation. Например, <code>https://va-host.domain/</code>. ■ Для развертывания высокой доступности базовый URL-адрес подсистемы балансировки нагрузки vRealize Automation. Например, <code>https://load-balancer-host.domain/</code>.
Адрес консоли SSH	Полное доменное имя узла SSH. Например, <code>ssh-host.domain</code> .
Пользователь консоли SSH	root
Пароль консоли SSH	Пароль для пользователя root.
Максимальное время ответа службы (мс)	Максимальное время ожидания ответа системой (в миллисекундах).

Таблица 1-22. Арендатор vRealize Automation

Параметр	Описание
Тестируемый арендатор	обеспечение качества
Имя администратора структуры	Имя администратора структуры. Примечание Чтобы выполнять все виды тестирования, администратор структуры должен также выполнять роль администратора арендаторов и инфраструктуры как услуги.
Пароль администратора структуры	Пароль для администратора структуры.

Таблица 1-23. Арендатор системы vRealize Automation

Параметр	Описание
Администратор арендатора системы	администратор
Пароль арендатора системы	Пароль для администратора.

Таблица 1-24. Мониторинг дискового пространства vRealize Automation

Параметр	Описание
Критический пороговый процент	Допустимый процент используемого дискового пространства виртуального устройства, при превышении которого критический тест завершается сбоем.

8. Нажмите кнопку **Далее**.
9. Ознакомьтесь с информацией на странице «Сводка».
10. Щелкните элемент **Готово**.

Тесты выполняются в соответствии с выбранным расписанием.

Следующие шаги

[Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation](#)

Настройка тестов vRealize Orchestrator

Администратор инфраструктуры как услуги настраивает параметры службы проверки работоспособности для выполнения тестов для vRealize Orchestrator на узле vRealize Orchestrator. Эти тесты определяют, зарегистрированы ли компоненты, например служба vro-server, и имеются ли на компьютере узла необходимые ресурсы, например достаточная динамическая память Java. После настройки службы тесты для vRealize Orchestrator отображаются на странице «Работоспособность» в виде карточки тестов.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Администрирование > Работоспособность**.
2. Щелкните **Новая конфигурация**.
3. На странице «Сведения о конфигурации» введите запрашиваемую информацию.

Параметр	Описание
Имя	Название этой конфигурации. Это название будет отображаться на карточке тестов.
Описание	Описание тестов.
Продукт	Выберите vRealize Orchestrator.
Расписание	Укажите, как часто должны выполняться тесты.

4. Нажмите кнопку **Далее**.
5. На странице «Выбор наборов тестов» выберите **Тесты для vRealize Orchestrator**.

6. Нажмите кнопку **Далее**.
7. На странице «Настройка параметров» введите запрашиваемую информацию.

Таблица 1-25. Узел vRealize Orchestrator/подсистема балансировки нагрузки

Параметр	Описание
Адрес клиента	<ul style="list-style-type: none"> ■ Полное доменное имя узла vRealize Orchestrator для минимального развертывания. Например, <i>vro-host.domain</i>. ■ Для развертывания высокой доступности базовый URL-адрес подсистемы балансировки нагрузки vRealize Orchestrator, <i>https://load-balancer-host.domain/</i>.
Имя клиента	администратор
Пароль клиента	Пароль администратора.
Имя пользователя консоли SSH	root
Пароль консоли SSH	Пароль пользователя root.
Пороговое использование динамической памяти	Допустимый процент используемой динамической памяти, при превышении которого предупредительный тест завершается сбоем.

Таблица 1-26. Экземпляры vRealize Orchestrator позади подсистемы балансировки нагрузки

Параметр	Описание
Адрес консоли SSH	IP-адрес или URL-адрес экземпляра vRealize Orchestrator позади подсистемы балансировки нагрузки.
Имя пользователя консоли SSH	Имя пользователя с доступом к этому экземпляру.
Пароль консоли SSH	Пароль пользователя.

- Щелкните **ДОБАВИТЬ** для добавления другого экземпляра vRealize Orchestrator в список.
- Щелкните **УДАЛИТЬ** для удаления выбранного экземпляра vRealize Orchestrator из списка экземпляров позади подсистемы балансировки нагрузки.

8. Нажмите кнопку **Далее**.
9. Ознакомьтесь с информацией на странице «Сводка».
10. Щелкните элемент **Готово**.

Тесты выполняются в соответствии с выбранным расписанием.

Следующие шаги

[Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation](#)

Пакет настраиваемых тестов

С помощью Python можно создать пакет настраиваемых тестов для проверки работоспособности vRealize Automation.

Создание пакета настраиваемых тестов расширяет возможность выбора при тестировании работоспособности и позволяет проводить испытания дополнительных компонентов vRealize Automation. Информацию о создании пакета настраиваемых тестов см. в *руководстве по расширению функциональности службы проверки работоспособности vRealize Automation*.

Добавление пакета настраиваемых тестов

Перед запуском пакета тестов **администратор инфраструктуры как услуги** должен добавить пакет настраиваемых тестов для службы проверки работоспособности vRealize Automation.

Чтобы добавить пакет настраиваемых тестов для ресурса vRealize Automation, выполните следующую процедуру.

Необходимые условия

- Создайте wheel-пакет Python для добавления файлов пакета настраиваемых тестов. Для получения дополнительных сведений см. *vRealize Automation Руководство по расширяемости службы проверки работоспособности*.
- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Щелкните **Администрирование > Работоспособность**.
2. В правом верхнем углу щелкните значок шестеренки и выберите **Расширяемость**.
3. Щелкните **Новый ресурс**.
4. Укажите необходимые данные в диалоговом окне «Добавить ресурс».

Параметр	Описание
Название ресурса	Имя и номер версии запускаемого пакета тестов, например, «Infoblox 1.0».
Описание ресурса	Описание тестов, содержащихся в wheel-пакете Python.
Версия ресурса	Номер версии пакета тестов.
Файл ресурса	Щелкните Выбрать файл и выберите файл пакета настраиваемых тестов.

5. Нажмите кнопку **Добавить**.

Новая строка добавляется в таблицу ресурсов с состоянием **ОТПРАВЛЕНО**. При изменении состояния на **УСТАНОВЛЕНО** набор тестов готов к использованию. В случае сбоя процесса установки появится всплывающее окно с объяснением причины.

Примечание Если страница не обновилась, щелкните значок «Обновить».

Следующие шаги

[Использование пакета настраиваемых тестов.](#)

Использование пакета настраиваемых тестов

Администратор инфраструктуры как услуги настраивает в службе проверки работоспособности выполнение пакетов тестов в среде vRealize Automation. При конфигурации пакета настраиваемых тестов на странице работоспособности он отображается в виде карточки тестирования.

Чтобы использовать пакет настраиваемых тестов при проверке работоспособности vRealize Automation, выполните следующую процедуру.

Необходимые условия

- [Добавление пакета настраиваемых тестов.](#)
- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Администрирование > Работоспособность**.
2. Щелкните **Новая конфигурация**.
3. На странице «Сведения о конфигурации» введите запрашиваемую информацию.

Параметр	Описание
Имя	Название этой конфигурации. Это название будет отображаться на карточке тестов.
Описание	Описание пакета тестов.
Продукт	Выберите продукт, который необходимо проверять, в раскрывающемся меню Продукт .
Расписание	Выберите частоту использования пакета тестов.

4. Нажмите кнопку **Далее**.
5. На странице «Выбор наборов тестов» выберите набор настраиваемых тестов и нажмите кнопку **Далее**.
6. На странице настройки параметров введите необходимые данные и нажмите **Далее**.
7. Ознакомьтесь с информацией на странице «Сводка» и нажмите кнопку **Готово**.

Пакет настраиваемых тестов используется согласно заданному расписанию.

Следующие шаги

[Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation](#)

Просмотр результатов набора тестов службы проверки работоспособности vRealize Automation

После выполнения тестов службы проверки работоспособности можно просмотреть их результаты.

На странице «Работоспособность» каждый настроенный набор тестов отображается в виде карточки теста. В ходе выполнения набора тестов результат тестирования появляется в середине карточки теста.

Карточки тестов, отображаемые на странице «Работоспособность», фильтруются в соответствии с вашими правами.

- Администраторы инфраструктуры как услуги могут видеть все карточки тестов.
- Администраторы арендаторов с ролью «Потребитель службы проверки работоспособности» могут видеть карточку теста только для своих арендаторов.

Необходимые условия

- Настроенный набор тестов был выполнен по расписанию.
- Войдите в консоль vRealize Automation в качестве **администратора инфраструктуры как услуги** или **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Работоспособность**.
2. Если выполнение теста не запланировано, нажмите **Запустить** в карточке тестов.
3. После завершения тестов щелкните в центре карточки тестов.

Появится страница, на которой отображается статус каждого теста. Чтобы увидеть причину сбоя, нажмите **Причина**. Чтобы открыть раздел, в котором объясняется, как устранить проблему, щелкните ссылку **Исправление**, если она отображается.

Устранение неполадок службы проверки работоспособности

В разделах, где рассматриваются процедуры устранения неполадок службы проверки работоспособности, описываются решения для проблем, которые могут происходить при использовании данной службы.

Тест состояния службы завершается сбоем

Если тест состояния службы завершился сбоем, измените настройки расписания тестирования.

Проблема

Если тест состояния службы завершается сбоем, и вы щелкаете **Причина**, появится следующее сообщение: Не удалось установить подключение SSH; сообщение «Исключение»: [Сбой проверки подлинности].

Причина

Если набор тестов должен выполняться в соответствии с расписанием каждые 15 минут, вход в систему приведет к блокировке учетной записи пользователя root.

Решение

- ◆ Измените расписание тестирования на **Нет**, подождите 15 минут и выполните набор тестов снова.

После обновления страница проверки работоспособности в консоли устройства пуста

После обновления vRealize Automation страница проверки работоспособности в консоли устройства пуста.

Проблема

Служба проверки работоспособности не запускается после обновления.

Решение

- ◆ На каждом виртуальном устройстве vRealize Automation откройте командную строку от имени **пользователя root** и выполните эти команды.
 - а) Для настройки автоматического запуска службы проверки работоспособности выполните эту команду.


```
chkconfig vrhb-service on
```
 - б) Для запуска службы проверки работоспособности на этом виртуальном устройстве выполните эту команду.


```
service vrhb-service start
```

Мониторинг ресурсов среды vRealize Automation с помощью протокола SNMP

Системному администратору, знакомому с протоколом SNMP, рекомендуется использовать vRealize Automation REST API для vSNMP, чтобы упростить мониторинг узлов vRealize Automation. Благодаря применению vSNMP можно использовать протокол SNMP в качестве системы ранних зашифрованных предупреждений о том, что ресурсы ЦП, ОЗУ и дискового пространства vRealize Automation почти исчерпаны, чтобы избежать снижения производительности.

Чтобы вручную отслеживать идентификаторы объектов протокола SNMP, а также выполнять активный мониторинг ресурсов, можно настроить прерывания протокола SNMP.

Например, если vSNMP отправляет вам некое событие (предположим, «Обнаружено интенсивное использование ЦП»), вы можете начать сбор информации о процессах, потребляющих ресурсы ЦП, и определить, какой из них использует чрезмерный объем ресурсов. Затем можно внести изменения в ЦП, память и другие параметры использования для устранения дополнительных проблем.

Благодаря применению vRealize Automation vSNMP можно предоставить доступ ко всему дереву Linux для мониторинга и получения данных с помощью REST API или с помощью управляющей программы vSNMPD, выполняемой в экземплярах vRealize Automation.

В vRealize Automation SNMP нет общего интерфейса использования. Необходимо использовать REST API или команды управляющей программы.

Дополнительные сведения см. в разделе «Использование протокола SNMP для мониторинга vRealize Automation» в руководстве по программированию vRealize Automation. Чтобы найти руководство по программированию, перейдите в раздел [Документация по API-интерфейсу vRealize Automation](#) и откройте ссылку на нужную версию.

Мониторинг и управление ресурсами

В разных ролях vRealize Automation мониторинг использования ресурсов и управление инфраструктурой осуществляются по-разному.

Выбор сценария мониторинга ресурсов

Во время мониторинга ресурсов перед администраторами структуры, администраторами арендаторов и диспетчерами бизнес-групп встают разные задачи. Поэтому vRealize Automation позволяет отслеживать разные аспекты использования ресурсов.

Например, администратору структуры нужно отслеживать потребление ресурсов резервирования и вычислительных ресурсов, тогда как администратору арендатора — использование ресурсов в группах подготовки в арендаторе. vRealize Automation позволяет использовать разные способы отслеживания потребления ресурсов в зависимости от того, какая у пользователя роль и какой аспект использования ресурсов нужно отслеживать.

Таблица 1-27. Выбор сценария мониторинга ресурсов

Сценарий мониторинга ресурсов	Требуются привилегии	Расположение
Отследите, какой объем физического хранилища и памяти сейчас потребляется на ваших вычислительных ресурсах, и определите, какой объем остается свободным. Кроме того, вы можете отслеживать, сколько компьютеров зарезервировано и подготовлено на каждом вычислительном ресурсе.	Администратор структуры (мониторинг потребления ресурсов в вычислительных ресурсах в вашей группе структуры)	Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы
Отследите, какие компьютеры сейчас подготовлены и находятся под управлением vRealize Automation.	Администратор структуры	Инфраструктура > Компьютеры > Управляемые компьютеры
Отследите, какой объем хранилища и памяти и какая часть квоты на компьютеры в вашем резервировании сейчас выделены, и определите, какие мощности остаются доступными для резервирования.	Администратор структуры (мониторинг использования ресурсов для резервирования в ваших вычислительных ресурсах и физических компьютерах)	Инфраструктура > Резервирования > Резервирования
Отследите, какой объем хранилища и памяти и какая часть квоты на компьютеры сейчас используются вашими бизнес-группами, и определите, какие мощности остаются доступными для резервирования.	<ul style="list-style-type: none"> ■ Администратор арендатора (мониторинг использования ресурсов для всех групп в вашем арендаторе) ■ Диспетчер бизнес-группы (мониторинг использования ресурсов для управляемых вами групп) 	Администрирование > Пользователи и группы > Бизнес-группы

Терминология в области использования ресурсов

В vRealize Automation для доступных ресурсов, ресурсов, которые предназначены для определенных задач, и ресурсов, которые активно используются подготовленными компьютерами, используются отдельные термины.

В таблице «Терминология в области использования ресурсов» приведено описание терминов, используемых в vRealize Automation для отображения использования ресурсов.

Таблица 1-28. Терминология в области использования ресурсов

Временная лицензия	Описание
Физический	Указывает фактический объем памяти или емкость хранилища вычислительного ресурса.
Зарезервировано	Указывает квоту на компьютеры, объем памяти и емкость хранилища, отведенные для резервирования. Например, если физическая емкость вычислительного ресурса составляет 600 ГБ и в нем есть три резервирования по 100 ГБ, то зарезервированная емкость хранения вычислительного ресурса составляет 300 ГБ, а в хранилище зарезервировано 50 % ресурсов.
Управляется	Указывает, что компьютер подготовлен и им управляет vRealize Automation.
Выделено	Указывает квоту на компьютеры, объем памяти или ресурсы хранения, которые активно используются подготовленными компьютерами. Например, рассмотрим резервирование с квотой на 10 компьютеров. Если в резервировании подготовлено 15 компьютеров, но включено только 6, квота на компьютеры выделена на 60 процентов.
Используется	Значение столбца Используется всегда равно значению столбца Выделено .
Свободно	Указывает на неиспользуемую физическую емкость в пути к хранилищу.

Подключение к облачному компьютеру

При первом подключении к облачному компьютеру необходимо выполнить вход в качестве администратора.

Позже можно добавить учетные данные, которые используются для входа в консоль vRealize Automation, от имени пользователя компьютера, и после этого выполнять вход с использованием учетных данных vRealize Automation.

Важно! Если вы используете службу Amazon Web Services, на экземпляре машины Amazon должен быть включен протокол удаленного рабочего стола (RDP) или SSH, а машины должны быть в группе безопасности, в которой открыты правильные порты.

Сбор учетных данных пользователей для компьютера Amazon Имена баз данных должны содержать не более 128 символов ASCII.

Для входа в систему компьютера Amazon в качестве администратора необходим пароль администратора компьютера.

Пароль администратора можно узнать на странице «Сведения о компьютере». Если образ компьютера Amazon, на основе которого был подготовлен компьютер, не настроен для генерации пароля администратора при каждой начальной загрузке, необходимо найти пароль, используя альтернативный способ. Сведения об альтернативном способе получения пароля администратора см. в теме *Connect to Your Amazon EC2 Instance* («Подключение к экземпляру Amazon EC2») в документации Amazon.

При необходимости можно создать необходимые учетные данные пользователя vRealize Automation. С помощью этих учетных данных в дальнейшем можно будет входить на этот компьютер.

Необходимые условия

- Компьютер Amazon уже подготовлен.
- Войдите в службу vRealize Automation в качестве владельца компьютера, **диспетчера бизнес-групп** или **пользователя поддержки**.
- Протокол RDP или SSH активен в образе компьютера Amazon, который будет использоваться для подготовки.
- Компьютеры находятся в группе безопасности, в которой открыты правильные порты.

Процедура

1. Перейдите на страницу **Элементы** и отфильтруйте управляемые группы или определенную группу.
2. Выберите компьютер Amazon в списке компьютеров.

Можно выбрать **Посмотреть сведения** в раскрывающемся меню **Действия**, чтобы отобразить подробные сведения, например о типе компьютера.

3. В раскрывающемся меню **Действия** выберите **Изменить**.
4. Щелкните **Показать пароль администратора**, чтобы узнать пароль администратора компьютера.

Помимо этого способа, пароль можно получить с помощью внешней процедуры Amazon.

5. В раскрывающемся меню **Действия** выберите **Подключиться с помощью RDP**.
6. Щелкните **Другая учетная запись пользователя**, если отобразится запрос на учетные данные для входа.

7. Введите **LOCAL\Administrator**, если отобразится запрос на имя пользователя.
8. Введите пароль администратора, если отобразится запрос.
9. Нажмите кнопку **ОК**.

Вы выполнили вход на компьютер в качестве администратора.

10. Соответствующим образом добавьте свои учетные данные vRealize Automation. Например, на компьютере сервера под управлением Windows откройте диспетчер сервера и выберите **Конфигурация > Локальные пользователи и группы** и добавьте свои учетные данные в формате **DOMAIN\username** в группу **Пользователи удаленного рабочего стола**.

Теперь эти имя пользователя и пароль vRealize Automation — допустимые учетные данные для входа на этот компьютер в дальнейшем.

11. Выйдите из системы компьютера Amazon.
12. В раскрывающемся меню **Действия** выберите **Подключиться с помощью RDP**.
13. При появлении запроса на вход введите имя пользователя и пароль vRealize Automation, чтобы войти в систему компьютера.

Результаты

Теперь владельцы компьютеров могут использовать свои учетные данные vRealize Automation для входа на компьютер.

Сбор учетных данных пользователей для компьютера vCloud

Чтобы войти на компьютер vCloud Air или vCloud Director в качестве администратора, нужно знать пароль администратора.

Пароль администратора можно узнать на странице «Сведения о компьютере». Если образ, на основе которого подготовлен компьютер, не настроен для создания пароля администратора при каждой загрузке, пароль можно найти другим способом. Дополнительные сведения о получении пароля администратора см. в документации vCloud Air или vCloud Director.

При необходимости можно создать необходимые учетные данные пользователя vRealize Automation. С помощью этих учетных данных в дальнейшем можно будет входить на этот компьютер.

Необходимые условия

- Компьютер vCloud Air или vCloud Director уже подготовлен.
- Войдите в службу vRealize Automation в качестве владельца компьютера, **диспетчера бизнес-групп** или **пользователя поддержки**.
- Активный параметр протокола RDP или SSH в образе компьютера vCloud Air или vCloud Director, который будет использоваться при подготовке.
- Компьютеры находятся в группе безопасности, в которой открыты правильные порты.

Процедура

1. Перейдите на страницу **Элементы** и отфильтруйте управляемые группы или определенную группу.
2. Выберите компьютер vCloud Air или vCloud Director в списке компьютеров.

Можно выбрать **Посмотреть сведения** в раскрывающемся меню **Действия**, чтобы отобразить подробные сведения, например о типе компьютера.

3. В раскрывающемся меню **Действия** выберите **Изменить**.
4. Щелкните **Показать пароль администратора**, чтобы узнать пароль администратора компьютера.
Кроме того, пароль можно получить с помощью внешнего решения vCloud Air или vCloud Director.
5. В раскрывающемся меню **Действия** выберите **Подключиться с помощью RDP**.
6. Щелкните **Другая учетная запись пользователя**, если отобразится запрос на учетные данные для входа.

7. Введите **LOCAL\Administrator**, если отобразится запрос на имя пользователя.
8. Введите пароль администратора, если отобразится запрос.
9. Нажмите кнопку **ОК**.

Вы выполнили вход на компьютер в качестве администратора.

10. Соответствующим образом добавьте свои учетные данные vRealize Automation. Например, на компьютере сервера под управлением Windows откройте диспетчер сервера и выберите **Конфигурация > Локальные пользователи и группы** и добавьте свои учетные данные в формате **DOMAIN\username** в группу **Пользователи удаленного рабочего стола**.

Теперь эти имя пользователя и пароль vRealize Automation — допустимые учетные данные для входа на этот компьютер в дальнейшем.

11. Выйдите из системы компьютера vCloud Air или vCloud Director.
12. В раскрывающемся меню **Действия** выберите **Подключиться с помощью RDP**.
13. При появлении запроса на вход введите имя пользователя и пароль vRealize Automation, чтобы войти в систему компьютера.

Результаты

Теперь владельцы компьютеров могут использовать свои учетные данные vRealize Automation для входа на компьютер.

Уменьшение использования резервирования путем сокращения

Администраторы структуры могут уменьшить количество компьютеров в конкретном резервировании в долгосрочной перспективе, при этом сохраняя резервирование и существующие подготовленные в нем компьютеры активными.

Можно уменьшить зарезервированную квоту на компьютеры, а также объем памяти и хранилища виртуального резервирования до показателя, ниже выделенного. Благодаря этому управление существующими компьютерами может осуществляться без изменений, при этом предотвращая подготовку новых компьютеров до тех пор, пока объем выделения не станет меньше новой зарезервированной величины.

Примечание Ввиду того, что выключенные виртуальные машины не учитываются в выделенной памяти и квоте на компьютеры, уменьшение выделенного объема памяти или количества компьютеров резервирования может предотвратить включение компьютеров, которые в настоящее время выключены.

К примеру, возьмем бизнес-группу с резервированием, содержащим 20 подготовленных компьютеров, срок действия которых истекает в течение следующих 90 дней. Если нужно уменьшить это резервирование, сократив количество компьютеров до 15, можно уменьшить квоту на компьютеры для резервирования с 20 до 15. В этом резервировании больше нельзя будет подготовить компьютеры, пока их количество не уменьшится естественным образом за счет приближающегося истечения срока действия.

Списание пути к хранилищу

Если вы выводите из употребления путь к хранилищу и перемещаете компьютеры в новое расположение, администратор структуры должен деактивировать путь к хранилищу в vRealize Automation.

Ниже приведен высокоуровневый обзор последовательности шагов, нужных для списания пути к хранилищу.

1. Администратор структуры деактивирует путь к хранилищу во всех резервированиях, которые его используют. См. раздел [Деактивация пути к хранилищу](#).
2. Переместите компьютеры в новое расположение хранилища вне vRealize Automation.
3. Подождите, пока решение vRealize Automation автоматически запустит сбор данных иерархии или иницируйте сбор данных иерархии вручную. См. раздел [Настройка сбора данных вычислительного ресурса](#).

Деактивация пути к хранилищу

Когда пути к хранилищу выведены из употребления, администраторы структуры могут деактивировать их использование в резервированиях.

Примечание Убедитесь, что в каждом резервировании, в котором деактивировано использование пути к хранилищу, в каталогах, на которые указывают другие пути к хранилищу, остается достаточно места.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора структуры**.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Наведите указатель мыши на резервирование, в котором используется списываемый путь к хранилищу, и щелкните **Изменить**.
3. Перейдите на вкладку **Ресурсы**.
4. Найдите путь к хранилищу, который нужно списать.
5. Щелкните значок **Изменить** (✎).
6. Чтобы деактивировать его использование, установите флажок в столбце «Отключено».
7. Щелкните значок **Сохранить** (✓).
8. Нажмите кнопку **ОК**.
9. Повторите эту процедуру для всех резервирований, использующих списываемый путь к хранилищу.

Сбор данных

vRealize Automation собирает данные из конечных точек источников инфраструктуры и их вычислительных ресурсов.

Сбор данных осуществляется с регулярной периодичностью. Для каждого типа сбора данных задан интервал по умолчанию, который можно переопределить или изменить. Для каждого типа сбора данных также задан интервал времени ожидания по умолчанию, который можно переопределить или изменить.

Администраторы инфраструктуры как услуги могут вручную инициировать сбор данных для конечных точек источников инфраструктуры, а администраторы структур могут вручную инициировать сбор данных для вычислительных ресурсов.

Таблица 1-29. Типы сбора данных

Тип сбора данных	Описание
Сбор данных конечных точек источников инфраструктуры	<p>Обновление информации об узлах виртуализации, шаблонах и образах ISO для сред виртуализации. Обновление виртуальных центров обработки данных и шаблонов для vCloud Director. Обновление областей Amazon и компьютеров, подготовленных в областях Amazon</p> <p>Сбор данных конечных точек запускается каждые 4 часа.</p>
Сбор данных об иерархии	<p>Обновление данных о виртуальных машинах, использование ресурсов которыми связано с определенным вычислительным ресурсом, в том числе подробных сведений о сетях, хранилище и виртуальных машинах. Эти данные также включают в себя информацию о неуправляемых виртуальных машинах, подготовленных не с помощью vRealize Automation.</p> <p>Сбор данных об иерархии запускается каждые 24 часа.</p> <p>Интервал времени ожидания по умолчанию для сбора данных об иерархии составляет 2 часа.</p>
Сбор данных о состоянии	<p>Обновление данных о состоянии питания каждого компьютера, обнаруженного с помощью сбора данных об иерархии. Сбор данных о состоянии также предусматривает запись данных об отсутствующих компьютерах, управление которыми осуществляется с помощью vRealize Automation и которые не могут быть обнаружены на вычислительном ресурсе виртуализации или облачной конечной точке.</p> <p>Сбор данных о состоянии запускается каждые 15 минут.</p> <p>Интервал времени ожидания по умолчанию для сбора данных о состоянии составляет 1 час.</p>
Сбор данных о производительности (только для вычислительных ресурсов vSphere)	<p>Обновление данных о среднем уровне использования ресурсов ЦП, хранилища, памяти и сети для каждой виртуальной машины, обнаруженной с помощью сбора данных об иерархии.</p> <p>Сбор данных о производительности запускается каждые 24 часа.</p> <p>Интервал времени ожидания по умолчанию для сбора данных о производительности составляет 2 часа.</p>

Таблица 1-29. Типы сбора данных (продолжение)

Тип сбора данных	Описание
Сбор данных об инвентаризации сети и системы безопасности (только вычислительные ресурсы vSphere)	Обновление записи данных о сети и безопасности, связанных с vCloud Networking and Security и NSX, в частности информации о группах безопасности и балансировке нагрузки, для каждого компьютера, участвующего в сборе данных об иерархии.
Сбор данных WMI (только для вычислительных ресурсов на базе Windows)	Обновление записи данных управления для каждого компьютера под управлением Windows. Агент WMI должен быть установлен (как правило, на узле службы диспетчера) и включен для сбора данных с компьютеров под управлением Windows.

Запуск сбора данных конечных точек вручную

Сбор данных конечных точек запускается автоматически каждые 4 часа. Тем не менее, администраторы инфраструктуры как услуги в любой момент могут вручную запустить сбор данных конечных точек, для которых не требуется наличие прокси-агентов.

На странице **Сбор данных** содержатся сведения о состоянии и возрасте процессов сбора данных. Здесь также можно вручную запустить новый сбор данных конечной точки.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Щелкните строку конечной точки, для которой требуется выполнить сбор данных.
3. Выберите доступное действие по сбору данных.

Настройка сбора данных вычислительного ресурса

Вы можете активировать или деактивировать сбор данных, настроить частоту сбора данных или вручную отправить запрос на сбор данных.

Страница **Сбор данных** содержит сведения о статусе и сроке сборов данных. На ней можно также настроить сбор данных для ваших вычислительных ресурсов.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора структуры**.

Процедура

1. Выберите **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**.
2. Укажите на вычислительный ресурс, для которого нужно настроить сбор данных, и щелкните **Сбор данных**.

3. Настройте спецификации сбора данных **Вычислительный ресурс.**

- Чтобы активировать сбор данных, выберите вариант **Включено**.
- Чтобы деактивировать сбор данных, выберите вариант **Отключено**.

4. Настройте сбор данных **Иерархия.**

- Чтобы активировать сбор данных, выберите вариант **Включено**.
- Чтобы деактивировать сбор данных, выберите вариант **Отключено**.
- Введите число в текстовом поле **Частота**, чтобы настроить интервал времени (в часах) между сборами данных об иерархии.
- Чтобы запустить сбор данных вручную, щелкните **Запросить сейчас**.

5. Настройте сбор данных **Состояние.**

- Чтобы активировать сбор данных, выберите вариант **Включено**.
- Чтобы деактивировать сбор данных, выберите вариант **Отключено**.
- Введите число в текстовом поле **Частота**, чтобы настроить интервал времени (в минутах) между сборами данных о состоянии.
- Чтобы запустить сбор данных вручную, щелкните **Запросить сейчас**.

6. Настройте сбор данных **Производительность.**

Этот сбор данных доступен только для интеграции с vSphere.

- Чтобы активировать сбор данных, выберите вариант **Включено**.
- Чтобы деактивировать сбор данных, выберите вариант **Отключено**.
- Введите число в текстовом поле **Частота**, чтобы настроить интервал времени (в часах) между сборами данных о производительности.
- Чтобы запустить сбор данных вручную, щелкните **Запросить сейчас**.

7. Настройте сбор данных **Иерархия моментальных снимков.**

Этот вариант доступен для вычислительных ресурсов, управляемых решением vRealize Business for Cloud.

- Чтобы активировать сбор данных, выберите вариант **Включено**.
- Чтобы деактивировать сбор данных, выберите вариант **Отключено**.
- Введите число в текстовом поле **Частота**, чтобы настроить интервал времени (в часах) между сборами данных о моментальных снимках.
- Чтобы запустить сбор данных вручную, щелкните **Запросить сейчас**.

8. Нажмите кнопку **ОК.**

Обновление данных о затратах для всех вычислительных ресурсов

Администраторы структуры могут вручную обновить сведения о затратах для всех вычислительных ресурсов под управлением vRealize Business for Cloud.

Необходимые условия

Войдите в службу vRealize Automation в качестве **администратора структуры**.

Процедура

1. Выберите **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**.
2. Щелкните элемент **Обновить затраты**.
3. Щелкните элемент **Запросить сейчас**.

Результаты

После завершения обновления затрат состояние изменится на «Успешно».

Общие сведения о проверке выделения vSwap для конечных точек vCenter Server

С помощью vSwap можно определить доступность пространства в области подкачки для создания на целевом компьютере файла подкачки максимального размера. Проверка vSwap выполняется при создании или изменении конфигурации виртуальной машины из vRealize Automation. Проверка выделения vSwap доступна только для конечных точек vCenter Server.

При выделении ресурсов хранилища vRealize Automation проверяется, доступно ли достаточное пространство в хранилище данных для размещения дисков виртуальных машин в случае запроса на создание или перенастройку. Тем не менее, если при включении компьютера недостаточно пространства для создания файла подкачки в конечной точке vCenter Server, включить машину не удастся. При сбое операции включения все процедуры настройки, которые зависят от этого компьютера, также заканчиваются сбоем. Компьютер также может быть списан. В зависимости от размера запрашиваемого пространства тот факт, что компьютер не включается или не подготавливается, не всегда очевиден сразу.

Чтобы преодолеть эти ограничения, можно использовать проверку выделения vSwap, которая позволяет определить доступность пространства подкачки для создания файла подкачки максимального размера в процессе создания и перенастройки vRealize Automation для конечных точек vCenter Server. Чтобы включить проверку выделения vSwap, установите для настраиваемого свойства `VirtualMachine.Storage.ReserveMemory` значение `True` в компоненте компьютера или общей схеме элементов.

Рассмотрим следующие варианты поведения для проверок выделения vSwap:

- Файл подкачки находится в хранилище, которое содержит виртуальную машину. Изменение конфигураций vCenter Server для размещения файлов подкачки в выделенном или другом хранилище не поддерживается.
- Размер файла подкачки учитывается при создании или перенастройке виртуальной машины. Максимальный размер файла подкачки — это размер памяти виртуальной машины.

- Зарезервированные значения для резервирования хранилища vRealize Automation на узле не должны превышать физическую емкость вычислительного ресурса.
- При создании резервирования сумма зарезервированных значений не должна превышать доступное пространство хранилища.
- Резервирования памяти на уровне пула ресурсов, узла или виртуальной машины в vSphere не собраны из конечной точки vSphere и не учитываются при расчетах в vRealize Automation.
- vSwap не проверяет пространство подкачки, которое доступно во время операций включения для существующих компьютеров.
- Чтобы учесть любые изменения, внесенные в связи с vSwap в конечной точке vSphere, необходимо повторно запустить сбор данных.

Удаление расположений центров обработки данных

Чтобы удалить расположение центра обработки данных с пользовательского меню, системный администратор должен удалить сведения о расположении из файла расположений, а администратор структуры — с вычислительного ресурса.

Например, добавив значение London в файл расположений, следует привязать десять вычислительных ресурсов к этому расположению, после чего удалить это расположение из файла. При этом вычислительные ресурсы по-прежнему будут привязаны к London как к месту расположения и это расположение все еще будет включено в раскрывающийся список на странице «Подтверждения запроса компьютера». Чтобы удалить расположение из раскрывающегося списка, администратор структуры должен внести изменения в вычислительный ресурс и выполнить сброс значения параметра Location для всех вычислительных ресурсов, связанных с этим расположением.

Ниже приведен общий обзор ряда действий, необходимых для удаления расположения центра обработки данных.

1. Системный администратор удаляет сведения о расположении центра обработки данных из файла расположений.
2. Администратор структуры удаляет связи с вычислительными ресурсами с их расположения путем внесения изменений в расположение каждого вычислительного ресурса.

Мониторинг контейнеров

Пользователь может контролировать состояние контейнера, созданного им в Контейнеры для vRealize Automation.

После создания контейнеров на основе шаблона можно контролировать их состояние. Щелкнув надпись **Сведения** на контейнере, можно контролировать такие параметры, как пропускная способность сети, использование ЦП и памяти, а также просматривать журналы и свойства данного контейнера.

Массовый импорт, обновление или перенос виртуальных машин

Можно использовать функцию Операции массового импорта для импорта, обновления или переноса виртуальных машин на vRealize Automation. Операции массового импорта позволяет оптимизировать управление несколькими компьютерами в нескольких средах.

Операции массового импорта создает CSV-файл, содержащий данные о виртуальных машинах, такие как резервирование, путь к хранилищу, схема элементов, владелец и различные настраиваемые свойства. Используйте CSV-файл для импорта виртуальных машин в среду vRealize Automation. Операции массового импорта поддерживает следующие задачи администрирования:

- импорт одной или нескольких неуправляемых виртуальных машин для управления ими в среде vRealize Automation;
- Внесение глобальных изменений в свойство виртуальных машин, например изменение пути к хранилищу.
- Перенос виртуальной машины из одной среды vRealize Automation в другую.

Примечание Массовый импорт поддерживается только в vCloud Director и vSphere. При настройке фильтра для другого типа конечной точки данные не заносятся в CSV-файл.

Команды функции Операции массового импорта можно выполнять с помощью консоли vRealize Automation или интерфейса командной строки CloudUtil. Дополнительные сведения об использовании интерфейса командной строки CloudUtil см. в документации по *Увеличение жизненного цикла*.

Примечание При массовом импорте компьютеров обычные шаги подготовки не пропускаются. Все существующие внешние рабочие процессы, запускаемые брокером событий во время подготовки, выполняются для импортированных компьютеров. Чтобы временно деактивировать рабочие процессы для импортированных компьютеров, выполните одно из следующих действий.

- Деактивируйте все подписки брокера событий. При деактивации подписок необходимо запланировать отключение службы в кластере vRealize Automation, так как расширяемость не применяется ни для одного обычного компьютера, подготовленного в течение этого времени.
 - Добавьте условие, чтобы подписки на события не запускались во время импорта компьютера. Чтобы добавить это условие, перейдите к подпискам на события, выберите подписку для деактивации и добавьте настраиваемое свойство `VirtualMachine.Imported.ConvergedBlueprint`, значение которого не равно <идентификатор схемы элементов импорта>. Это условие не влияет на компьютеры, подготовленные обычным образом, а применяется только к импортированным компьютерам.
-

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры и диспетчера бизнес-групп**.

- При импорте виртуальных машин, использующих статические IP-адреса, нужно подготовить правильно настроенный пул адресов.

Импорт виртуальной машины в среду vRealize Automation

Неуправляемую виртуальную машину можно импортировать в среду vRealize Automation.

Неуправляемая виртуальная машина существует в гипервизоре, но ей невозможно управлять в среде vRealize Automation, и ее невозможно просматривать в консоли. После импорта неуправляемой виртуальной машины ею управляют с помощью интерфейса управления vRealize Automation. В зависимости от привилегий виртуальная машина отображается на вкладках **Управляемые компьютеры** или **Развертывания**.

Параметр массового импорта не поддерживается для развертываний, подготовленных из схемы элементов, которая содержит компонент сети и безопасности NSX или компонент программного обеспечения.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры и диспетчера бизнес-групп**.
- При импорте виртуальных машин, использующих статические IP-адреса, нужно подготовить правильно настроенный пул адресов. Дополнительные сведения об использовании профиля сети для управления диапазонами IP-адресов см. в разделе *Настройка vRealize Automation*.
- При использовании массового импорта для импорта виртуальной машины со статическим IP-адресом, выделенным для другой ВМ, произойдет сбой.

Процедура

1. Временно деактивируйте все подписки брокера событий.

Примечание При отключении подписок необходимо запланировать отключение службы для кластера vRealize Automation. Во время этого процесса расширяемость не применяется к компьютерам, подготовленным обычным образом. Сбой деактивации подписок может привести к потере данных и безвозвратному удалению компьютеров из резервной инфраструктуры.

2. Создайте CSV-файл данных виртуальной машины.
 - а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
 - б) Щелкните **Создать CSV-файл**.
 - в) В раскрывающемся меню **Компьютеры** выберите значение **Не управляется**.
 - г) В этом же раскрывающемся меню выберите значение по умолчанию в поле **Бизнес-группа**.
 - д) Введите значение по умолчанию в поле **Владелец**.
 - е) В этом же раскрывающемся меню выберите значение по умолчанию в поле **Схема элементов**.
Необходимо опубликовать схему элементов и добавить для нее право на импорт.

- ж) В этом же раскрываемом меню выберите значение по умолчанию в поле **Компьютер компонента**.

При выборе значения для элементов **Бизнес-группа** и **Схема элементов** в CSV-файле данных отобразятся следующие результаты:

- Host Reservation (Name or ID) = INVALID_RESERVATION
- Host To Storage (Name or ID) = INVALID_HOST_RESERVATION_TO_STORAGE

Эти сообщения отображаются, если в выбранной бизнес-группе нет резервирования для узла, на котором также размещена неуправляемая виртуальная машина. Если в этой бизнес-группе есть резервирование для узла неуправляемой виртуальной машины, значения «Резервирование узла» и «Хранилище для узла» будут заданы правильно.

- з) Выберите один из доступных типов ресурсов в раскрываемом меню **Ресурсы**.

Пункт меню	Описание
Конечная точка	Информация, необходимая для доступа к узлу виртуализации.
Вычислительный ресурс	Информация, необходимая для доступа к группе виртуальных машин, выполняющих аналогичную функцию.

- и) Выберите имя ресурса виртуальной машины в раскрываемом меню **Имя**.
- к) Нажмите кнопку **ОК**.

3. Отредактируйте CSV-файл данных виртуальной машины.

- а) Откройте CSV-файл и измените категории данных, чтобы они соответствовали существующим категориям в целевой среде vRealize Automation.

Для импорта виртуальных машин, содержащихся в CSV-файле данных, каждая виртуальная машина должна быть связана со следующими элементами:

- Резервирование
- Расположение хранилища
- Схема элементов
- Компонент виртуальной машины
- Владелец, существующий в целевом развертывании

Для успешного выполнения импорта в целевой среде vRealize Automation должны быть заданы все значения каждой виртуальной машины. Отредактировав CSV-файл, можно изменить значения для резервирования, места хранения, схемы элементов и владельца или добавить значение статического IP-адреса для отдельных виртуальных машин.

Заголовок	Комментарий
# Import—Yes or No	Выберите значение «Нет», чтобы предотвратить импорт определенной виртуальной машины.
Имя виртуальной машины	Оставьте без изменений.
Идентификатор виртуальной машины	Оставьте без изменений.
Резервирование узла (имя или идентификатор)	Введите имя или идентификатор резервирования в целевой среде vRealize Automation.
Хранилище для узла (имя или идентификатор)	Введите имя или идентификатор расположения хранилища в целевой среде vRealize Automation.
Имя развертывания	Введите новое имя для развертывания, например имя виртуальной машины, созданной в целевой среде vRealize Automation. Примечание Каждую виртуальную машину необходимо импортировать в собственное развертывание. Нельзя импортировать виртуальную машину в существующее развертывание. Нельзя импортировать несколько виртуальных машин в одно развертывание.
Идентификатор схемы элементов	Введите идентификатор схемы элементов в целевой среде vRealize Automation, который используется для импорта виртуальной машины. Примечание Необходимо ввести не имя схемы элементов, а только ее идентификатор. Необходимо выбрать схему элементов, которая содержит только один компонент виртуальной машины. Схема элементов должна быть опубликована, и к ней должны быть добавлены права. Для импортированных виртуальных машин не связывайте схему элементов, которая включает в себя профили компонентов. Существующие параметры импортированных виртуальных машин (например, объем памяти или хранилища) могут выходить за пределы профиля. Если такое происходит, проверка любой будущей перенастройки виртуальных машин на основе схем элементов будет завершена с ошибкой.

Заголовок	Комментарий
Идентификатор компьютера компонента	Введите имя компонента виртуальной машины, который содержится в выбранной схеме элементов. Нельзя импортировать виртуальную машину в схему элементов с несколькими компонентами.
Имя владельца	В целевой среде vRealize Automation введите пользователя, которому предоставлены права на схему элементов.

При импорте виртуальной машины с одним или несколькими настраиваемыми свойствами необходимо определить каждое настраиваемое свойство с помощью трех разделенных запятыми значений, которые добавляются к строке со значениями для этого компьютера. Используйте этот формат для каждого настраиваемого свойства.

,Имя.настраиваемого.свойства, Значение, ФЛАГИ

ФЛАГИ — это три символа, которые описывают, как свойство воспринимается vRealize Automation. По использованию флаги делятся на следующие группы.

1. Н или N = скрытые или нескрытые
2. Е или О = зашифрованные или незашифрованные
3. R или P = с временем выполнения или без времени выполнения

Например, можно добавить настраиваемое свойство, чтобы настроить статический IP-адрес для компьютера. При использовании следующего формата это настраиваемое свойство выделяет доступный статический IP-адрес из профиля сети.

,VirtualMachine.Network#.Address, w.x.y.z, НОР

Настройте команду с соответствующей информацией для своей виртуальной машины.

- Замените # на номер сетевого интерфейса, который настроен для этого статического IP-адреса. Например, VirtualMachine.Network0.Address.
- Замените w.x.y.z на статический IP-адрес виртуальной машины. Например, 11.27.42.57.

Строка флагов НОР (скрыто, не зашифровано, без среды выполнения) задает видимость свойства. Поскольку это конкретное свойство используется только для массового импорта, оно удаляется с виртуальной машины после успешного импорта.

Чтобы это настраиваемое свойство сработало, IP-адрес должен быть доступен в верно настроенном пуле адресов. Если адрес не удастся найти или он уже используется, импорт продолжается без определения статического IP-адреса и при этом регистрируется ошибка.

- б) Сохраните CSV-файл.
4. Используйте интерфейс управления vRealize Automation, чтобы импортировать виртуальную машину в среду vRealize Automation.
 - а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
 - б) Нажмите кнопку **Создать**.
 - в) В текстовом поле **Имя** введите уникальное имя для выполнения этой задачи, например **неуправляемый импорт = 10**.

- г) Найдите имя CSV-файла и введите его в текстовом поле **CSV-файл**.
- д) Выберите параметры импорта.

Параметр	Описание
Время начала	Планирование будущей даты начала. Выбранное время начала — это местное время сервера, а не местное время рабочей станции пользователя.
Сейчас	Сразу же начинайте процесс импорта.
Задержка (с)	При импорте множества виртуальных машин выберите количество секунд задержки регистрации каждой виртуальной машины. При выборе этого пункта меню процесс импорта замедляется. Чтобы задержки не было, оставьте поле пустым.
Размер пакета	При импорте множества виртуальных машин выберите общее количество виртуальных машин для регистрации в данный момент. При выборе этого пункта меню процесс импорта замедляется. Чтобы ограничения не было, оставьте поле пустым.
Игнорировать управляемые компьютеры	Оставьте не выбранными.
Пропустить проверку пользователя	Выбор этого пункта меню позволяет задать для владельца виртуальной машины значение, указанное в столбце «Владелец» в списке CSV-файла данных, не проверяя наличие такого пользователя. Выбрав этот пункт меню, можно сократить время импорта.
Проверить импорт	Проверьте процесс импорта без импорта виртуальных машин, чтобы убедиться в отсутствии ошибок в CSV-файле.

- е) Нажмите кнопку **ОК**.

Информация о процессе отображается на странице Операции массового импорта.

Обновление виртуальной машины в среде vRealize Automation

Можно изменить свойство виртуальной машины, например путь к хранилищу, чтобы обновить одну или несколько управляемых виртуальных машин в среде vRealize Automation.

Управляемая виртуальная машина является компьютером, которым можно управлять в среде vRealize Automation, и который можно просматривать в консоли.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры и диспетчера бизнес-групп**.

Процедура

1. Создайте CSV-файл данных виртуальной машины.
 - а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
 - б) Щелкните **Создать CSV-файл**.
 - в) В раскрывающемся меню **Компьютеры** выберите значение **Управляется**.

- г) Выберите один из доступных типов ресурсов в раскрывающемся меню **Ресурсы**.

Параметр	Описание
Конечная точка	Информация, необходимая для доступа к узлу виртуализации.
Вычислительный ресурс	Информация, необходимая для доступа к группе виртуальных машин, выполняющих аналогичную функцию.

- д) Выберите имя ресурса виртуальной машины в раскрывающемся меню **Имя**.
- е) (Необязательно). Выберите **Включить в состав настраиваемые свойства** при необходимости переноса настраиваемых свойств виртуальной машины.
- ж) Нажмите кнопку **ОК**.

2. Отредактируйте CSV-файл данных виртуальной машины.

- а) Откройте CSV-файл в текстовом редакторе и отредактируйте категории данных, которые необходимо изменить в глобально.

Для обновления виртуальных машин, содержащихся в CSV-файле данных, каждая машина должна быть связана со следующими элементами:

- Резервирование
- Расположение хранилища
- Схема элементов
- Компонент компьютера
- Владелец, существующий в целевом развертывании

Для успешного выполнения обновления в целевой среде vRealize Automation должны быть заданы все значения каждого компьютера. Отредактировав CSV-файл, можно изменить значения для резервирования, места хранения, схемы элементов и владельца или добавить значение статического IP-адреса для отдельных компьютеров.

- б) При изменении виртуальной машины со статическим IP-адресом добавьте в CSV-файл команду в следующем виде.

```
,VirtualMachine.Network#.Address, w.x.y.z, NOP
```

Настройте команду с соответствующей информацией для своей виртуальной машины.

- Замените # на номер сетевого интерфейса, который настроен для этого статического IP-адреса. Например, VirtualMachineNetwork0.Address.
- Замените w.x.y.z на статический IP-адрес виртуальной машины. Например, 11.27.42.57.
- Строка *NOP* (скрытый, не зашифровано, без среды выполнения) задает видимость свойства. После успешного импорта это свойство по умолчанию удаляется из виртуальной машины.

Для успешного обновления IP-адрес должен быть доступен в правильно настроенном пуле адресов. Если адрес не удастся найти или он уже используется, обновление продолжается без определения статического IP-адреса и при этом регистрируется ошибка.

- в) Сохраните CSV-файл и закройте текстовый редактор.

3. Используйте интерфейс управления vRealize Automation, чтобы обновить одну или несколько виртуальных машин в среде vRealize Automation.

- а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
- б) Нажмите кнопку **Создать**.
- в) В текстовом поле **Имя** введите уникальное имя для выполнения этой задачи, например управляемое глобальное обновление 10.
- г) Найдите имя CSV-файла и введите его в текстовом поле **CSV-файл**.

д) Выберите параметры импорта.

Параметр	Описание
Время начала	Планирование будущей даты начала. Указанное время начала — это местное время сервера, а не местное время рабочей станции пользователя.
Сейчас	Сразу же начинайте процесс импорта.
Задержка (с)	При обновлении большого количества виртуальных машин выберите количество секунд задержки регистрации каждой виртуальной машины. При выборе этого параметра процесс обновления замедляется. Чтобы задержки не было, оставьте поле пустым.
Размер пакета	При обновлении большого количества виртуальных машин выберите общее количество компьютеров для регистрации в данный момент. При выборе этого параметра процесс обновления замедляется. Чтобы ограничения не было, оставьте поле пустым.
Игнорировать управляемые компьютеры	Оставьте не выбранными.
Пропустить проверку пользователя	Выбор этого параметра позволяет задать для владельца компьютера значение, указанное в столбце «Владелец» в списке CSV-файла данных, не проверяя наличие такого пользователя. Выбрав этот параметр, можно сократить время обновления.
Проверить импорт	Оставьте не выбранными.

е) Нажмите кнопку **ОК**.

Информация о процессе импорта будет отображаться на странице «Массовый импорт».

Перенос виртуальной машины в другую среду vRealize Automation

Можно перенести одну или несколько управляемых виртуальных машин из среды VMware vRealize™ Automation в другую среду vRealize Automation.

Управляемая виртуальная машина является виртуальной машиной, которой можно управлять в среде vRealize Automation, и которую можно просматривать на консоли.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры и диспетчера бизнес-групп**.
- При импорте виртуальных машин, использующих статические IP-адреса, нужно подготовить правильно настроенный пул адресов. Дополнительные сведения об использовании профиля сети для управления диапазонами IP-адресов см. в разделе *Настройка vRealize Automation*.

Процедура

1. Создайте CSV-файл данных виртуальной машины.
 - а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
 - б) Щелкните **Создать CSV-файл**.

- в) В раскрывающемся меню **Компьютеры** выберите значение **Управляется**.
- г) Выберите один из доступных типов ресурсов в раскрывающемся меню **Ресурсы**.

Параметр	Описание
Конечная точка	Информация, необходимая для доступа к узлу виртуализации.
Вычислительный ресурс	Информация, необходимая для доступа к группе виртуальных машин, выполняющих аналогичную функцию.

- д) Выберите имя ресурса виртуальной машины в раскрывающемся меню **Имя**.
- е) При необходимости выберите **Включить настраиваемые свойства**.

Включите в состав настраиваемые свойства при импорте виртуальной машины в новое развертывание с теми же свойствами.

- ж) Нажмите кнопку **ОК**.

2. Отредактируйте CSV-файл данных виртуальной машины.

Необходимость редактирования CSV-файла данных зависит от сходства исходной и целевой сред. Если значения конфигурации в исходной среде не совпадают со значениями в целевой, перед началом переноса необходимо отредактировать CSV-файл данных, чтобы значения совпадали.

- а) Откройте CSV-файл и измените категории данных, чтобы они соответствовали существующим категориям в целевой среде vRealize Automation.

Чтобы переносить виртуальные машины, содержащиеся в CSV-файле данных, с каждой виртуальной машиной должны быть связаны резервирование, место хранения, схема элементов, компонент компьютера и владелец, который существует в целевой среде vRealize Automation. Для успешного выполнения переноса в целевой среде vRealize Automation должны быть заданы все значения каждой виртуальной машины. Отредактировав CSV-файл, можно изменить значения для резервирования, места хранения, схемы элементов и владельца или добавить значение статического IP-адреса для отдельных виртуальных машин.

Заголовок	Комментарий	Пример
№ импорта — «Да» или «Нет»	Выберите значение «Нет», чтобы предотвратить импорт определенной виртуальной машины.	Да
Имя виртуальной машины	Оставьте без изменений.	MyMachine
Идентификатор виртуальной машины	Оставьте без изменений.	a6e05812-0b06-4d4e-a84a-fed242340426a
Резервирование узла (имя или идентификатор)	Введите имя или идентификатор резервирования в целевой среде vRealize Automation.	DevReservation
Хранилище для узла (имя или идентификатор)	Введите имя или идентификатор расположения хранилища в целевой среде vRealize Automation.	ce-san-1:custom-nfs-2
Имя развертывания	Введите новое имя для развертывания, которое создается в целевой среде vRealize Automation. Каждую виртуальную машину необходимо перенести в собственное развертывание. Нельзя импортировать виртуальную машину в существующее развертывание. Нельзя импортировать несколько виртуальных машин в одну среду.	ImportedDeployment0001
Идентификатор конвергированной схемы элементов	Введите идентификатор схемы элементов в целевой среде vRealize Automation, который используется для импорта виртуальной машины. Убедитесь, что введен только идентификатор схемы элементов. Не вводите имя схемы элементов. Необходимо выбрать схему элементов, которая содержит только один компонент виртуальной машины. Схема элементов должна быть опубликована, и к ней должны быть добавлены права.	ImportBlueprint

Заголовок	Комментарий	Пример
Идентификатор компонента схемы элементов	Введите имя компонента виртуальной машины, который содержится в выбранной схеме элементов. Нельзя импортировать виртуальную машину в схему элементов с несколькими компонентами.	ImportedMachine
Имя владельца	Введите пользователя в целевой среде vRealize Automation.	user@tenant

Образец полной, правильно отформатированной строки CSV: Yes, MyMachine, a6e05812-0b06-4d4e-a84a-fed242340426, DevReservation, ce-san-1:custom-nfs-2, Imported Deployment 0001, ImportBlueprint, ImportedMachine, user@tenant

- б) При переносе виртуальной машины со статическим IP-адресом добавьте в CSV-файл команду в следующем виде.

```
,VirtualMachine.Network#.Address, w.x.y.z, HOP
```

Настройте команду с соответствующей информацией для своей виртуальной машины.

- Замените # на номер сетевого интерфейса, который настроен для этого статического IP-адреса. Например, VirtualMachineNetwork0.Address.
- Замените w.x.y.z на статический IP-адрес виртуальной машины. Например, 11.27.42.57.
- Строка HOP (скрытый, не зашифровано, без среды выполнения) задает видимость свойства. После успешного импорта это свойство по умолчанию удаляется из виртуальной машины.

Для успешного переноса IP-адрес должен быть доступен в правильно настроенном пуле адресов. Если адрес не удастся найти или он уже используется, перенос продолжается без определения статического IP-адреса и при этом регистрируется ошибка.

- в) Сохраните CSV-файл.

3. Используйте интерфейс управления vRealize Automation, чтобы перенести виртуальную машину в среду vRealize Automation.

- а) Выберите **Инфраструктура > Администрирование > Операции массового импорта**.
- б) Нажмите кнопку **Создать**.
- в) В текстовом поле **Имя** введите уникальное имя для выполнения этой задачи, например управляемый перенос 10.
- г) Найдите имя CSV-файла и введите его в текстовом поле **CSV-файл**.

д) Выберите параметры импорта.

Параметр	Описание
Время начала	Планирование будущей даты начала. Выбранное время начала — это местное время сервера, а не местное время рабочей станции пользователя.
Сейчас	Сразу можно приступить к процессу переноса.
Задержка (с)	При переносе множества виртуальных машин выберите количество секунд задержки регистрации каждой виртуальной машины. При выборе этого параметра процесс переноса замедляется. Чтобы задержки не было, оставьте поле пустым.
Размер пакета	При переносе множества виртуальных машин выберите общее количество виртуальных машин для регистрации в данный момент. При выборе этого параметра процесс переноса замедляется. Чтобы ограничения не было, оставьте поле пустым.
Игнорировать управляемые компьютеры	Оставьте не выбранными.
Пропустить проверку пользователя	Выбор этого параметра позволяет задать для владельца виртуальной машины значение, указанное в столбце «Владелец» в списке CSV-файла данных, не проверяя наличие такого пользователя. Выбрав этот параметр, можно сократить время переноса.
Проверить импорт	Проверьте процесс переноса без переноса виртуальных машин, чтобы убедиться в отсутствии ошибок в CSV-файле.

е) Нажмите кнопку **ОК**.

Информация о процессе импорта будет отображаться на странице «Массовый импорт».