

Настройка 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

Настройка vRealize Automation 6

Обновленные сведения 7

1 Внешние приготовления к подготовке схемы элементов 8

Подготовка среды для управления vRealize Automation 8

Контрольный список для подготовки к настройке сети и системы безопасности NSX 10

Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами 15

Контрольный список для настройки Контейнеры для vRealize Automation 19

Подготовка среды vCloud Director к использованию vRealize Automation 20

Подготовка среды vCloud Air к использованию vRealize Automation 21

Подготовка среды Amazon Web Services 21

Подготовка возможностей сети и обеспечения безопасности Red Hat OpenStack 28

Подготовка среды SCVMM 29

Настройка подключения VPC «сеть к Azure» 30

Подготовка к процессу подготовки компьютера 31

Выбор необходимого метода подготовки компьютера 32

Контрольный список для запуска сценариев Visual Basic во время подготовки 35

Подготовка с помощью гостевого агента vRealize Automation 36

Контрольный список для подготовки к процессу подготовки путем клонирования 45

Подготовка к резервированию vCloud Air и vCloud Director 60

Подготовка к процессу подготовки Linux Kickstart 61

Подготовка к процессу подготовки SCCM 64

Подготовка к процессу подготовки WIM 65

Подготовка к процессу подготовки образов виртуальных машин 73

Подготовка к процессу подготовки образов компьютеров Amazon 74

Сценарий: работа с ресурсами vSphere для подготовки компьютера 76

Подготовка к процессу подготовки Программное обеспечение 79

Подготовка к процессу подготовки компьютеров с Программное обеспечение 80

Подготовка шаблона vSphere для клонированного компьютера и схем элементов программных компонентов 84

Сценарий: подготовка к импорту схемы элементов образца приложения Dukes Bank для vSphere 88

2 Приготовление арендатора и ресурса для подготовки схемы элементов 94

Настройка параметров арендатора 94

Выбор вариантов настройки службы управления каталогами 95

Обновление внешних соединителей для управления каталогами 165

Сценарий: настройка ссылки Active Directory для обеспечения высокой доступности vRealize Automation	173
Настройка внешних соединителей для проверки подлинности с помощью смарт-карты и сторонних поставщиков удостоверений в vRealize Automation	176
Создание ссылки на Active Directory в нескольких доменах или лесах	183
Настройка групп и ролей пользователей	186
Создание дополнительных арендаторов	194
Удаление арендатора	197
Настройка параметров безопасности в средах с несколькими арендаторами	197
Настройка пользовательской фирменной символики	198
Контрольный список для настройки уведомлений	200
Создание настраиваемого RDP-файла для поддержки подключений RDP для подготовленных компьютеров	211
Сценарий: добавление данных о расположении центра обработки данных при развертываниях в нескольких регионах	212
Настройка vRealize Orchestrator	214
Настройка ресурсов	218
Контрольный список для настройки ресурсов инфраструктуры как услуги	218
Настройка ресурсов Все как услуга	367
Создание и настройка контейнеров	380
Установка дополнительных подключаемых модулей на заданный по умолчанию сервер vRealize Orchestrator	404
Работа с политиками Active Directory	404
Параметры пользователя для уведомлений и делегатов	408
3 Предоставление пользователям схем элементов служб	409
Проектирование схем элементов	409
Создание библиотеки проектов	412
Проектирование схем элементов компьютера	414
Проектирование компонентов Программное обеспечение	534
Проектирование схем элементов и действий ресурсов Все как услуга	549
Публикация схемы элементов	615
Работа со схемами элементов, создаваемыми разработчиками	616
Экспорт и импорт схем элементов и содержимого	616
Загрузка и настройка стандартной автономной схемы элементов	622
Создание схем элементов и другого контента инфраструктуры как услуги в среде для нескольких разработчиков	623
Сборка составных схем элементов	623
Общие сведения о поведении вложенных схем элементов	625
Использование компонентов компьютера и компонентов Программное обеспечение при сборке схемы элементов	628
Создание привязки свойств между компонентами схемы элементов	629
Создание зависимостей и управление порядком подготовки	630
Настройка форм запроса схем элементов	632

Создание настраиваемой формы запроса с параметрами Active Directory	635
Свойства полей в конструкторе настраиваемых форм	645
Использование действий vRealize Orchestrator в конструкторе настраиваемых форм	651
Использование средства выбора значений или древовидного средства выбора в конструкторе настраиваемых форм	653
Использование элемента сетки данных в конструкторе пользовательских форм	655
Использование внешней проверки в конструкторе настраиваемых форм	660
Тестирование и устранение неполадок неудачных запросов на подготовку	664
Как работает действие «Возобновить»	668
Принудительное удаление развертывания после неудачного запроса на удаление	670
Устранение неполадок при неудачном развертывании, включающем рабочий процесс vRealize Orchestrator	671
Управление каталогом служб	671
Контрольный список для настройки каталога служб	672
Создание служб	673
Работа с элементами каталога и действиями	676
Создание прав	679
Работа с политиками подтверждения	687
Запрос подготовки компьютера с помощью параметризованной схемы элементов	716
Сценарий: предоставление доступа к CentOS со схемой элементов приложения MySQL в каталоге служб	718

4 Использование каталога и управление развертываниями 723

Работа с каталогом	724
Отправка запроса в каталог	725
Работа с развертываниями	727
Мониторинг запросов на подготовку	727
Управление развернутыми элементами каталога	731
Работа с папкой "Входящие"	777

Настройка vRealize Automation

Настройка vRealize Automation содержит сведения о настройке vRealize Automation и внешних сред для подготовки к процессу подготовки vRealize Automation и управления каталогом.

Целевая аудитория

Эти сведения предназначены для ИТ-специалистов, которые отвечают за настройку среды vRealize Automation, а также для администраторов инфраструктуры, отвечающих за подготовку элементов в существующей инфраструктуре, которые будут использоваться при подготовке vRealize Automation. Эта информация предназначена для опытных системных администраторов сред Windows и Linux, знакомых с технологией виртуальных машин и функционированием центра обработки данных.

Обновленные сведения

В следующей таблице приведены изменения, внесенные в *Настройка vRealize Automation* для этого выпуска продукта.

Редакция	Описание
XX подлежит уточнению 202X	Обновлен раздел Настройка поставщика показателей .
14 февраля 2020 г.	<ul style="list-style-type: none">■ Обновлен раздел Просмотр вычислительных ресурсов и запуск сбора данных.■ Обновлен раздел Создание конечной точки NSX-T и настройка связи с конечной точкой vSphere в vRealize Automation.
24 октября 2019 г.	<ul style="list-style-type: none">■ Добавлен элемент Устранение неполадок, связанных с неожиданными записями для фильтрации.■ Незначительные изменения и обновления текста.
9 сентября 2019 г.	<ul style="list-style-type: none">■ Добавлен элемент Настройка конечной точки Microsoft Azure.■ Незначительные изменения текста.
18 июля 2019 г.	Приведены разъяснения по поводу параметра распространения значений в Настройки свойств схемы элементов .
14 июня 2019 г.	Незначительные изменения текста.
30 мая 2019 г.	<ul style="list-style-type: none">■ Добавлен раздел о сопоставлении с использованием подстановочных знаков для динамически добавляемых пользователей. См. раздел Сопоставления с использованием подстановочных знаков для динамически добавляемых пользователей
7 мая 2019 г.	<ul style="list-style-type: none">■ Исправлено несколько гиперссылок.■ Обновлен Подготовка к процессу подготовки SCCM для описания недавно добавленных свойств конфигурации.
11 апреля 2019 г.	Первоначальная редакция документа.

Внешние приготовления к подготовке схемы элементов

1

Возможно, чтобы обеспечить подготовку элементов каталога, понадобится создать или подготовить некоторые элементы за пределами vRealize Automation. Например, если необходимо предоставить элемент каталога для подготовки клонированного компьютера, нужно создать на гипервизоре шаблон для клонирования.

В эту главу входят следующие разделы:

- [Подготовка среды для управления vRealize Automation](#)
- [Настройка подключения VPC «сеть к Azure»](#)
- [Подготовка к процессу подготовки компьютера](#)
- [Подготовка к процессу подготовки Программное обеспечение](#)

Подготовка среды для управления vRealize Automation

В зависимости от рабочей среды может потребоваться внести некоторые изменения в конфигурацию перед переводом среды под управление vRealize Automation или перед использованием некоторых функций.

Таблица 1-1. Подготовка среды для интеграции vRealize Automation







Среда	Подготовка
 NSX for vSphere и NSX-T	<p>Если вы хотите использовать NSX for vSphere или NSX-T для управления сетью, безопасностью и подсистемой балансировки нагрузки на виртуальных машинах, подготовленных с помощью vRealize Automation, подготовьте экземпляр NSX для интеграции. См. раздел Контрольный список для подготовки к настройке сети и системы безопасности NSX.</p>
 vCloud Director	<p>Установите и настройте экземпляр vCloud Director, настройте vSphere и облачные ресурсы, а также укажите или создайте соответствующие учетные данные, чтобы обеспечить для vRealize Automation доступ к среде vCloud Director. См. раздел Подготовка среды vCloud Director к использованию vRealize Automation.</p>
 vCloud Air	<p>Зарегистрируйтесь, чтобы создать учетную запись vCloud Air, настройте среду vCloud Air, а также укажите или создайте соответствующие учетные данные, чтобы обеспечить для vRealize Automation доступ к этой среде. См. раздел Подготовка к резервированию vCloud Air и vCloud Director.</p>
 Amazon Web Services	<p>Подготовьте элементы и роли пользователей в среде Amazon Web Services для использования в vRealize Automation и узнайте, как функции Amazon Web Services сопоставляются с функциями vRealize Automation. См. раздел Подготовка среды Amazon Web Services.</p>
Microsoft Azure	<p>Настройте сеть, чтобы использовать туннели VPN для поддержки компонентов программного обеспечения в схемах элементов Azure. См. раздел Настройка подключения VPC «сеть к Azure».</p>
 Red Hat OpenStack	<p>Чтобы управлять функциями сети и безопасности компьютеров, подготовленных с помощью vRealize Automation, в среде Red Hat OpenStack, необходимо подготовить экземпляр Red Hat OpenStack для интеграции. См. раздел Подготовка возможностей сети и обеспечения безопасности Red Hat OpenStack.</p>

Таблица 1-1. Подготовка среды для интеграции vRealize Automation (продолжение)

Среда	Подготовка
 SCVMM	Необходимо настроить параметры сети и хранилища, а также разобраться с ограничениями при именовании шаблонов и профилей оборудования. См. раздел Подготовка среды SCVMM .
Внешние поставщики управления IP-адресами	Зарегистрируйте пакет или подключаемый модуль внешнего поставщика управления IP-адресами, запустите рабочие процессы конфигурации и зарегистрируйте решение управления IP-адресами в качестве новой конечной точки vRealize Automation. См. раздел Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами .
Другие среды	Вносить изменения в среду не требуется. Подготовку к процессу подготовки компьютеров можно начать с создания шаблонов, сред загрузки или образов компьютеров. См. раздел Подготовка к процессу подготовки компьютера .

Контрольный список для подготовки к настройке сети и системы безопасности NSX

Перед использованием параметров сети и системы безопасности NSX в vRealize Automation необходимо настроить требуемую внешнюю сеть и систему безопасности NSX for vSphere или NSX-T.

Чтобы использовать Все как услуга для расширения интеграции vRealize Automation и NSX for vSphere, установите подключаемый модуль NSX в vRealize Orchestrator. Этот подключаемый модуль не поддерживает NSX-T.

В процессе подготовки к использованию возможностей сети, безопасности и балансировки нагрузки NSX в vRealize Automation при использовании учетных данных диспетчера NSX необходимо использовать учетную запись администратора диспетчера NSX.

vRealize Automation поддерживает NSX for vSphere и NSX-T. Дополнительные сведения о приложении NSX см. в [документации по продукту NSX for vSphere](#) или [документации по продукту NSX-T](#).

Большинство параметров сети и безопасности NSX, которые используются в vRealize Automation, настраиваются извне и становятся доступными после сбора данных на вычислительных ресурсах.

Для получения информации о параметрах NSX, которые можно настроить для схем элементов vRealize Automation, см. раздел [Настройка параметров компонентов сети и безопасности в vRealize Automation](#).

Таблица 1-2. Подготовка контрольного списка сети и системы безопасности NSX

Задача	Расположение	Сведения
<input type="checkbox"/> Настройка параметров сети NSX, в том числе параметров шлюзов и транспортной зоны	Настройте параметры сети в приложении NSX.	<p>В зависимости от продукта NSX см. раздел администрирования в следующей документации по NSX:</p> <ul style="list-style-type: none"> ■ документация по продукту NSX for vSphere ■ документация по продукту NSX-T
<input type="checkbox"/> Создание политик безопасности NSX, тегов и групп	Настройте параметры безопасности в приложении NSX.	<p>В зависимости от продукта NSX см. раздел администрирования в следующей документации по NSX:</p> <ul style="list-style-type: none"> ■ документация по продукту NSX for vSphere ■ документация по продукту NSX-T

Таблица 1-2. Подготовка контрольного списка сети и системы безопасности NSX (продолжение)

Задача	Расположение	Сведения
<input type="checkbox"/> Настройка параметров подсистемы балансировки нагрузки NSX	Настройте параметры подсистемы балансировки нагрузки NSX в приложении NSX.	<p>В зависимости от продукта NSX см. раздел администрирования в следующей документации по NSX:</p> <ul style="list-style-type: none"> ■ документация по продукту NSX for vSphere ■ документация по продукту NSX-T <p>См. также настраиваемые свойства для сети в PDF-документе <i>Справочник по настраиваемым свойствам</i> на сайте docs.vmware.com.</p>
<input type="checkbox"/> При развертывании нескольких виртуальных серверов NSX for vSphere убедитесь, что данному диспетчеру вычислительных ресурсов NSX назначена роль основного диспетчера вычислительных ресурсов NSX.	Для подготовки vRealize Automation необходимо, чтобы диспетчер вычислительных ресурсов NSX для области, в которой находятся компьютеры, был основным диспетчером вычислительных ресурсов NSX.	<p>См. раздел Требования для администраторов при подготовке универсальных объектов NSX for vSphere.</p> <p>См. сведения о развертывании нескольких виртуальных серверов, об универсальных объектах и о роли основного диспетчера NSX в документации по NSX for vSphere.</p>

Установка подключаемого модуля NSX в vRealize Orchestrator

Для установки подключаемого модуля NSX требуется загрузить файл установщика vRealize Orchestrator, передать файл подключаемого модуля с помощью интерфейса конфигурации vRealize Orchestrator и установить подключаемый модуль на сервер vRealize Orchestrator.

Общие сведения об обновлении подключаемого модуля и устранении неполадок см. в [документации по продукту vRealize Orchestrator](#).

Необходимые условия

Чтобы использовать Все как услуга для расширения интеграции vRealize Automation и NSX for vSphere, установите подключаемый модуль NSX в vRealize Orchestrator. Этот подключаемый модуль не поддерживает NSX-T.

Если используется встроенный vRealize Orchestrator, который уже содержит установленный подключаемый модуль NSX, эту процедуру можно не проводить.

- Убедитесь, что запущен поддерживаемый экземпляр vRealize Orchestrator.

Дополнительные сведения о настройке vRealize Orchestrator см. в разделе *Установка и настройка VMware vRealize Orchestrator* в [документации по продукту vRealize Orchestrator](#).

- Убедитесь в наличии учетных данных учетной записи с разрешением на установку подключаемых модулей vRealize Orchestrator и проверку подлинности с помощью vCenter Single Sign-On.
- Убедитесь, что клиент vRealize Orchestrator установлен и можно выполнить вход с учетными данными администратора.
- Убедитесь в наличии правильной версии подключаемого модуля NSX в [матрице поддержки vRealize Automation](#).

Процедура

1. Загрузите файл подключаемого модуля в папку, доступную с сервера vRealize Orchestrator.

Формат имени файла установщика подключаемого модуля с соответствующими значениями версии — `o11nplugin-nsx-1.n.n.vmoapp`. Установочные файлы подключаемого модуля для NSX for vSphere доступны на [сайте загрузки продуктов VMware](#).

2. Откройте браузер и запустите интерфейс конфигурации vRealize Orchestrator.

Пример формата URL-адреса: `https://сервер_оркестратора.com:8283`.

3. На левой панели щелкните **Подключаемые модули** и прокрутите вниз до раздела «Установка нового подключаемого модуля».

4. В текстовом поле **Файл подключаемого модуля** перейдите к файлу установщика подключаемого модуля и щелкните **Передать и установить**.

Файл должен иметь формат VMOAPP.

5. При появлении запроса примите условия лицензионного соглашения на панели «Установка подключаемого модуля».

6. Проверьте, что в разделе «Состояние установки включенных подключаемых модулей» указано правильное имя подключаемого модуля NSX.

Сведения о версии см. в [таблице поддержки vRealize Automation](#).

Появится состояние Подключаемый модуль будет установлен при следующем запуске сервера.

7. Перезапустите службу сервера vRealize Orchestrator.
8. Перезапустите интерфейс конфигурации vRealize Orchestrator.
9. Щелкните **Подключаемые модули** и убедитесь, что состояние изменилось на **Установка выполнена успешно**.
10. Запустите клиентское приложение vRealize Orchestrator, войдите и используйте вкладку **Рабочий процесс** для навигации по библиотеке и перехода к папке NSX.

Можно просмотреть рабочие процессы, предоставляемые подключаемым модулем NSX.

Следующие шаги

Создайте конечную точку vRealize Orchestrator в vRealize Automation, чтобы использовать ее для выполнения рабочих процессов. См. раздел [Создание конечной точки vRealize Orchestrator](#).

Требования для администраторов при подготовке универсальных объектов NSX for vSphere

Для подготовки компьютеров в среде NSX с несколькими серверами vCenter при использовании универсальных объектов NSX необходимо выполнять подготовку на vCenter Server, где диспетчер вычислительных ресурсов NSX является основным.

В среде NSX for vSphere с несколькими серверами vCenter каждый сервер должен быть связан с собственным диспетчером NSX. Одному NSX назначается роль основного диспетчера NSX, а остальным — роль дополнительного диспетчера NSX.

Основной диспетчер NSX может создавать универсальные объекты, например универсальные логические коммутаторы. Эти объекты синхронизируются с дополнительными диспетчерами NSX. С помощью дополнительных диспетчеров NSX эти объекты можно просматривать, но нельзя редактировать. Для управления универсальными объектами необходимо использовать основной диспетчер NSX. Основной диспетчер NSX можно использовать для настройки любого из дополнительных диспетчеров NSX в данной среде.

Дополнительную информацию о среде NSX с несколькими серверами vCenter см. в разделе *Обзор сетевых подключений и средств безопасности в среде с несколькими серверами vCenter* в руководстве по администрированию NSX в [документации по продукту NSX for vSphere](#).

Для конечной точки vSphere (vCenter), связанной с конечной точкой NSX основного диспетчера NSX, vRealize Automation поддерживает локальные объекты NSX, такие как локальные логические коммутаторы, локальные шлюзы Edge, а также локальные подсистемы балансировки нагрузки, группы безопасности и теги безопасности. Также он поддерживает сети NAT «один к одному» и «один ко многим» с универсальной транспортной зоной, маршрутизируемые сети с универсальной транспортной зоной и универсальными логическими распределенными маршрутизаторами (DLR), а также подсистему балансировки нагрузки с сетью любого типа.

vRealize Automation не поддерживает имеющиеся и создаваемые по требованию универсальные группы безопасности и теги безопасности NSX.

Для подготовки локальных сетей по требованию в качестве основного диспетчера NSX используйте локальную транспортную зону, предназначенную специально для vCenter. Можно настроить резервирования vRealize Automation для использования локальной транспортной зоны и объектов Virtual Wire для развертываний на данном локальном экземпляре vCenter Server.

При подключении конечной точки vSphere (vCenter) к соответствующей конечной точке дополнительного диспетчера NSX можно подготавливать и использовать только локальные объекты.

vRealize Automation может использовать универсальный логический коммутатор NSX в качестве внешней сети. Если универсальный коммутатор существует, то система собирает данные о нем, а затем он подключается к каждому компьютеру в развертывании (или используется ими).

- Подготовка сети по требованию для универсальной транспортной зоны может привести к созданию нового универсального логического коммутатора.
- Подготовка сети по требованию для универсальной транспортной зоны в основном диспетчере NSX приводит к созданию универсального логического коммутатора.
- Подготовка сети по требованию для универсальной транспортной зоны в дополнительном диспетчере NSX завершается ошибкой, так как NSX не может создать универсальный логический коммутатор в дополнительном диспетчере NSX.

Дополнительные сведения об универсальных объектах NSX см. в статье базы знаний VMware *Ошибка развертывания схем элементов vRealize Automation с объектами NSX (2147240)* по адресу <http://kb.vmware.com/kb/2147240>.

Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами

IP-адреса и диапазоны для использования в определении профиля сети можно получить от поддерживаемого стороннего поставщика управления IP-адресами, например Infoblox.

Перед созданием и использованием конечной точки внешнего поставщика управления IP-адресами в профиле сети vRealize Automation необходимо загрузить или иным образом получить подключаемый модуль или пакет поставщика управления IP-адресами vRealize Orchestrator, импортировать его, запустить необходимые рабочие процессы в vRealize Orchestrator и зарегистрировать решение управления IP-адресами в качестве конечной точки vRealize Automation.

Для получения дополнительных сведений о подготавливаемом процессе для использования внешнего поставщика управления IP-адресами с целью указания диапазона возможных IP-адресов см. раздел [Подготовка развертывания vRealize Automation с использованием решений для управления IP-адресами стороннего поставщика](#).

Таблица 1-3. Подготовка контрольного списка для поддержки внешнего поставщика управления IP-адресами

Задача	Описание	Сведения
<input type="checkbox"/> Получение и импорт подключаемого модуля vRealize Orchestrator от поддерживаемого внешнего поставщика управления IP-адресами	<p>Загрузите с портала VMware Solution Exchange (https://solutionexchange.vmware.com/store/category_groups/cloud-management) подключаемый модуль или пакет поставщика управления IP-адресами, например подключаемый модуль управления IP-адресами Infoblox для vRealize Orchestrator, и импортируйте этот подключаемый модуль либо пакет в vRealize Orchestrator.</p> <p>Если на портале VMware Solution Exchange отсутствует необходимый вам пакет поставщика управления IP-адресами, вы можете создать свой собственный пакет с помощью комплекта SDK стороннего поставщика управления IP-адресами и сопроводительной документации.</p> <p>Комплекты SDK сторонних поставщиков управления IP-адресами для различных версий vRealize Automation, а также сопроводительную документацию и соответствующие начальные пакеты для vRealize Orchestrator и vRealize Automation можно загрузить по ссылкам: https://code.vmware.com/sdks и https://code.vmware.com/samples.</p>	См. раздел Получение и импорт пакета стороннего поставщика управления IP-адресами в vRealize Orchestrator .
<input type="checkbox"/> Запустите необходимые рабочие процессы конфигурации и зарегистрируйте внешнее решение управления IP-адресами в качестве конечной точки vRealize Automation.	Запустите рабочие процессы конфигурации vRealize Orchestrator и зарегистрируйте тип конечной точки поставщика управления IP-адресами в vRealize Orchestrator.	См. раздел Запустите рабочий процесс для регистрации типа сторонней конечной точки управления IP-адресами в vRealize Orchestrator .

Получение и импорт пакета стороннего поставщика управления IP-адресами в vRealize Orchestrator

Чтобы подготовить конечную точку стороннего поставщика управления IP-адресами к определению и использованию, необходимо сначала получить пакет стороннего поставщика управления IP-адресами и импортировать его в vRealize Orchestrator.

Можно загрузить и использовать подключаемый модуль существующего стороннего поставщика управления IP-адресами, например системы управления IP-адресами Infoblox. Кроме того, можно создать собственный подключаемый модуль или пакет стороннего поставщика для управления IP-адресами с помощью начального пакета, поставляемого VMware, и сопроводительной документации SDK для использования другого решения для управления IP-адресами, предоставленного сторонним поставщиком, например BlueCat.

- Загрузите имеющийся [подключаемый модуль управления IP-адресами Infoblox для vRealize Orchestrator](#) и сопроводительную документацию с сайта marketplace.vmware.com. Загружаемый файл также содержит документацию по установке и использованию подключаемого модуля.
- Для создания собственного стороннего решения для управления IP-адресами загрузите комплект SDK для управления IP-адресами, предоставленный сторонним поставщиком, сопроводительную документацию и соответствующий начальный пакет для vRealize Orchestrator и vRealize Automation. См. страницу [vRealize Automation Example Third-Party IPAM Package](#) («Пример интеграции стороннего решения для управления IP-адресами с vRealize Automation») по адресу code.vmware.com/web/sdk.

После импорта подключаемого модуля или пакета стороннего поставщика управления IP-адресами в vRealize Orchestrator необходимо запустить нужные рабочие процессы и зарегистрировать тип конечной точки управления IP-адресами в vRealize Orchestrator.

Дополнительные сведения об импорте подключаемых модулей и пакетов, а также запуске необходимых рабочих процессов vRealize Orchestrator см. в разделе *Использование клиента VMware vRealize Orchestrator*. Дополнительные сведения о расширении vRealize Automation за счет подключаемых модулей, пакетов и рабочих процессов vRealize Orchestrator см. в разделе *Увеличение жизненного цикла*.

В этой последовательности шагов в качестве примера используется подключаемый модуль управления IP-адресами Infoblox. Последовательность шагов зависит от версии vRealize Automation или подключаемого модуля.

Необходимые условия

- Загрузите пакет или подключаемый модуль с сайта marketplace.vmware.com.
- Войдите в vRealize Orchestrator с правами администратора для импорта, настройки и регистрации подключаемого модуля или пакета vRealize Orchestrator.

Процедура

1. Откройте сайт marketplace.vmware.com.
2. Найдите и загрузите подключаемый модуль или пакет.

Например, можно импортировать подключаемый модуль Infoblox, поддерживающий конечную точку стороннего поставщика управления IP-адресами Infoblox в vRealize Orchestrator и vRealize Automation 7.1 и более поздних версий.

- а) В категории **Издатель** выберите **Infoblox** и нажмите **Применить**.
- б) Выберите [Подключаемый модуль Infoblox для vRealize Orchestrator](#).

- в) Щелкните **Технические характеристики** и просмотрите предварительные требования.
- г) Нажмите **Попробовать**, чтобы получить дополнительные сведения и электронное письмо с ссылкой для скачивания.
- д) Скачайте ZIP-файл, следуя инструкциям в сообщении.

Версии подключаемого модуля 4.0 и выше поддерживают vRealize Automation 7.1 и выше.
Файл zip также содержит документацию по подключаемому модулю.

3. В vRealize Orchestrator перейдите на вкладку **Администратор** и щелкните **Импортировать пакет**.
4. Выберите пакет для импорта.
5. Выберите все рабочие процессы и артефакты и щелкните **Импортировать выделенные элементы**.

Следующие шаги

[Запустите рабочий процесс для регистрации типа сторонней конечной точки управления IP-адресами в vRealize Orchestrator.](#)

Запустите рабочий процесс для регистрации типа сторонней конечной точки управления IP-адресами в vRealize Orchestrator

Запустите рабочий процесс регистрации в vRealize Orchestrator, чтобы предоставить стороннему поставщику управления IP-адресами возможность использования vRealize Automation и зарегистрировать тип конечной точки управления IP-адресами для использования в vRealize Automation.

Необходимые условия

- [Получение и импорт пакета стороннего поставщика управления IP-адресами в vRealize Orchestrator](#)
- Убедитесь, что вы вошли в vRealize Orchestrator с правами на запуск рабочих процессов регистрации.
- При появлении соответствующего запроса рабочего процесса регистрации введите учетные данные администратора vRealize Automation. При регистрации типов конечной точки управления IP-адресами в vRealize Orchestrator появится запрос на ввод учетных данных администратора vRealize Automation.

Процедура

1. В vRealize Orchestrator перейдите на вкладку **Проектирование** и выберите **Администратор > Библиотека**, а затем — **Компонент SDK пакета службы управления IP-адресами**.

Каждый пакет поставщика управления IP-адресами имеет уникальное имя и содержит уникальные рабочие процессы. Каждый поставщик предоставляет собственный рабочий процесс регистрации. Имена рабочих процессов в пакетах поставщика должны быть одинаковыми, но расположение рабочих процессов в vRealize Orchestrator может быть разным и зависит от поставщика.

2. Например, запустите рабочий процесс регистрации **Register IPAM Endpoint** и укажите тип конечной точки управления IP-адресами **Infloblox**.

3. При запросе учетных данных vRealize Automation введите учетные данные администратора vRealize Automation, например учетные данные администратор структуры.

Необходимо указать рабочий процесс регистрации с помощью учетных данных системного администратора vRealize Automation. Даже если в клиент vRealize Orchestrator вошел пользователь, не являющийся системным администратором, но учетные данные системного администратора vRealize Automation предоставлены для рабочего процесса, регистрация будет выполнена успешно.

Результаты

В этом примере пакет регистрирует Infoblox как новый тип конечной точки управления IP-адресами в службе конечной точки vRealize Automation. После этого тип конечной точки станет доступным при создании или изменении конечных точек в vRealize Automation.

Примечание Если подключение для управления IP-адресами Infoblox исчезнет с вкладки vRealize Orchestrator **Иерархия** после перезапуска сервера vRealize Orchestrator в центре управления vRealize Orchestrator, решить эту проблему можно следующим образом. Запустите рабочий процесс **Create IPAM Connection**, последовательно выбрав пункты меню **Администратор vRO > Библиотека > Infoblox > vRA > Помощники**. Затем перейдите на вкладку **Иерархия** vRealize Orchestrator, выберите **Управление IP-адресами Infoblox** и обновите страницу, чтобы отобразить подключение для управления IP-адресами Infoblox.

Следующие шаги

Теперь можно создать конечную точку типа «управление IP-адресами Infoblox» либо конечную точку для любого стороннего пакета или только что зарегистрированного подключаемого модуля в vRealize Automation. См. раздел [Создание конечной точки стороннего поставщика управления IP-адресами](#).

Контрольный список для настройки Контейнеры для vRealize Automation

Чтобы начать работу с компонентом Containers, необходимо настроить поддержку ролей пользователей vRealize Automation.

После указания определений контейнера в компоненте Containers можно добавить и настроить компоненты контейнера в схеме элементов.

Таблица 1-4. Контрольный список для настройки Контейнеры для vRealize Automation

Задача	Сведения
Назначение ролей администратора контейнера и архитектора контейнера.	Сведения о ролях для компонента «Контейнеры» см. здесь: <i>Принципы и понятия</i> .
Указание определений контейнера на вкладке Контейнеры в vRealize Automation.	См. раздел <i>Настройка vRealize Automation</i> .
Добавление компонентов контейнера и сетевых компонентов контейнера к схемам элементов на вкладке Проект в vRealize Automation.	См. раздел <i>Настройка vRealize Automation</i> .

Настройка Containers с помощью устройства vRealize Automation

Сведения о службе Xenon доступны в устройстве vRealize Automation (Параметры **vRA** > **Xenon**).

Здесь содержится информация о ВМ узла, порте прослушивания и состоянии службы Xenon. Здесь также отображаются сведения о кластерных узлах службы Xenon.

Службой Xenon Linux можно управлять, используя следующие команды интерфейса командной строки в устройстве vRealize Automation.

Команда	Описание
service xenon-service status	Отображение состояния службы: запущена или остановлена.
service xenon-service start	Запуск службы.
service xenon-service stop	Остановка службы.
service xenon-service restart	Перезапуск службы.
service xenon-service get_host	Отображение имени узла, на котором запущена служба.
service xenon-service get_port	Отображение порта службы.
service xenon-service status_cluster	Отображение сведений о всех кластерных узлах в формате JSON.
service xenon-service reset	Удаление каталога, в котором в службе Xenon хранятся все файлы конфигурации, и перезапуск службы.

Кластеризация контейнеров

С помощью службы Xenon и Контейнеры для vRealize Automation можно присоединять узлы к кластеру. Если узлы включены в кластеры, то при запуске службы Xenon автоматически устанавливается связь с другими узлами.

Чтобы отслеживать состояние кластера, используйте вкладку **Xenon** в устройстве vRealize Automation или запустите следующую команду в интерфейсе командной строки:

```
service xenon-service status_cluster
```

Служба Xenon работает на основе кворумной модели кластеризации. Кворум рассчитывается по формуле $(\text{number of nodes} / 2) + 1$.

Подготовка среды vCloud Director к использованию vRealize Automation

Прежде чем интегрировать vCloud Director с vRealize Automation, необходимо установить и настроить экземпляр vCloud Director, настроить vSphere и облачные ресурсы, а также указать или создать соответствующие учетные данные, чтобы обеспечить для vRealize Automation доступ к среде vCloud Director.

Настройка среды

Настройте ресурсы vSphere и облачные ресурсы, в том числе виртуальные сети и центры обработки данных. Дополнительные сведения см. в документации по vCloud Director.

Требования к учетным данным для интеграции

Создайте или укажите учетные данные администратора организации или системного администратора, которые администраторы инфраструктуры как услуги vRealize Automation смогут использовать, чтобы обеспечить управление средой vCloud Director в качестве конечной точки с помощью vRealize Automation.

Рекомендации по использованию ролей пользователей

Обеспечивать соответствие ролей пользователей vCloud Director в организации и ролей бизнес-групп vRealize Automation не обязательно. Если в vCloud Director нет учетной записи пользователя, vCloud Director выполнит поиск в соответствующем протоколе LDAP или в Active Directory и создаст учетную запись при условии, что пользователь существует в хранилище удостоверений. Если создать учетную запись пользователя невозможно, то в журнал записывается предупреждение, но процесс подготовки не прерывается. Затем подготовленный компьютер назначается учетной записи пользователя, которая использовалась для настройки конечной точки vCloud Director.

Дополнительные сведения об управлении пользователями vCloud Director см. в документации по vCloud Director.

Подготовка среды vCloud Air к использованию vRealize Automation

Прежде чем интегрировать vCloud Air с vRealize Automation, необходимо зарегистрироваться, чтобы создать учетную запись vCloud Air, настроить среду vCloud Air, а также указать или создать соответствующие учетные данные, чтобы обеспечить для vRealize Automation доступ к этой среде.

Настройка среды

Настройте среду согласно инструкциям в документации vCloud Air.

Требования к учетным данным для интеграции

Создайте или укажите учетные данные администратора виртуальной инфраструктуры или учетной записи, которые администраторы инфраструктуры как услуги vRealize Automation смогут использовать, чтобы обеспечить управление средой vCloud Air в качестве конечной точки с помощью vRealize Automation.

Рекомендации по использованию ролей пользователей

Обеспечивать соответствие ролей пользователей vCloud Air в организации и ролей бизнес-групп vRealize Automation не обязательно. Дополнительные сведения об управлении пользователями vCloud Air см. в документации по vCloud Air.

Подготовка среды Amazon Web Services

Подготовка элементов и ролей пользователей в среде Amazon Web Services, подготовка для обмена данными гостевого агента Amazon Web Services и агент начальной загрузки Программное обеспечение и понимание принципа сопоставления функций Amazon Web Services функциям vRealize Automation.

Роли и учетные данные пользователей Amazon Web Services, необходимые для vRealize Automation

В Amazon AWS следует настроить учетные данные с разрешениями, которые необходимы vRealize Automation для управления средой.

Для vRealize Automation требуются ключи доступа для учетных данных конечных точек. Использование имени пользователя и пароля не поддерживается.

■ Авторизация ролей и разрешений в Amazon Web Services

Роль привилегированного пользователя в AWS обеспечивает пользователю или группе пользователей службы каталогов AWS полный доступ к службам и ресурсам AWS. Тем не менее ее наличие не является обязательным. Поддерживаются также роли пользователя с меньшим набором привилегий. Политика безопасности AWS, отвечающая требованиям для реализации возможностей vRealize Automation:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeImages",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeVolumes",

      "ec2:DescribeVpcAttribute",
      "ec2:DescribeAddresses",
      "ec2:DescribeAvailabilityZones",
      "ec2:DescribeImageAttribute",
      "ec2:DescribeInstanceAttribute",
      "ec2:DescribeVolumeStatus",
      "ec2:DescribeVpnConnections",
      "ec2:DescribeRegions",
      "ec2:DescribeTags",
      "ec2:DescribeVolumeAttribute",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeNetworkInterfaceAttribute",

      "ec2:DisassociateAddress",
      "ec2:GetPasswordData",

      "ec2:ImportKeyPair",
      "ec2:ImportVolume",

      "ec2:CreateVolume",
      "ec2>DeleteVolume",
      "ec2:AttachVolume",
      "ec2:ModifyVolumeAttribute",
      "ec2:DetachVolume",
```

```

        "ec2:AssignPrivateIpAddresses",
        "ec2:UnassignPrivateIpAddresses",

        "ec2:CreateKeyPair",
        "ec2:DeleteKeyPair",

        "ec2:CreateTags",
        "ec2:AssociateAddress",
        "ec2:ReportInstanceState",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:MonitorInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ec2:TerminateInstances",

        "elasticloadbalancing:RegisterInstancesWithLoadBalancer",
        "elasticloadbalancing:DeregisterInstancesFromLoadBalancer",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeInstanceHealth"
    ],
    "Resource": "*"
}
}]

```

■ Учетные данные для аутентификации в Amazon Web Services

Для управления пользователями и группами Amazon Identity and Access Management (IAM) необходимы учетные данные администратора AWS с полным доступом.

При создании конечной точки AWS в vRA вам потребуется ввести ключ и секретный ключ. Получить ключ доступа, необходимый для создания конечной точки Amazon, можно двумя способами. Во-первых, администратор может запросить ключ у пользователя с учетными данными администратора AWS с полным доступом. Во-вторых, можно дополнительно настроить права привилегированного пользователя с помощью политики для администратора AWS с полным доступом. См. раздел [Создание конечной точки Amazon](#).

Сведения о включении политик и ролей см. в разделе *AWS Identity and Access Management (IAM)* (Управление учетными данными и доступом в AWS) документации продукта Amazon Web Services.

Включение в Amazon Web Services возможности обмена данными с агентом начальной загрузки и гостевым агентом Программное обеспечение

Если планируется подготавливать схемы элементов приложения, содержащие Программное обеспечение, или если необходима возможность дальнейшей настройки подготовленных компьютеров с помощью гостевого агента, нужно настроить связь между средой Amazon Web Services, в которой подготавливаются компьютеры, и средой vRealize Automation, в которой агенты загружают пакеты и получают инструкции.

При подготовке компьютеров Amazon Web Services с гостевым агентом vRealize Automation и агентом начальной загрузки Программное обеспечение с помощью vRealize Automation нужно настроить связь между сетью и Amazon VPC. Это обеспечит обмен данными между подготовленными компьютерами и vRealize Automation для настройки компьютеров.

Для получения дополнительных сведений об установке связи с сетью VPC Amazon Web Services см. документацию Amazon Web Services.

Использование дополнительных компонентов Amazon

vRealize Automation поддерживает несколько компонентов Amazon, включая Amazon Virtual Private Cloud, эластичные подсистемы балансировки нагрузки, эластичные IP-адреса и Elastic Block Storage.

Использование групп безопасности Amazon

При создании резервирования Amazon укажите по крайней мере одну группу безопасности. Для каждой доступной области следует указать как минимум одну группу безопасности.

Группа безопасности выступает в качестве брандмауэра для контроля доступа к компьютеру. Каждая область включает в себя как минимум группу безопасности по умолчанию. Администраторы могут использовать Amazon Web Services Management Console, чтобы создавать дополнительные группы безопасности, настраивать порты для Microsoft Remote Desktop Protocol или SSH и виртуальные частные сети для Amazon VPN.

При создании резервирования Amazon или настройке компонента компьютера в схеме элементов можно выбрать одну из групп безопасности, которые доступны учетной записи в определенной области Amazon. Группы безопасности импортируются во время сбора данных.

Дополнительные сведения о создании и использовании групп безопасности в Amazon Web Services см. в документации Amazon.

Общие сведения об областях Amazon Web Service

Каждая учетная запись Amazon Web Services представлена облачной конечной точкой. При создании конечной точки Amazon Elastic Cloud Computing в vRealize Automation области собираются как вычислительные ресурсы. После того как администратор IaaS выберет вычислительные ресурсы для бизнес-группы, сбор данных иерархии и данных о состоянии будет выполняться автоматически.

В процессе сбора данных иерархии, который выполняется автоматически один раз в день, собираются данные обо всем происходящем с вычислительными ресурсами, например следующие сведения:

- Эластичные IP-адреса
- Эластичная подсистема балансировки нагрузки
- Тома хранилищ Elastic Block Storage

По умолчанию сбор данных о состоянии выполняется автоматически каждые 15 минут. При этом собирается информация о состоянии управляемых экземпляров (эти экземпляры создает vRealize Automation). Ниже приведены примеры данных о состоянии:

- Пароли для Windows

- Состояние компьютеров в подсистемах балансировки нагрузки
- Эластичные IP-адреса

Администратор структуры может инициировать сбор данных иерархии и данных о состоянии и деактивировать или изменить частоту выполнения этой процедуры.

Использование виртуального частного облака Amazon Virtual Private Cloud

С помощью Amazon Virtual Private Cloud можно подготовить экземпляры компьютера Amazon в частной части облака Amazon Web Services.

Пользователи Amazon Web Services могут использовать Amazon VPC, чтобы настроить топологию виртуальной сети в соответствии с требованиями. Можно назначить Amazon VPC в vRealize Automation. Тем не менее, vRealize Automation не отслеживает затраты на использование Amazon VPC.

При подготовке с помощью Amazon VPC vRealize Automation ожидает наличия подсети VPC, по которой Amazon получает основной IP-адрес. Этот адрес является статическим, пока экземпляр не будет удален. Кроме того, можно использовать пул эластичных IP-адресов, чтобы назначить эластичный IP-адрес экземпляру в vRealize Automation. Таким образом, если постоянно подготавливать и удалять экземпляр в Amazon Web Services, получится сохранить тот же IP-адрес.

С помощью AWS Management Console создайте следующие элементы:

- Amazon VPC, включающее в себя сетевые шлюзы, таблицу маршрутизации, группы безопасности, подсети и доступные IP-адреса;
- Amazon Virtual Private Network, если пользователям понадобится войти в компьютеры Amazon вне AWS Management Console.

При работе с Amazon VPC пользователи vRealize Automation могут выполнять следующие задачи:

- Администратор структуры может назначить Amazon VPC облачному резервированию. См. [Создание резервирования Amazon EC2](#).
- Владелец компьютера может назначить экземпляр компьютера Amazon Amazon VPC.

Дополнительные сведения о создании Amazon VPC см. в документации по Amazon Web Services.

Использование эластичной подсистемы балансировки нагрузки для Amazon Web Services

Эластичные подсистемы балансировки нагрузки распределяют входящий трафик приложений между экземплярами Amazon Web Services. Балансировка нагрузки компании Amazon обеспечивает повышенную отказоустойчивость и производительность.

Amazon предоставляет эластичную балансировку нагрузки для компьютеров, подготовленных с использованием схем элементов Amazon EC2.

Эластичная подсистема балансировки нагрузки должна быть доступна в Amazon Web Services, Amazon Virtual Private Network и в распоряжении для подготовки. Например, если подсистема балансировки нагрузки доступна в области us-east1c, а компьютер находится в области us-east1b, этот компьютер не сможет использовать имеющуюся подсистему балансировки нагрузки.

vRealize Automation не создает, не отслеживает эластичные подсистемы балансировки нагрузки и не управляет ими.

Чтобы получить информацию о создании эластичных подсистем балансировки нагрузки компании Amazon с помощью Amazon Web Services Management Console, см. документацию по Amazon Web Services.

Использование эластичного IP-адреса для Amazon Web Services

С помощью эластичного IP-адреса можно быстро переключиться на другой компьютер в динамичной облачной среде Amazon Web Services. В vRealize Automation эластичный IP-адрес доступен для всех бизнес-групп, у которых есть права на область.

Администратор может выделить эластичные IP-адреса учетной записи Amazon Web Services, используя AWS Management Console. В каждой области есть две группы эластичных IP-адресов. Один диапазон выделен для экземпляров, отличных от экземпляров Amazon VPC, и другой диапазон для экземпляров Amazon VPC. Если выделить адреса только в области, отличной от Amazon VPC, адреса не будут доступны в области Amazon VPC. Верно и обратное. Если выделить адреса только в области Amazon VPC, адреса будут не доступны в области, отличной от области Amazon VPC.

Эластичный IP-адрес связан с учетной записью Amazon Web Services, а не конкретным компьютером, однако одновременно его может использовать только один компьютер. Адрес связан с учетной записью Amazon Web Services, пока вы не решите освободить его. Его можно освободить, чтобы сопоставить с конкретным экземпляром компьютера.

Архитектор инфраструктуры как услуги может добавить в схему элементов настраиваемое свойство, чтобы назначить эластичные IP-адреса для компьютеров во время подготовки. Владельцы компьютеров и администраторы могут просматривать назначенные компьютерам эластичные IP-адреса, а те владельцы компьютеров и администраторы, у которых есть права изменения компьютеров, могут назначать эластичные IP-адреса после подготовки. Тем не менее, если адрес уже связан с экземпляром компьютера, а экземпляр содержится в развертывании Amazon Virtual Private Cloud, Amazon не назначает его.

Дополнительные сведения о создании и использовании эластичных IP-адресов Amazon см. в документации по Amazon Web Services.

Использование Elastic Block Storage для Amazon Web Services

Elastic Block Storage компании Amazon предоставляет тома хранилищ на уровне блоков, которые можно использовать с экземпляром компьютера Amazon и Amazon Virtual Private Cloud. Тома хранилищ могут сохраняться после выхода из строя связанного с ними экземпляра компьютера Amazon в облачной среде Amazon Web Services.

При использовании тома хранилища Elastic Block Storage компании Amazon с vRealize Automation применяются следующие ограничения:

- Вы не можете подключить существующий том хранилища Elastic Block Storage при подготовке экземпляра компьютера. Тем не менее, если при создании нового тома запросить несколько компьютеров одновременно, том будет создан и подключен к каждому экземпляру. Например, если при создании одного тома volume_1 запросить три компьютера, для каждого компьютера будет создано по тому. Будет создано три тома volume_1, которые будут подключены к каждому компьютеру. Каждому тому присвоен уникальный идентификатор тома. Все тома имеют одинаковый размер и расположены в одном и том же месте.
- Томом должна управлять та же операционная система, что и компьютером, к которому подключается том. Кроме того, том должен быть расположен там же, где и компьютер.
- vRealize Automation не управляет основным томом экземпляра Elastic Block Storage.

Дополнительные сведения о хранилище Elastic Block Storage компании Amazon и о том, как включить его с помощью Amazon Web Services Management Console, см. в документации по Amazon Web Services.

Настройка подключения между сетью и Amazon VPC для среды демонстрационной установки

Если ИТ-специалист настраивает среду для оценки vRealize Automation, для обеспечения поддержки функции vRealize Automation Программное обеспечение нужно настроить временное подключение сети к Amazon VPC.

Подключение сети к Amazon VPC потребуется только тогда, когда нужно использовать гостевой агент для настройки подготовленных компьютеров или когда нужно включить в схемы элементов компоненты Программное обеспечение. Для производственной среды следовало бы официально настроить ее с помощью Amazon Web Services. Однако при работе с испытательной средой вместо этого нужно создать временное подключение к сети Amazon VPC. Установите туннель SSH, а затем настройте резервирование Amazon в vRealize Automation для маршрутизации по туннелю.

Необходимые условия

- Создайте группу безопасности Amazon Web Services с именем TunnelGroup и настройте ее таким образом, чтобы разрешить доступ через порт 22.
- Создайте или определите компьютер CentOS в группе безопасности TunnelGroup Amazon Web Services и обратите внимание на следующие параметры:
 - административные учетные данные, например root;
 - Общедоступный IP-адрес.
 - Частный IP-адрес.
- Создайте или определите компьютер CentOS в той же локальной сети, в которой определено установленное устройство vRealize Automation.
- Установите сервер OpenSSH SSHD на обоих компьютерах в туннеле.

Процедура

1. Войдите в компьютер в туннеле Amazon Web Services в качестве пользователя root или пользователя с аналогичными правами.

2. Деактивируйте iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

3. Измените /etc/ssh/sshd_config, чтобы включить AllowTCPForwarding и GatewayPorts.

4. Перезапустите службу.

```
/etc/init.d/sshd restart
```

5. Войдите в компьютер CentOS от имени пользователя root в той же локальной сети, в которой установлено устройство vRealize Automation.
6. Вызовите туннель SSH на компьютере в локальной сети для компьютера Amazon Web Services в туннеле.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \

-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Amazon tunnel machine@Public IP Address of Amazon tunnel machine
```

Настроено перенаправление портов, чтобы предоставить компьютеру туннеля Amazon Web Services доступ к ресурсам vRealize Automation, но ваш туннель SSH не будет работать, пока не настроено резервирование Amazon для маршрутизации по туннелю.

Следующие шаги

1. Установите агент начальной загрузки программного обеспечения и гостевой агент на эталонном компьютере Windows или Linux, чтобы создать образ компьютера Amazon, с помощью которого архитекторы инфраструктуры как услуги смогут создавать схемы элементов. См. раздел [Подготовка к процессу подготовки Программное обеспечение](#).
2. Настройте резервирование Amazon в vRealize Automation для маршрутизации по туннелю SSH. См. раздел [Сценарий: создание резервирования Amazon для экспериментальной среды](#).

Подготовка возможностей сети и обеспечения безопасности Red Hat OpenStack

vRealize Automation поддерживает несколько компонентов в OpenStack, включая группы безопасности и плавающие IP-адреса. Этот раздел поможет понять принцип работы этих компонентов с vRealize Automation и настроить их в своей среде.

Использование групп безопасности OpenStack

В группах безопасности указаны правила, управляющие перемещением сетевого трафика через определенные порты.

При запросе компьютера можно указать группы безопасности. Помимо этого, на холсте проекта можно указать существующую группу безопасности или группу безопасности NSX по требованию.

Группы безопасности импортируются во время сбора данных.

Для каждой доступной области следует указать как минимум одну группу безопасности. При создании резервирования отображаются группы безопасности, доступные в этой области. Каждая область включает в себя как минимум группу безопасности по умолчанию.

Дополнительные группы безопасности следует настраивать в исходном ресурсе. Дополнительные сведения об управлении группами безопасности для различных компьютеров см. в документации по OpenStack.

Использование плавающих IP-адресов с OpenStack

Плавающие IP-адреса можно назначить работающему виртуальному экземпляру в OpenStack.

Для назначения плавающих IP-адресов нужно настроить переадресацию IP-адресов и создать пул плавающих IP-адресов в Red Hat OpenStack. Дополнительные сведения см. в документации по Red Hat OpenStack.

Необходимо назначить владельцам компьютеров право на доступ к действиям «Связать плавающий IP-адрес» и «Отменить связь плавающего IP-адреса». Уполномоченные пользователи могут связать плавающий IP-адрес с подготовленным компьютером во внешних сетях, привязанных к компьютеру, выбрав доступный IP-адрес в пуле плавающих IP-адресов. После привязки плавающего IP-адреса к компьютеру пользователь vRealize Automation может выбрать параметр «Отменить связь плавающего IP-адреса», чтобы просматривать текущие назначенные плавающие IP-адреса и отменять связь адреса с компьютером.

Подготовка среды SCVMM

Прежде чем начать создавать шаблоны и профили оборудования SCVMM, используемые при подготовке компьютера vRealize Automation, вы должны понять ограничения при именовании шаблонов и профилей оборудования и настроить параметры сети и хранилища SCVMM.

Дополнительные сведения о подготовке среды см. в информации о требованиях SCVMM в разделе *Установка vRealize Automation*.

Дополнительные сведения о подготовке компьютера см. в разделе [Создание конечной точки Hyper-V \(SCVMM\)](#).

vRealize Automation не поддерживает развертывание среды, использующей конфигурацию частного облака SCVMM. vRealize Automation в настоящее время не может осуществлять получение данных от частных облаков SCVMM, а также выделение ресурсов для них и подготовку ресурсов на их основе.

Именованние шаблонов и профилей оборудования

Согласно правилам именования, применяемым SCVMM и vRealize Automation к шаблонам и профилям оборудования, не начинайте имена шаблонов или профилей оборудования со слов «временный» или «профиль». Например, во время сбора данных игнорируются следующие слова:

- временный_шаблон;
- временный шаблон;
- временный_профиль;
- временный профиль;
- профиль.

Сетевая конфигурация для кластеров SCVMM

Кластеры SCVMM делают виртуальные сети доступными только для vRealize Automation. Поэтому отношение между виртуальными и логическими сетями должно быть 1:1. Сопоставьте каждую виртуальную сеть с логической сетью с помощью консоли SCVMM и настройте кластер SCVMM таким образом, чтобы он мог получать доступ к компьютерам по виртуальной сети.

Конфигурация хранилища для кластеров SCVMM

vRealize Automation собирает данные в кластерах Hyper-V SCVMM и выполняет подготовку только в общих томах. Используя консоль SCVMM, настройте кластеры таким образом, чтобы они использовали общие тома ресурсов для хранения.

Конфигурация хранилища для автономных узлов SCVMM

Для автономных узлов SCVMM vRealize Automation собирает данные и выполняет подготовку, используя путь к виртуальной машине по умолчанию. Используя консоль SCVMM, настройте пути к виртуальной машине по умолчанию для автономных узлов.

Настройка подключения VPC «сеть к Azure»

Чтобы иметь возможность использовать компоненты схемы элементов Azure, необходимо настроить подключение «сеть к Azure».

Необходимые условия

- Создайте группу безопасности Azure с именем TunnelGroup и настройте ее таким образом, чтобы разрешить доступ через порт 22.
- Создайте или определите компьютер, например компьютер CentOS, в группе безопасности Azure TunnelGroup и обратите внимание на следующие параметры:
 - административные учетные данные, например *root*;
 - Общедоступный IP-адрес.
 - Частный IP-адрес.

- Создайте или определите компьютер CentOS в той же локальной сети, в которой определено установленное устройство vRealize Automation.
- Установите сервер OpenSSH SSHD на обоих компьютерах в туннеле.

Процедура

1. Войдите в компьютер Azure в туннеле в качестве пользователя root или пользователя с аналогичными правами.
2. Деактивируйте iptables.

```
# service iptables save
# service iptables stop
# chkconfig iptables off
```

3. Измените /etc/ssh/sshd_config, чтобы включить AllowTCPForwarding и GatewayPorts.
4. Перезапустите службу.

```
/etc/init.d/sshd restart
```

5. Войдите в компьютер CentOS от имени пользователя root в той же локальной сети, в которой установлено устройство vRealize Automation.
6. Вызовите туннель SSH на компьютере в локальной сети для компьютера Azure в туннеле.

```
ssh -N -v -o "ServerAliveInterval 30" -o "ServerAliveCountMax 40" -o "TCPKeepAlive yes" \
-R 1442:vRealize_automation_appliance_fqdn:5480 \
-R 1443:vRealize_automation_appliance_fqdn:443 \
-R 1444:manager_service_fqdn:443 \
User of Azure tunnel machine@Public IP Address of Azure tunnel machine
```

Настроено перенаправление портов, чтобы предоставить компьютеру Azure в туннеле доступ к vRealize Automation ресурсам, но ваш туннель SSH не будет работать, пока не настроено резервирование Azure для маршрутизации по туннелю.

Следующие шаги

1. Установите агент начальной загрузки программного обеспечения и гостевой агент на эталонном компьютере Windows или Linux, чтобы создать образ компьютера Azure, с помощью которого архитекторы инфраструктуры как услуги смогут создавать схемы элементов. См. раздел [Подготовка к процессу подготовки Программное обеспечение](#).
2. Настройте резервирование Azure в vRealize Automation для маршрутизации по туннелю SSH. См. раздел [Создание резервирования для Microsoft Azure](#).

Подготовка к процессу подготовки компьютера

В зависимости от среды и метода подготовки компьютера может потребоваться настройка элементов за пределами vRealize Automation.

Например, может потребоваться настроить шаблоны или образы компьютера.

Кроме того, может потребоваться настройка параметров NSX или запуск рабочих процессов vRealize Orchestrator.

Дополнительные сведения о назначении портов на предварительном этапе подготовки компьютеров см. PDF-файл *Эталонная архитектура* в [документации по продукту vRealize Automation](#).

Выбор необходимого метода подготовки компьютера

Для большинства методов подготовки компьютеров необходимо подготовить некоторые элементы за пределами vRealize Automation.

Таблица 1-5. Выбор необходимого метода подготовки компьютера

Сценарий	Поддерживаемая конечная точка	Поддержка агента	Способ подготовки	Приготовление к предварительной подготовке
До или после подготовки компьютера настройте в решении vRealize Automation запуск настраиваемых сценариев Visual Basic в качестве дополнительных шагов в жизненном цикле компьютера. Например, можно использовать сценарий предварительной подготовки, чтобы создать сертификаты или маркеры безопасности перед подготовкой, а затем сценарий последующей подготовки, чтобы использовать сертификаты и маркеры после подготовки компьютера.	Можно запускать сценарии Visual Basic с использованием любой поддерживаемой конечной точки, кроме Amazon Web Services.	Зависит от используемого метода подготовки.	Сценарии Visual Basic поддерживаются в качестве дополнительных шагов при любых способах подготовки, однако нельзя использовать эти сценарии на компьютерах Amazon Web Services.	Контрольный список для запуска сценариев Visual Basic во время подготовки
Подготовка схем элементов приложения, которые обеспечивают автоматизацию установки, настройки и управление жизненным циклом промежуточного программного обеспечения и компонентов развертывания приложения, таких как Oracle, MySQL, WAR и схемы базы данных.	<ul style="list-style-type: none"> ■ vSphere ■ vCloud Air ■ vCloud Director ■ Amazon Web Services 	<ul style="list-style-type: none"> ■ Гостевой агент (обязательно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (обязательно) 	<ul style="list-style-type: none"> ■ Клонирование ■ Клонирование (для vCloud Air или vCloud Director) ■ Связанный клон ■ Образ компьютера Amazon 	Если необходимо использовать компоненты Программное обеспечение в схемах элементов, настройте метод подготовки с поддержкой гостевого агента и агента начальной загрузки Программное обеспечение. Для получения дополнительных сведений о подготовке для Программное обеспечение см. Подготовка к процессу подготовки Программное обеспечение .

Таблица 1-5. Выбор необходимого метода подготовки компьютера (продолжение)

Сценарий	Поддерживаемая конечная точка	Поддержка агента	Способ подготовки	Приготовления к предварительной подготовке
Дальнейшая настройка компьютеров после подготовки с использованием гостевого агента.	Все виртуальные конечные точки и Amazon Web Services.	<ul style="list-style-type: none"> ■ Гостевой агент (обязательно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (дополнительно) 	Поддерживается для всех методов подготовки, кроме использования образа виртуальной машины.	Если необходимо настроить компьютеры после подготовки, выберите метод подготовки с поддержкой гостевого агента.
Подготовка компьютера без гостевой операционной системы. Операционную систему можно установить по окончании процесса подготовки.	Все конечные точки виртуальных машин.	Не поддерживается	Обычная	Приготовления к предварительной подготовке за пределами vRealize Automation не требуются.
Подготовка копии виртуального компьютера с более эффективным использованием пространства, именуемой связанным клоном. Связанные клоны создаются на основе моментального снимка виртуальной машины и используют цепочку дельта-дисков для отслеживания отличий от родительской виртуальной машины	vSphere	<ul style="list-style-type: none"> ■ Гостевой агент (дополнительно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (дополнительно) 	Связанный клон	Необходимо наличие существующей виртуальной машины vSphere. Если требуется поддержка Программное обеспечение, нужно установить гостевой агент и агент начальной загрузки программного обеспечения на компьютере, который необходимо клонировать. Перед подготовкой виртуальных машин связанного клона выключите моментальный снимок виртуальной машины.
Подготовка копии виртуального компьютера с более эффективным использованием пространства с помощью технологии Net App FlexClone.	vSphere	Гостевой агент (дополнительно)	NetApp FlexClone	См. раздел Контрольный список для подготовки к процессу подготовки путем клонирования .

Таблица 1-5. Выбор необходимого метода подготовки компьютера (продолжение)

Сценарий	Поддерживаемая конечная точка	Поддержка агента	Способ подготовки	Приготовления к предварительной подготовке
Подготовка компьютеров путем клонирования из объекта шаблона, созданного на основе существующего компьютера Windows или Linux, который именуется эталонным компьютером, и объекта настройки	<ul style="list-style-type: none"> ■ vSphere ■ KVM (RHEV) ■ SCVMM 	<ul style="list-style-type: none"> ■ Гостевой агент (дополнительно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (дополнительно только для vSphere) 	Клонирование	<p>См. раздел Контрольный список для подготовки к процессу подготовки путем клонирования.</p> <p>Если требуется поддержка Программное обеспечение, нужно установить гостевой агент и агент начальной загрузки программного обеспечения на компьютере vSphere, который необходимо клонировать.</p>
Подготовка компьютеров vCloud Air или vCloud Director путем клонирования из шаблона и объекта настройки.	<ul style="list-style-type: none"> ■ vCloud Air ■ vCloud Director 	<ul style="list-style-type: none"> ■ Гостевой агент (дополнительно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (дополнительно) 	Клонирование vCloud Air или vCloud Director	<p>См. раздел Подготовка к резервированию vCloud Air и vCloud Director.</p> <p>Если требуется поддержка Программное обеспечение, создайте шаблон с гостевым агентом и агентом начальной загрузки программного обеспечения. Для vCloud Air настройте сетевое подключение между средами vRealize Automation и vCloud Air.</p>
Подготовка компьютера путем загрузки из образа ISO, используя файл конфигурации kickstart или autoYaSt и образ дистрибутива Linux для установки операционной системы на компьютер	<ul style="list-style-type: none"> ■ Все виртуальные конечные точки ■ Red Hat OpenStack 	Гостевой агент установлен в ходе выполнения подготовки.	Linux Kickstart	Подготовка к процессу подготовки Linux Kickstart
Подготовка компьютера и передача управления последовательности задач SCCM для загрузки из образа ISO, развертывания операционной системы Windows и установки гостевого агента vRealize Automation	Все конечные точки виртуальных машин.	Гостевой агент установлен в ходе выполнения подготовки.	SCCM	Подготовка к процессу подготовки SCCM

Таблица 1-5. Выбор необходимого метода подготовки компьютера (продолжение)

Сценарий	Поддерживаемая конечная точка	Поддержка агента	Способ подготовки	Приготовление к предварительной подготовке
Подготовка компьютера путем его загрузки в среду WinPE и установки операционной системы с помощью образа WIM существующего эталонного компьютера Windows	<ul style="list-style-type: none"> ■ Все виртуальные конечные точки ■ Red Hat OpenStack 	Необходимо указать гостевой агент. Создавая образ WinPE, нужно вручную добавить гостевой агент.	WIM	Подготовка к процессу подготовки WIM
Запуск экземпляра из образа виртуальной машины.	Red Hat OpenStack	Не поддерживается	Образ виртуальной машины	См. раздел Подготовка к процессу подготовки образов виртуальных машин .
Запуск экземпляра из образа компьютера Amazon	Amazon Web Services	<ul style="list-style-type: none"> ■ Гостевой агент (дополнительно) ■ Агент начальной загрузки программного обеспечения и гостевой агент (дополнительно) 	Образ компьютера Amazon	<p>Свяжите образы компьютера Amazon и типы экземпляров с учетной записью Amazon Web Services.</p> <p>Если требуется поддержка Программное обеспечение, создайте образ компьютера Amazon, содержащий гостевой агент и агент начальной загрузки программного обеспечения, и настройте связь по схеме «сеть-VPC» между средами Amazon Web Services и vRealize Automation.</p>

Контрольный список для запуска сценариев Visual Basic во время подготовки

До или после подготовки компьютера можно настроить в решении vRealize Automation запуск настраиваемых сценариев Visual Basic в качестве дополнительных шагов в жизненном цикле компьютера. Например, можно использовать сценарий предварительной подготовки, чтобы создать сертификаты или маркеры безопасности перед подготовкой, а затем сценарий последующей подготовки, чтобы использовать сертификаты и маркеры после подготовки компьютера. Сценарии Visual Basic можно запускать с любыми способами подготовки, однако эти сценарии нельзя использовать на компьютерах с Amazon AWS.

Таблица 1-6. Контрольный список для запуска сценариев Visual Basic во время подготовки

Задача	Расположение	Сведения
<input type="checkbox"/> Установка и настройка агентов EPI для сценариев Visual Basic.	Обычно узел службы диспетчера	См. раздел <i>Установка vRealize Automation</i> .
<input type="checkbox"/> Создание сценариев Visual Basic.	Компьютер, на котором установлен агент EPI	<p>Решение vRealize Automation содержит образец сценария Visual Basic <code>PrePostProvisioningExample.vbs</code> в подкаталоге Сценарии каталога установки агента EPI. Этот сценарий содержит верхний колонтитул для загрузки всех аргументов в словарь, текст, в который можно добавить функции, и нижний колонтитул, который позволяет возвращать обновленные настраиваемые свойства в vRealize Automation.</p> <p>При исполнении сценария Visual Basic агент EPI передает все настраиваемые свойства компьютера в сценарий в качестве аргументов. Чтобы вернуть обновленные значения свойств в решение vRealize Automation, разместите эти свойства в словаре и вызовите функцию, предоставленную решением vRealize Automation.</p>
<input type="checkbox"/> Сбор информации, нужной для того, чтобы включить сценарии в схемы элементов.	<p>Сбор данных и их перенос в разработчик архитектуры инфраструктуры</p> <p>Примечание Для предоставления необходимых сведений администратор структуры может создать группу свойств, используя наборы свойств <code>ExternalPreProvisioningVbScript</code> и <code>ExternalPostProvisioningVbScript</code>. Для разработчиков схем элементов это упрощает процесс добавления такой информации в схемы элементов.</p>	<ul style="list-style-type: none"> ■ Полный путь к сценарию Visual Basic, включая имя файла и расширение. Например, <code>%System Drive%\Program Files (x86)\VMware\vCAC_Agents\EPI_Agents\Scripts\SendEmail.vbs</code>. ■ Чтобы запустить сценарий перед подготовкой, настройте разработчики архитектуры так, чтобы они вводили полный путь к сценарию как значение настраиваемого свойства <code>ExternalPreProvisioningVbScript</code>. Чтобы запустить сценарий после подготовки, нужно использовать настраиваемое свойство <code>ExternalPostProvisioningVbScript</code>.

Подготовка с помощью гостевого агента vRealize Automation

Гостевой агент можно установить на эталонных компьютерах для дальнейшей настройки компьютера после развертывания. Вы можете использовать настраиваемые свойства зарезервированного гостевого агента для выполнения задач по общей настройке, таких как добавление и форматирование дисков, или

создать собственные настраиваемые сценарии для гостевого агента, которые будут выполняться в гостевой операционной системе подготавливаемого компьютера.

После завершения развертывания и настройки пользовательских параметров (если они были предоставлены) гостевой агент создает XML-файл (`c:\VRMGuestAgent\site\workitem.xml`), который содержит все настраиваемые свойства развернутого компьютера. Этот файл завершает все задачи, назначенные ему настраиваемыми свойствами гостевого агента, а затем удаляется с подготавливаемого компьютера.

Можно создать собственные сценарии для гостевого агента, которые будут выполняться на развернутых компьютерах, и использовать настраиваемые свойства на схеме элементов, чтобы указать расположение этих сценариев и порядок их выполнения. Кроме того, можно использовать настраиваемые свойства на схеме элементов компьютера, чтобы передать их значения в сценарии в качестве параметров.

Например, с помощью гостевого агента можно выполнить такие настройки в развернутых компьютерах:

- изменение IP-адреса;
- добавление или форматирование дисков;
- выполнение сценариев безопасности;
- подготовка другого агента, например Puppet или Chef.

Помимо этого, можно предоставить зашифрованную строку как настраиваемое свойство в аргументе командной строки. Это позволяет сохранить зашифрованную информацию, которую гостевой агент может расшифровать и определить как допустимый аргумент командной строки.

Примечание Гостевой агент Linux назначает статические IP-адреса во время создания и клонирования при подготовке Linux Kickstart и PXE относительно настраиваемых свойств vRealize Automation в рабочих элементах. Гостевой агент не может размещать более новые согласованные схемы именования сетей (например, Ubuntu 16.x) при назначении статических IP-адресов.

Настраиваемые сценарии не нужно устанавливать на компьютере. Пока подготавливаемый компьютер имеет доступ к расположению сценариев по сети, гостевой агент может получить доступ к сценариям и выполнять их. Таким образом снижаются затраты на техническое обслуживание благодаря возможности обновить сценарии без необходимости восстановления всех шаблонов.

Для настройки параметров безопасности можно указать сведения в резервировании, схеме элементов или сценарии гостевого агента. Если для компьютеров требуется гостевой агент, добавьте правило безопасности в резервирование или в схему элементов.

При установке гостевого агента для выполнения настраиваемых сценариев на подготавливаемых компьютерах схемы элементов должны включать соответствующие настраиваемые свойства гостевого агента. Например, если вы установите гостевой агент в шаблон для клонирования, создадите настраиваемый сценарий, который изменяет IP-адрес подготавливаемого компьютера, и поместите его в общую папку, на схему элементов потребуется добавить ряд настраиваемых свойств.

Таблица 1-7. Настраиваемые свойства для изменения IP-адреса подготавливаемого компьютера с помощью гостевого агента

Настраиваемое свойство	Описание
VirtualMachine.Admin.UseGuestAgent	Задайте значение true , чтобы подготовить гостевой агент при запуске подготавливаемого компьютера.
VirtualMachine.Customize.WaitComplete	Если задано значение «Истина», то рабочий процесс подготовки не будет отправлять рабочие элементы гостевому агенту до полного завершения настройки. Задайте значение «Ложь», чтобы разрешить создание рабочих элементов до завершения настройки.

Таблица 1-7. Настраиваемые свойства для изменения IP-адреса подготавливаемого компьютера с помощью гостевого агента (продолжение)

Настраиваемое свойство	Описание
VirtualMachine.SoftwareN.ScriptPath	<p>Указывает полный путь к сценарию установки приложения. Путь должен быть допустимым абсолютным путем в том виде, в котором он отображается для гостевой операционной системы, и должен включать в себя имя файла сценария.</p> <p>Можно передать значения настраиваемых свойств в качестве параметров сценария, вставив <code>{CustomPropertyName}</code> в строке пути. Например, если имя настраиваемого свойства — <code>ActivationKey</code>, а его значение — <code>1234</code>, путь к сценарию будет таким: <code>D:\InstallApp.bat -key {ActivationKey}</code>. Гостевой агент запускает команду <code>D:\InstallApp.bat -key 1234</code>. Файл сценария можно затем запрограммировать на принятие и использование этого значения.</p> <p>Укажите значение для переменной <code>{Owner}</code> (владелец), чтобы передать имя владельца компьютера в сценарий.</p> <p>Можно также передать значения настраиваемых свойств в качестве параметров сценария, вставив <code>{YourCustomProperty}</code> в строке пути. Например, при вводе значения</p> <p>\\vra-scripts.mycompany.com\scripts\changeIP.bat</p> <p>выполняется сценарий <code>changeIP.bat</code> из общей папки, а при вводе значения</p> <p>\\vra-scripts.mycompany.com\scripts\changeIP.bat {VirtualMachine.Network0.Address}</p> <p>выполняется сценарий <code>changeIP</code>, а также в сценарий передается значение свойства <code>VirtualMachine.Network0.Address</code> в качестве параметра.</p>
VirtualMachine.ScriptPath.Decrypt	<p>Позволяет vRealize Automation получить зашифрованную строку, которая передается как надлежащим образом отформатированное указание настраиваемого свойства <code>VirtualMachine.SoftwareN.ScriptPath</code> в командную строку агента.</p> <p>Зашифрованную строку, например пароль, можно представить в виде настраиваемого свойства в аргументе командной строки. Это позволяет хранить зашифрованную информацию, которую гостевой агент может расшифровать и интерпретировать как допустимый аргумент командной строки. Например, строка настраиваемого свойства</p> <p><code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat password</code> не является защищенной, поскольку содержит фактический пароль.</p>

Таблица 1-7. Настраиваемые свойства для изменения IP-адреса подготавливаемого компьютера с помощью гостевого агента (продолжение)

Настраиваемое свойство	Описание
	<p>Чтобы зашифровать пароль, можно создать настраиваемое свойство vRealize Automation, например <code>MyPassword = password</code>, и включить шифрование, установив соответствующий флажок. Гостевой агент расшифровывает запись [MyPassword] в значение в настраиваемом свойстве <code>MyPassword</code> и запускает сценарий как <code>c:\dosomething.bat password</code>.</p> <ul style="list-style-type: none"> ■ Создайте настраиваемое свойство MyPassword = <i>пароль</i>, где <i>пароль</i> — это значение фактического пароля. Включите шифрование, установив соответствующий флажок. ■ Для настраиваемого свойства <code>VirtualMachine.ScriptPath.Decrypt</code> задайте значение <code>VirtualMachine.ScriptPath.Decrypt = true</code>. ■ Для настраиваемого свойства <code>VirtualMachine.Software0.ScriptPath</code> задайте значение <code>VirtualMachine.Software0.ScriptPath = c:\dosomething.bat [MyPassword]</code>. <p>Если для <code>VirtualMachine.ScriptPath.Decrypt</code> задать значение «Ложь» или не создать настраиваемое свойство <code>VirtualMachine.ScriptPath.Decrypt</code>, то строка в квадратных скобках ([and]) не будет расшифрована.</p>

Дополнительные сведения о настраиваемых свойствах, которые можно использовать с гостевым агентом, см. в разделе *Справочник по настраиваемым свойствам*.

Настройка в гостевом агенте доверия к серверу

Установка PEM-файла открытого ключа для узла службы диспетчера vRealize Automation в правильной папке гостевого агента — самый безопасный подход при настройке в гостевом агенте доверия к серверу.

Найдите папку гостевого агента, который должен доверять серверу, в каждом шаблоне для PEM-файла `cert.pem` на узле службы диспетчера.

- Папка гостевого агента Windows в каждом шаблоне, в котором используется агент

```
C:\VRMGuestAgent\cert.pem
```

- Папка гостевого агента Linux в каждом шаблоне, в котором используется агент

```
/usr/share/gugent/cert.pem
```

Если не поместить файл `cert.pem` в это расположение, на эталонном компьютере шаблона будет невозможно использовать гостевой агент. Например, если попытаться собрать сведения об открытом ключе после запуска ВМ путем изменения сценариев, нарушится условие безопасности.

В зависимости от настроенной среды следует обратить внимание на дополнительные факторы.

- В установках WIM содержимое PEM-файла открытого ключа необходимо добавить в исполняемый файл консоли и интерфейс пользователя. Флаг консоли — **/cert filename**.
- В установках RedHat Kickstart открытый ключ необходимо вырезать и вставить в файл образца, иначе гостевой агент не сможет выполнить операцию.
- В установке SCCM файл `cert.pem` должен находиться в папке `VRMGuestAgent`.
- В установках Linux vSphere файл `cert.pem` должен находиться в папке `/usr/share/gugent`.

Примечание При необходимости программное обеспечение и гостевые агенты можно установить вместе, загрузив следующий сценарий с веб-страницы <https://APPLIANCE/software/index.html>. Этот сценарий позволяет обрабатывать прием отпечатков пальцев по сертификату SSL при создании шаблонов.

- Linux
`prepare_vra_template.sh`
- Windows
`prepare_vra_template.ps1`

Если программное обеспечение и гостевой агент устанавливаются вместе, инструкции в разделе [Установка гостевого агента на эталонном компьютере Linux](#) или [Установка гостевого агента на эталонном компьютере Windows](#) не нужно использовать.

Получение файла `cert.pem` из узла службы диспетчера

1. На узле службы диспетчера перейдите в раздел «Администрирование» и откройте диспетчер IIS.
2. В дереве слева выделите узел службы диспетчера.
3. В правой части откройте «Сертификаты сервера».
4. Найдите сертификат, у которого в поле **Кому выдан** указано VMware vRA, а **Кем выдан** — VMware vRA.
5. Щелкните правой кнопкой мыши сертификат и экспортируйте его.
6. Сохраненный сертификат будет иметь формат PFX. Чтобы преобразовать его в формат PEM, используйте OpenSSL из командной строки.

```
openssl pkcs12 -in filename.pfx -out cert.pem -nodes
```

Установка гостевого агента на эталонном компьютере Linux

Установите гостевой агент Linux на своих эталонных компьютерах, чтобы выполнить дополнительную настройку после развертывания.

Необходимые условия

- Определите или создайте эталонный компьютер.

- Загружаемые файлы гостевого агента содержат пакеты в формате `tar.gz` и RPM. Если операционной системе не удалось установить файлы формата `tar.gz` или RPM, преобразуйте установочные файлы в нужный формат пакета с помощью средства преобразования.
- Установите безопасное доверие между гостевым агентом и своим компьютером со службой диспетчера. См. раздел [Настройка в гостевом агенте доверия к серверу](#).

Процедура

1. Перейдите на страницу консоли управления устройства vRealize Automation.
Например, `https://va-hostname.domain.com`.
2. Выберите **страницу гостевого агента и агента программного обеспечения** в разделе страницы установки компонентов vRealize Automation.
Например, `https://va-hostname.domain.com/software/index.html`.
Откроется страница **Средства установки гостевого агента и агента программного обеспечения** со ссылками, доступными для загрузки.
3. Выберите **Пакеты гостевых агентов Linux** в разделе страницы средств установки гостевых агентов, чтобы загрузить и сохранить файл `LinuxGuestAgentPkgs.zip`.
4. Распакуйте загруженный файл `LinuxGuestAgentPkgs.zip`, чтобы создать папку `VraLinuxGuestAgent`.
5. Установите пакет гостевого агента, который соответствует гостевой операционной системе, развертываемой во время подготовки.
 - а) Перейдите в подкаталог `VraLinuxGuestAgent`, соответствующий гостевой операционной системе, для развертывания во время подготовки, например `rhel32`.
 - б) Найдите пакет нужного формата или преобразуйте его в предпочтительный формат.
 - в) Установите пакет гостевого агента на эталонный компьютер.
Например, чтобы установить файлы из пакета формата RPM, выполните команду `rpm -i gugent-gugent-7.1.0-4201531.i386.rpm`.

6. Настройте гостевой агент для обмена данными со службой диспетчера, выполнив команду `installgugent.sh Manager_Service_Hostname_fdqn:portnumber ssl platform`.

Номер порта по умолчанию для службы диспетчера — 443. Допустимые значения платформы — `ec2`, `vcd`, `vca`, а также `vsphere`.

Параметр	Описание
Если используется подсистема балансировки нагрузки	<p>Введите полное доменное имя и номер порта своей подсистемы балансировки нагрузки службы диспетчера. Пример:</p> <pre>cd /usr/share/gugent ./installgugent.sh load_balancer_manager_service.mycompany.com:443 ssl ec2</pre>
Без подсистемы балансировки нагрузки	<p>Введите полное доменное имя и номер порта компьютера со службой диспетчера. Пример:</p> <pre>cd /usr/share/gugent ./installgugent.sh manager_service_machine.mycompany.com:443 ssl vsphere</pre>

7. Если развернутые компьютеры не настроены для доверия сертификату SSL службы диспетчера, для установки доверия на эталонном компьютере необходимо установить файл `cert.pem`.

- Безопаснее всего получить сертификат `cert.pem` и установить файл на эталонном компьютере вручную.
- Для удобства можно подключиться к подсистеме балансировки нагрузки или компьютеру службы диспетчера и загрузить сертификат `cert.pem`.

Параметр	Описание
Если используется подсистема балансировки нагрузки	<p>Выполните следующую команду на эталонном компьютере в качестве привилегированного пользователя:</p> <pre>echo openssl s_client -connect подсистема_балансировки_нагрузки_службы_диспетчера.моя_компания.ком: 443 sed -ne '/--BEGIN CERTIFICATE--/,/--END CERTIFICATE--p' > cert.pem</pre>
Без подсистемы балансировки нагрузки	<p>Выполните следующую команду на эталонном компьютере в качестве привилегированного пользователя:</p> <pre>echo openssl s_client -connect компьютер_службы_диспетчера.моя_компания.ком:443 sed -ne '/-- BEGIN CERTIFICATE--/,/--END CERTIFICATE--p' > cert.pem</pre>

8. Если гостевой агент устанавливается в операционной системе Ubuntu, создайте символичные ссылки на общие объекты, выполнив один из следующих наборов команд.

Параметр	Описание
64-разрядные системы	<pre>cd /lib/x86_64-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>
32-разрядные системы	<pre>cd /lib/i386-linux-gnu sudo ln -s libssl.so.1.0.0 libssl.so.10 sudo ln -s libcrypto.so.1.0.0 libcrypto.so.10</pre>

Следующие шаги

Преобразование эталонного компьютера в шаблон для клонирования, образ компьютера Amazon или моментальный снимок, который архитекторы инфраструктуры смогут использовать при создании схем элементов.

Установка гостевого агента на эталонном компьютере Windows

Установите на эталонном компьютере с Windows гостевой агент Windows vRealize Automation, который будет запускаться как служба Windows, и сделайте возможной дополнительную настройку компьютеров.

Необходимые условия

- Определите или создайте эталонный компьютер.
- Установите безопасное доверие между гостевым агентом и своим компьютером со службой диспетчера. См. раздел [Настройка в гостевом агенте доверия к серверу](#).

Процедура

1. Перейдите на страницу vRealize Automation **Средства установки гостевого и программного агента**:
<https://vrealize-automation-appliance-FQDN/software>
2. В разделе **Средства установки гостевого агента** загрузите исполняемый файл 32- или 64-разрядной версии и сохраните его в корневой каталог диска C:.

Примечание Для установки гостевого агента можно также использовать командную строку. Вместо загрузки исполняемых файлов можно перейти в раздел **Средства установки ПО Windows** на странице «Средства установки гостевых и программных агентов». Оттуда необходимо загрузить сценарий PowerShell `prepare_vra_template.ps1` и выполнить его.

```
PowerShell -NoProfile -ExecutionPolicy Bypass -Command prepare_vra_template.ps1
```

3. Запустите исполняемый файл, чтобы извлечь файлы гостевого агента Windows.

При извлечении создается каталог `C:\VRMGuestAgent` и добавляются файлы.

Не переименовывайте каталог C:\VRMGuestAgent.

4. Настройте гостевой агент для обмена данными со службой диспетчера.

- а) Откройте окно командной строки с повышенными привилегиями.
- б) Перейдите в папку C:\VRMGuestAgent.
- в) Поместите файл PEM доверенной службы диспетчера в каталог C:\VRMGuestAgent\, чтобы настроить в гостевом агенте доверие к компьютеру со службой диспетчера.
- г) Выполните команду `win service -i -h Manager_Service_Hostname_fqdn:portnumber -p ssl`.

Номер порта по умолчанию для службы диспетчера — 443.

Параметр	Описание
Если используется подсистема балансировки нагрузки	Введите полное доменное имя и номер порта своей подсистемы балансировки нагрузки службы диспетчера. Например, <code>win service -i -h load_balancer_manager_service.mycompany.com:443 -p ssl</code> .
Без подсистемы балансировки нагрузки	Введите полное доменное имя и номер порта компьютера со службой диспетчера. Например, <code>win service -i -h manager_service_machine.mycompany.com:443 -p ssl</code> .
При подготовке образа компьютера Amazon	Нужно указать, что используется Amazon. Например, <code>win service -i -h manager_service_machine.mycompany.com:443:443 -p ssl -c ec2</code> .

Результаты

Имя службы Windows — VCACGuestAgentService. Файл журнала установки VCACGuestAgentService.log можно найти в каталоге C:\VRMGuestAgent.

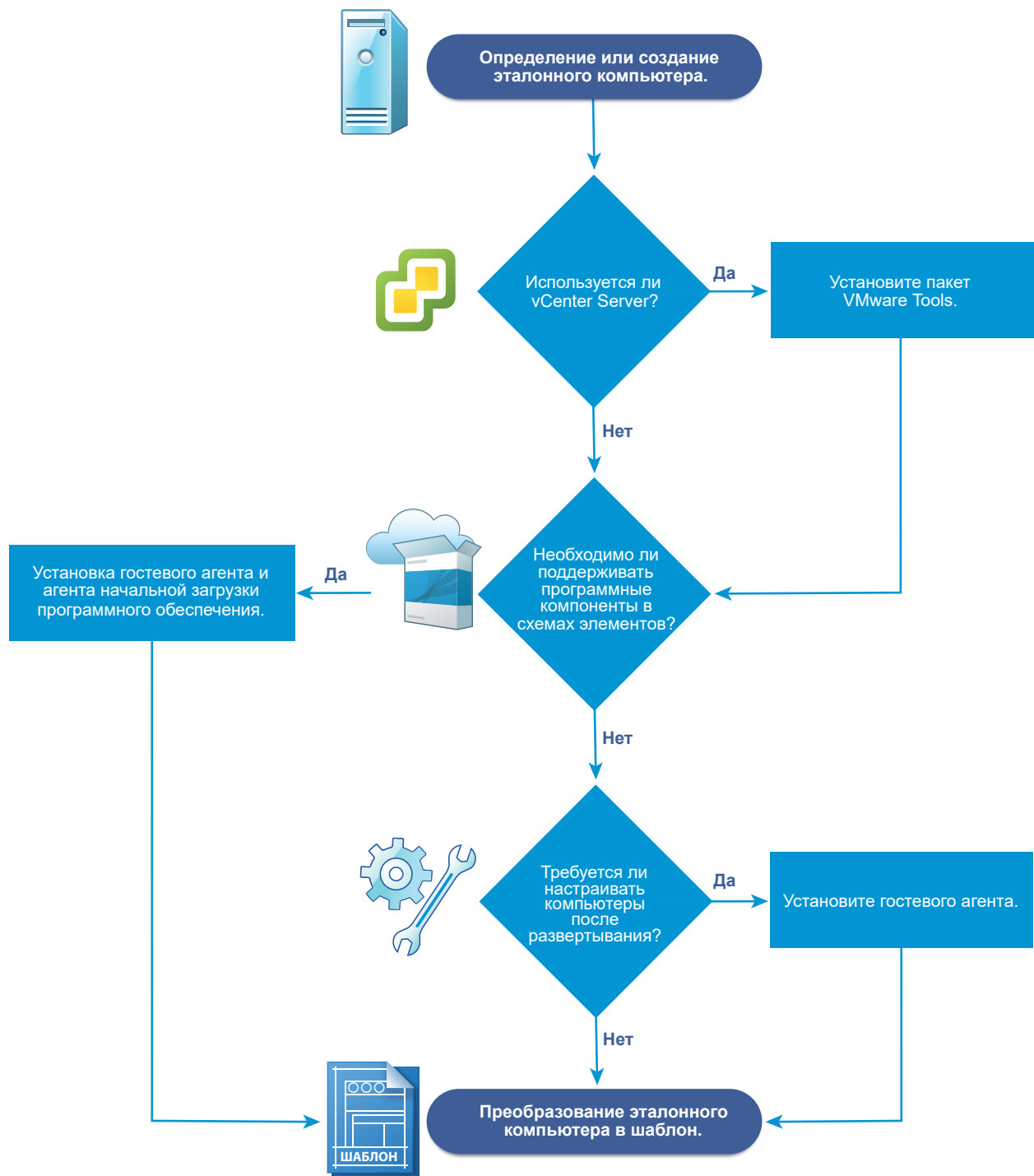
Следующие шаги

Преобразуйте эталонный компьютер в шаблон для клонирования, образ компьютера Amazon или моментальный снимок, чтобы архитекторы инфраструктуры могли использовать ваш шаблон при создании схем элементов.

Контрольный список для подготовки к процессу подготовки путем клонирования

Для того чтобы создать шаблон и объекты настройки, используемые для клонирования виртуальных машин Linux и Windows, необходимо выполнить некоторые подготовительные операции за рамками vRealize Automation.

Для клонирования требуется шаблон, созданный на основе эталонного компьютера.



При подготовке компьютера Windows путем клонирования единственным способом присоединения подготовленного компьютера к домену Active Directory является использование спецификации настройки из vCenter Server или включение профиля гостевой операционной системы в шаблон SCVMM. Компьютеры, подготовленные путем клонирования, не могут быть размещены в контейнере Active Directory во время подготовки. Необходимо сделать это вручную после инициализации.

Таблица 1-8. Контрольный список для подготовки к процессу подготовки путем клонирования

Задача	Расположение	Сведения
<input type="checkbox"/> Определите или создайте эталонный компьютер.	Гипервизор	Дополнительные сведения см. в документации, предоставленной гипервизором.
<input type="checkbox"/> (Необязательно) Если нужно, чтобы шаблон клонирования поддерживал компоненты Программное обеспечение, установите на эталонном компьютере гостевого агента vRealize Automation и агента начальной загрузки программного обеспечения.	Эталонный компьютер	Сведения об эталонных компьютерах Windows см. в Подготовка эталонного компьютера Windows для поддержки Программное обеспечение . Сведения об эталонных компьютерах Linux см. в Подготовка эталонного компьютера Linux для поддержки Программное обеспечение .
<input type="checkbox"/> (Необязательно) Если не нужно, чтобы шаблон клонирования поддерживал компоненты Программное обеспечение, но требуется возможность настройки развернутых компьютеров, установите на эталонном компьютере гостевого агента vRealize Automation.	Эталонный компьютер	См. раздел Подготовка с помощью гостевого агента vRealize Automation .
<input type="checkbox"/> При работе в среде vCenter Server установите VMware Tools на эталонном компьютере.	vCenter Server	См. документацию по VMware Tools.
<input type="checkbox"/> Создайте шаблон для клонирования, используя эталонный компьютер.	Гипервизор	Эталонный компьютер может быть включен или выключен. При клонировании в vCenter Server можно использовать эталонный компьютер напрямую, не создавая шаблон. Дополнительные сведения см. в документации, предоставленной гипервизором.
<input type="checkbox"/> Создайте объект настройки, чтобы настроить клонированные компьютеры с применением информации System Preparation Utility или настройки Linux.	Гипервизор	При клонировании Linux можно установить гостевой агент Linux и предоставить внешние сценарии настройки вместо создания объекта настройки. При клонировании с помощью vCenter Server необходимо предоставить спецификацию настройки в качестве объекта настройки. Дополнительные сведения см. в документации, предоставленной гипервизором.
<input type="checkbox"/> Соберите информацию, необходимую для создания схем элементов, выполняющих клонирование шаблона.	Сбор данных и их передача разработчикам архитектуры инфраструктуры как услуги	См. раздел Ведомость для виртуальной подготовки путем клонирования .

Ведомость для виртуальной подготовки путем клонирования

Заполните приведенные здесь ведомости сведениями о шаблоне, настройках и настраиваемых свойствах, необходимых для создания схем элементов клонов для шаблонов, подготовленных в среде. Не все эти сведения требуются для каждой реализации. Используйте эти ведомости в качестве примера или скопируйте и вставьте приведенные здесь таблицы в инструмент обработки текста, чтобы внести необходимые изменения.

Требуемые сведения о шаблоне и резервировании

Таблица 1-9. Ведомость по шаблону и резервированию

Требуемые сведения	Мое значение	Сведения
Имя шаблона		
Резервирования, в которых доступен шаблон, или применяемая политика резервирования		Во избежание ошибок при подготовке убедитесь, что шаблон доступен во всех резервированиях, или создайте политики резервирования, которые разработчики могут использовать, чтобы добавлять в схему элементов только резервирования, в которых доступен шаблон.
Тип клонирования, запрашиваемый для этого шаблона (только vSphere)		<ul style="list-style-type: none"> ■ Клонирование ■ Связанный клон ■ NetApp FlexClone
Имя спецификации настройки (требуется для клонирования при использовании статических IP-адресов)		Компьютеры Windows нельзя настраивать без спецификации настройки vSphere. См. раздел Присоединение компьютера Linux к домену Windows Active Directory .
Имя ISO (только SCVMM)		
Виртуальный жесткий диск (только SCVMM)		
Профиль оборудования, который необходимо подключить к подготовленным компьютерам (только SCVMM)		

Группы требуемых свойств

Можно заполнить разделы сведений о настраиваемых свойствах в ведомости или создать группы свойств и попросить разработчиков архитектуры добавить их в схемы элементов вместо большого количества отдельных настраиваемых свойств.

Требуемая операционная система vCenter Server

Для подготовки vCenter Server необходимо указать настраиваемое свойство гостевой операционной системы.

Таблица 1-10. Операционная система vCenter Server

Настраиваемое свойство	Мое значение	Описание
VMware.VirtualCenter.OperatingSystem		Указывает версию гостевой операционной системы vCenter Server (VirtualMachineGuestOsIdentifier), с помощью которой решение vCenter Server создает компьютер. Версия операционной системы должна соответствовать версии операционной системы, которую нужно установить на подготовленном компьютере. Администраторы могут создавать группы свойств с помощью нескольких наборов свойств (например, VMware[OS_Version]Properties), в которых предварительно настроено наличие верных значений VMware.VirtualCenter.OperatingSystem. Это свойство предназначено для виртуальной подготовки.

Сведения о сценариях Visual Basic

При настройке vRealize Automation для выполнения настраиваемых сценариев Visual Basic в качестве дополнительных шагов в жизненном цикле компьютера требуется добавить в схему элементов сведения о сценариях.

Примечание Для предоставления необходимых сведений администратор структуры может создать группу свойств, используя наборы свойств ExternalPreProvisioningVbScript и ExternalPostProvisioningVbScript. Для разработчиков схем элементов это упрощает процесс добавления такой информации в схемы элементов.

Таблица 1-11. Сведения о сценариях Visual Basic

Настраиваемое свойство	Мое значение	Описание
ExternalPreProvisioningVbScript		Запустите сценарий перед подготовкой. Введите полный путь к сценарию, включая имя файла и расширение. %System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs.
ExternalPostProvisioningVbScript		Запустите сценарий после подготовки. Введите полный путь к сценарию, включая имя файла и расширение. %System Drive%Program Files (x86)\VMware\VCAC Agents\EPI_Agents\Scripts\SendEmail.vbs

Сведения о сценарии настройки гостевого агента Linux

Если шаблон Linux настроен для выполнения сценариев настройки с использованием гостевого агента, требуется добавить в схему элементов сведения о сценариях.

Таблица 1-12. Ведомость по сценарию настройки гостевого агента Linux

Настраиваемое свойство	Мое значение	Описание
Linux.ExternalScript.Name		Указывает имя необязательного сценария, например config.sh, запускаемого гостевым агентом Linux после установки операционной системы. Это свойство доступно для компьютеров Linux, клонированных из шаблонов, на базе которых установлен агент Linux. Если указать внешний сценарий, нужно также определить его расположение с помощью свойств Linux.ExternalScript.LocationType и Linux.ExternalScript.Path.
Linux.ExternalScript.LocationType		Указывает тип расположения сценария настройки, обозначенного в свойстве Linux.ExternalScript.Name. Это может быть локальное расположение или файловая система NFS. Кроме того, нужно указать расположение сценария с помощью свойства Linux.ExternalScript.Path. Если тип расположения — NFS, используйте также свойство Linux.ExternalScript.Server.
Linux.ExternalScript.Server		Указывает имя NFS-сервера, например lab-ad.lab.local, на котором находится внешний сценарий настройки Linux, обозначенный в имени Linux.ExternalScript.Name.
Linux.ExternalScript.Path		Указывает локальный путь к сценарию настройки Linux или к пути экспорта к настройке Linux на NFS-сервере. Значение должно начинаться с косой черты и не должно включать в себя имя файла (например, /scripts/linux/config.sh).

Другие настраиваемые свойства гостевого агента

Если на эталонном компьютере установлен гостевой агент, можно использовать настраиваемые свойства для дальнейшей настройки компьютеров после развертывания.

Таблица 1-13. Настраиваемые свойства для настройки клонированных компьютеров с помощью ведомости по гостевому агенту

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.Admin.AddOwnerToAdmins		Задайте значение «Истина» (по умолчанию), чтобы добавить владельца компьютера, обозначенного свойством VirtualMachine.Admin.Owner, в группу локальных администраторов в компьютере.
VirtualMachine.Admin.AllowLogin		Задайте значение «Истина», чтобы добавить владельца компьютера в локальную группу пользователей удаленного рабочего стола, обозначенную свойством VirtualMachine.Admin.Owner.
VirtualMachine.Admin.UseGuestAgent		Если гостевой агент установлен как услуга в шаблоне для клонирования, задайте значение «Истина» в схеме элементов компьютера, чтобы включить службу гостевого агента в компьютерах, клонированных на основе этого шаблона. Служба гостевого агента запускается тогда, когда запускается компьютер. Чтобы деактивировать гостевой агент, установите значение «ложь» (False). Если задать значение «Ложь», улучшенный клонированный рабочий процесс не будет пользоваться гостевым агентом для задач гостевой операционной системы, сводя его функциональность к процессу VMwareCloneWorkflow. Если значение не указано или задано любое значение, кроме значения «Ложь», улучшенный клонированный рабочий процесс будет отправлять рабочие элементы в гостевой агент.
VirtualMachine.DiskN.Active		Задайте значение «Истина» (по умолчанию), чтобы указать, что диск <i>N</i> компьютера активен. Задайте значение «Ложь», чтобы указать, что диск <i>N</i> компьютера неактивен.
VirtualMachine.DiskN.Label		Указывает метку для диска компьютера <i>N</i> . Длина метки диска не может превышать 32 символа. Нумерация дисков должна быть последовательной. При использовании с гостевым агентом указывает метку диска компьютера <i>N</i> внутри гостевой операционной системы.

Таблица 1-13. Настраиваемые свойства для настройки клонированных компьютеров с помощью ведомости по гостевому агенту (продолжение)

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.DiskN.Letter		Указывает букву диска или точку подключения диска <i>N</i> компьютера. Значение по умолчанию — C. Например, чтобы указать букву D для диска 1, задайте настраиваемое свойство в качестве VirtualMachine.Disk1.Letter и введите значение D. Нумерация дисков должна быть последовательной. При использовании вместе с гостевым агентом это значение указывает букву диска или точку подключения, которая используется гостевым агентом в гостевой операционной системе для подключения дополнительного диска <i>N</i> .
VirtualMachine.Admin.CustomizeGuestOSDelay		Задаёт время ожидания после окончания настройки и перед запуском настройки гостевой операционной системы. Формат значения должен быть такой: ЧЧ:ММ:СС. Если значение не задано, то значение по умолчанию — это одна минута (00:01:00). Если не добавлять настраиваемое свойство, подготовка может закончиться ошибкой. Это происходит, когда виртуальная машина перезапускается до завершения выполнения рабочих элементов гостевого агента, что приводит к ошибке подготовки.
VirtualMachine.Customize.WaitComplete		Если задано значение «Истина», то рабочий процесс подготовки не будет отправлять рабочие элементы гостевому агенту до полного завершения настройки. Задайте значение «Ложь», чтобы разрешить создание рабочих элементов до завершения настройки.
VirtualMachine.SoftwareN.Name		Указывает описательное имя приложения <i>N</i> или сценария, которые нужно установить или запустить во время подготовки. Это необязательное свойство, используемое лишь в информационных целях. Оно не несёт практического значения для улучшенного рабочего процесса клонирования или гостевого агента. Оно может пригодиться, когда пользователь выбирает программное обеспечение в интерфейсе пользователя или когда создаются отчёты по использованию программного обеспечения.

Таблица 1-13. Настраиваемые свойства для настройки клонированных компьютеров с помощью ведомости по гостевому агенту (продолжение)

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.SoftwareN.ScriptPath		<p>Указывает полный путь к сценарию установки приложения. Путь должен быть допустимым абсолютным путем в том виде, в котором он отображается для гостевой операционной системы, и должен включать в себя имя файла сценария.</p> <p>Можно передать значения настраиваемых свойств в качестве параметров сценария, вставив {CustomPropertyName} в строке пути. Например, если имя настраиваемого свойства — ActivationKey, а его значение — 1234, путь к сценарию будет таким: D:\InstallApp.bat -key {ActivationKey}. Гостевой агент запускает команду D:\InstallApp.bat -key 1234. Файл сценария можно затем запрограммировать на принятие и использование этого значения.</p>
VirtualMachine.SoftwareN.ISOName		<p>Указывает путь и имя ISO-файла относительно к корневому каталогу хранилища данных. Используется такой формат: /folder_name/subfolder_name/file_name.iso. Если значение не указано, ISO-файл не подключается.</p>
VirtualMachine.SoftwareN.ISOLocation		<p>Указывает путь к хранилищу, содержащий файл образа ISO, который будет использоваться приложением или сценарием. Отформатируйте путь, чтобы он выглядел так, как он выглядит в резервировании узла, например: netapp-1:it_nfs_1. Если значение не указано, ISO-файл не подключается.</p>

Настраиваемые свойства сети

Можно указать конфигурацию для конкретных сетевых устройств на компьютере с помощью настраиваемых свойств.

Общие настраиваемые свойства, относящиеся к сети, перечислены в следующей таблице. Сведения о дополнительных и связанных настраиваемых свойствах см. в разделах *Настраиваемые свойства для схем элементов клонов* и *Настраиваемые свойства для сети* в *Справочник по настраиваемым свойствам*.

Таблица 1-14. Настраиваемые свойства для конфигурации сетей

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.NetworkN.Addresses		Указывает IP-адрес сетевого устройства <i>N</i> в компьютере, подготовленном с помощью статического IP-адреса.
VirtualMachine.NetworkN.MacAddressType		<p>Указывает, создается ли MAC-адрес сетевого устройства <i>N</i> автоматически или его задает пользователь (статический адрес). Это свойство доступно для клонирования.</p> <p>Создается значение по умолчанию. Если значение статичное, то, чтобы указать MAC-адрес, следует использовать параметр <code>VirtualMachine.NetworkN.MacAddress</code>.</p> <p>Настраиваемые свойства <code>VirtualMachine.NetworkN</code> используются как уникальные свойства для схем элементов и компьютеров. Когда запрашивается компьютер, выделение сетевого адреса и IP-адреса выполняется перед назначением компьютера резервированию. Так как схемы элементов не всегда назначаются определенному резервированию, не используйте это свойство в резервировании. Это свойство не поддерживается для NAT или маршрутизируемых сетей по требованию.</p>

Таблица 1-14. Настраиваемые свойства для конфигурации сетей (продолжение)

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.NetworkN.MacAddress		<p>Указывает MAC-адрес сетевого устройства <i>N</i>. Это свойство доступно для клонирования.</p> <p>Если значение параметра <code>VirtualMachine.NetworkN.MacAddressType</code> создается автоматически, это свойство содержит созданный адрес.</p> <p>Если значение параметра <code>VirtualMachine.NetworkN.MacAddressType</code> статично, это свойство указывает MAC-адрес. Для виртуальных машин, подготовленных на узлах сервера ESX, адрес должен находиться в диапазоне, указанном решением VMware. Дополнительную информацию см. в документации по vSphere.</p> <p>Настраиваемые свойства <code>VirtualMachine.NetworkN</code> используются как уникальные свойства для схем элементов и компьютеров. Когда запрашивается компьютер, выделение сетевого адреса и IP-адреса выполняется перед назначением компьютера резервированию. Так как схемы элементов не всегда назначаются определенному резервированию, не используйте это свойство в резервировании. Это свойство не поддерживается для NAT или маршрутизируемых сетей по требованию.</p>

Таблица 1-14. Настраиваемые свойства для конфигурации сетей (продолжение)

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.NetworkN.Name		<p>Указывает имя сети, к которой нужно подключиться, например сетевое устройство <i>N</i>, к которому подключен компьютер. Это эквивалент сетевого адаптера от сетевой платы (NIC).</p> <p>По умолчанию сеть назначается на основании сетевых путей, доступных в резервировании, в котором подготавливается компьютер. См. также <code>VirtualMachine.NetworkN.AddressType</code>.</p> <p>Чтобы убедиться, что сетевое устройство подключено к определенной сети, задайте в качестве значения этого свойства имя сети в доступном резервировании. Например, если задать свойства для <i>N= 0</i> и <i>1</i> и если сеть выбрана в связанном резервировании, вы получите две сетевые интерфейсные карты и назначенное им значение.</p> <p>Настраиваемые свойства <code>VirtualMachine.NetworkN</code> используются как уникальные свойства для отдельных схем элементов и компьютеров. Когда запрашивается компьютер, выделение сетевого адреса и IP-адреса выполняется перед назначением компьютера резервированию. Так как схемы элементов не всегда назначаются определенному резервированию, не используйте это свойство в резервировании. Это свойство не поддерживается для NAT или маршрутизируемых сетей по требованию.</p> <p>Пример того, как использовать это настраиваемое свойство для динамического задания <code>VirtualMachine.Network0.Name</code> на основе элементов, которые потребитель выбрал в списке предварительно определенных доступных сетей, см. в записи блога Добавление раскрывающегося списка «Выбор сети» в vRA 7.</p>

Таблица 1-14. Настраиваемые свойства для конфигурации сетей (продолжение)

Настраиваемое свойство	Мое значение	Описание
VirtualMachine.NetworkN.PortID		<p>Указывает идентификатор порта, который нужно использовать для сетевого устройства <i>N</i> при использовании группы dvPort с распределенным коммутатором vSphere.</p> <p>Настраиваемые свойства VirtualMachine.NetworkN используются как уникальные свойства для схем элементов и компьютеров. Когда запрашивается компьютер, выделение сетевого адреса и IP-адреса выполняется перед назначением компьютера резервированию. Так как схемы элементов не всегда назначаются определенному резервированию, не используйте это свойство в резервировании. Это свойство не поддерживается для NAT или маршрутизируемых сетей по требованию.</p>
VirtualMachine.NetworkN.NetworkProfileName		<p>Указывает имя профиля сети, на базе которого нужно назначить статический IP-адрес сетевому устройству <i>N</i> или получить диапазон статических IP-адресов, которые можно назначить сетевому устройству <i>N</i> клонированного компьютера, где <i>N=0</i> для первого устройства, 1 для второго и т. д.</p> <p>Профиль сети, на который указывает это свойство, используется для выделения IP-адреса. Это свойство определяет сеть, к которой подключен компьютер, на основе резервирования.</p>

Таблица 1-14. Настраиваемые свойства для конфигурации сетей (продолжение)

Настраиваемое свойство	Мое значение	Описание
<ul style="list-style-type: none"> ■ VirtualMachine.NetworkN.SubnetMask ■ VirtualMachine.NetworkN.Gateway ■ VirtualMachine.NetworkN.PrimaryDns ■ VirtualMachine.NetworkN.SecondaryDns ■ VirtualMachine.NetworkN.PrimaryWins ■ VirtualMachine.NetworkN.SecondaryWins ■ VirtualMachine.NetworkN.DnsSuffix ■ VirtualMachine.NetworkN.DnsSearchSuffixes 		<p>Добавление имени позволяет создавать несколько версий настраиваемого свойства. Например, пулы подсистем балансировки нагрузки, настроенные для общего пользования, и компьютеры с высокими, средними и низкими требованиями к производительности могут быть обозначены следующими свойствами.</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low <p>Настраивает атрибуты профиля сети, указанные в VirtualMachine.NetworkN.NetworkProfileName.</p>
VCNS.LoadBalancerEdgePool.Name <i>s.name</i>		<p>Указывает пулы подсистем балансировки нагрузки NSX, которым назначается виртуальная машина во время подготовки. Виртуальная машина назначается всем портам службы всех указанных пулов. Значение — это имя <i>края</i> или <i>пула</i> либо список имен <i>краев</i> или <i>пулов</i>, разделенных запятыми. Имена следует вводить с учетом регистра.</p> <p>Добавление имени позволяет создавать несколько версий настраиваемого свойства. Например, пулы подсистем балансировки нагрузки, настроенные для общего пользования, и компьютеры с высокими, средними и низкими требованиями к производительности могут быть обозначены следующими свойствами.</p> <ul style="list-style-type: none"> ■ VCNS.LoadBalancerEdgePool.Names ■ VCNS.LoadBalancerEdgePool.Names.moderate ■ VCNS.LoadBalancerEdgePool.Names.high ■ VCNS.LoadBalancerEdgePool.Names.low

Таблица 1-14. Настраиваемые свойства для конфигурации сетей (продолжение)

Настраиваемое свойство	Мое значение	Описание
<code>VCNS.SecurityGroup.Names.name</code>		<p>Указывает группу или группы безопасности NSX, которым назначается виртуальная машина во время подготовки. Значение — это имя группы безопасности или список имен, разделенных запятыми. Имена следует вводить с учетом регистра.</p> <p>Добавление имени позволяет создавать несколько версий свойства, которые можно использовать по отдельности или в сочетании. Например, группы безопасности, предназначенные для общего использования, для отдела продаж и для отдела поддержки, могут обозначаться следующими свойствами:</p> <ul style="list-style-type: none"> ■ <code>VCNS.SecurityGroup.Names</code> ■ <code>VCNS.SecurityGroup.Names.sale</code> <code>s</code> ■ <code>VCNS.SecurityGroup.Names.support</code> <code>ort</code>
<code>VCNS.SecurityTag.Names.name</code>		<p>Указывает тег или теги безопасности NSX, которым назначается виртуальная машина во время подготовки. Значение — это имя тега безопасности или список имен, разделенных запятыми. Имена следует вводить с учетом регистра.</p> <p>Добавление имени позволяет создавать несколько версий свойства, которые можно использовать по отдельности или в сочетании. Например, теги системы безопасности, предназначенные для общего использования, для отдела продаж и для отдела поддержки, могут обозначаться следующими свойствами:</p> <ul style="list-style-type: none"> ■ <code>VCNS.SecurityTag.Names</code> ■ <code>VCNS.SecurityTag.Names.sales</code> ■ <code>VCNS.SecurityTag.Names.support</code> <code>t</code>

Присоединение компьютера Linux к домену Windows Active Directory

При подготовке компьютера присоединить компьютер Linux к домену Windows Active Directory можно несколькими способами.

- При подготовке компьютера путем клонирования необходимо использовать спецификацию настройки (для подготовки компьютера vSphere) или включить профиль гостевой операционной системы с шаблоном SCVMM. После подготовки компьютера он присоединится к указанному домену.

- Если компьютер подготавливается не путем клонирования, можно для указания домена использовать параметр суффикса DNS в профиле сети, связанном с данной схемой элементов. Однако для подготовки клона Windows с использованием назначения статического IP-адреса *необходимо* использовать спецификацию настройки vSphere.
- При использовании спецификации настройки vSphere подготавливаемые компьютеры присоединяются к домену, указанному в спецификации настройки, а не к домену, указанному в DNS-суффиксе в профиле сети, связанном с данной схемой элементов.

Спецификации настройки vSphere — это объекты vSphere, которые содержат предварительно определенный набор условий для параметров гостевой операционной системы Windows или Linux. Имя спецификации настройки можно добавить в схему элементов vRealize Automation в параметре

Спецификация настройки на вкладке **Сведения о сборке** данного компьютера.

Дополнительные сведения о создании спецификаций настройки в vSphere см. в разделах о спецификации настройки в [документации по продукту vSphere](#), например в разделе *Создание спецификаций настройки и управление ими*.

Подготовка к резервированию vCloud Air и vCloud Director

Чтобы подготовиться к резервированию компьютеров vCloud Air и vCloud Director с помощью vRealize Automation, необходимо настроить виртуальный центр обработки данных организации с шаблонами и объектами настройки.

Для подготовки ресурсов vCloud Air и vCloud Director с помощью vRealize Automation в организации нужен шаблон клонирования, который состоит из одного или нескольких ресурсов компьютера.

Шаблоны, которые должны быть общими для всех организаций, нужно опубликовать. Для vRealize Automation в качестве источника клонирования доступны только зарезервированные шаблоны.

Примечание При создании схемы элементов путем клонирования из шаблона уникальный идентификатор шаблона ассоциируется со схемой элементов. При публикации схемы элементов в каталоге vRealize Automation и использовании ее в процессах подготовки и сбора данных распознается связанный шаблон. Если удалить шаблон в vCloud Air или vCloud Director, последующая подготовка vRealize Automation и сбор данных будут невозможны, потому что они связаны с уже несуществующим шаблоном. Вместо удаления и повторного создания шаблона, например для загрузки обновленной версии, замените шаблон, следуя процедуре замены шаблона vCloud Air/vCloud Director. Использование vCloud Air или vCloud Director для замены, а не удаления и повторного создания шаблона, позволяет сохранить уникальный идентификатор шаблона неизменным и обеспечить выделение ресурсов и сбор данных, чтобы продолжить работу.

Следующий обзор иллюстрирует шаги, которые необходимо выполнить, прежде чем использовать vRealize Automation для создания конечных точек, а также определения резервирований и схем элементов. Дополнительные сведения об этих задачах администрирования см. в документации по продукту vCloud Air и vCloud Director.

1. В vCloud Air или vCloud Director создайте шаблон для клонирования и добавьте его в каталог организации.

2. В vCloud Air или vCloud Director используйте шаблон, чтобы задать на каждом компьютере пользовательские настройки, такие как пароли, домен и сценарии для гостевой операционной системы. vRealize Automation можно использовать, чтобы переопределить некоторые из этих параметров. Настройки могут отличаться в зависимости от гостевой операционной системы ресурса.
3. В vCloud Air или vCloud Director настройте каталог для совместного доступа в организации. В vCloud Air или vCloud Director настройте доступ администратора учетных записей к соответствующим организациям, чтобы у всех пользователей и групп в организации был доступ к каталогу. Без такого назначения общего доступа шаблоны каталога не будут видны конечным точкам или архитекторам схем элементов в vRealize Automation.
4. Соберите следующую информацию, чтобы добавить ее в схемы элементов:
 - Имя шаблона vCloud Air или vCloud Director.
 - Общий объем хранилища, указанного для шаблона.

Подготовка к процессу подготовки Linux Kickstart

При подготовке Linux Kickstart используется файл конфигурации, чтобы автоматизировать установку Linux на подготовленном компьютере. Чтобы подготовиться к подготовке, необходимо создать загружаемый образ ISO и файл конфигурации Kickstart или autoYaST.

Ниже приведен общий обзор шагов, необходимых для подготовки к процессу подготовки Linux Kickstart.

1. Убедитесь, что сервер DHCP доступен в сети. vRealize Automation может выполнять подготовку компьютеров с помощью подготовки Linux Kickstart, только если сервер DHCP доступен.
2. Подготовьте файл конфигурации. В файле конфигурации необходимо указать расположение сервера vRealize Automation и установочного пакета агента Linux. См. [Подготовка примера файла конфигурации Linux Kickstart](#).
3. В файлах isolinux/isolinux.cfg или loader/isolinux.cfg укажите имя и расположение файла конфигурации и соответствующего источника распределения Linux.
4. Создайте образ загрузки ISO и сохраните его в расположении, которое соответствует требованиям платформы виртуализации. Дополнительные сведения о требованиях к расположению см. в документации, предоставленной гипервизором.
5. (дополнительно) Добавьте сценарии настройки.
 - а) Дополнительные сведения о том, как указать послеустановочные сценарии настройки в файле конфигурации, см. в разделе [Указание пользовательских сценариев в файлах конфигурации Kickstart и AutoYaST](#).
 - б) Дополнительные сведения о том, как вызвать сценарии Visual Basic в схеме элементов, см. в разделе [Контрольный список для запуска сценариев Visual Basic во время подготовки](#).
6. Соберите следующую информацию, чтобы разработчики схем элементов могли добавить ее в свои схемы элементов:
 - а) название и расположение образа ISO;

- б) для интеграций vCenter Server версию гостевой операционной системы vCenter Server, с помощью которой vCenter Server должен создать компьютер.

Примечание Чтобы добавить требуемую информацию об образе ISO, можно создать группу свойств с набором свойств `BootIsoProperties`. Это упрощает процесс добавления этой информации в схемы элементов должным образом.

Подготовка примера файла конфигурации Linux Kickstart

vRealize Automation предоставляет примеры файлов конфигурации, которые можно изменять в соответствии со своими потребностями. Чтобы сделать файлы пригодными к использованию, необходимо внести несколько изменений.

Процедура

1. Перейдите на страницу консоли управления устройства vRealize Automation.
Например, <https://va-hostname.domain.com>.
2. Выберите **страницу гостевого агента и агента программного обеспечения** в разделе страницы установки компонентов vRealize Automation.
Например, <https://va-hostname.domain.com/software/index.html>.
Откроется страница **Средства установки гостевого агента и агента программного обеспечения** со ссылками, доступными для загрузки.
3. Выберите **Пакеты гостевых агентов Linux** в разделе страницы средств установки гостевых агентов, чтобы загрузить и сохранить файл `LinuxGuestAgentPkgs.zip`.
4. Распакуйте загруженный файл `LinuxGuestAgentPkgs.zip`, чтобы создать папку `VraLinuxGuestAgent`.
5. Перейдите в подкаталог `VraLinuxGuestAgent`, соответствующий гостевой операционной системе, для развертывания во время подготовки.
Например, `rhel32`.
6. Откройте файл в подкаталоге примеров, соответствующем целевой системе.
На пример, `samples/sample-https-rhel6-x86.cfg`.
7. Замените все экземпляры строки `host=dcac.example.net` на IP-адрес или полное доменное имя и номер порта для службы диспетчера или подсистемы балансировки нагрузки для нее.

Платформа	Требуемый формат
vSphere ESXi	Пример IP-адреса — <code>—host=172.20.9.59</code>
vSphere ESX	Пример IP-адреса — <code>—host=172.20.9.58</code>
SUSE 10	Пример IP-адреса — <code>—host=172.20.9.57</code>
Все остальные	Пример полного доменного имени — <code>—host=mycompany-host1.mycompany.local: 443</code>

- Найдите каждый экземпляр `gugent.rpm` или `gugent.tar.gz` и замените URL-адрес `rpm.example.net` на расположение пакета гостевого агента.

Пример:

```
rpm -i nfs:172.20.9.59/suseagent/gugent.rpm
```

- Сохраните файл в папку, которая доступна для подготовленных компьютеров.

Указание пользовательских сценариев в файлах конфигурации Kickstart и AutoYaST

Файл конфигурации можно изменить, чтобы скопировать пользовательские сценарии на новые подготовленные компьютеры или установить их. Агент Linux выполняет сценарии в указанной точке рабочего процесса.

Сценарий может ссылаться на любой из файлов `./properties.xml` в каталогах `/usr/share/gugent/site/workitem`.

Необходимые условия

- Подготовьте файл конфигурации Kickstart или AutoYaST. См. раздел [Подготовка примера файла конфигурации Linux Kickstart](#).
- Сценарий должен вернуть ненулевое значение для сбоя, чтобы предотвратить сбой подготовки компьютера.

Процедура

- Создайте или определите сценарий, который необходимо использовать.
- Сохраните сценарий, указав для него имя `NN_scriptname`, где
`NN` — двузначное число. Сценарии выполняются в порядке приоритета: от самого низкого до самого высокого. Если у двух сценариев одинаковое число, порядок определяется по алфавиту в зависимости от `scriptname`.
- Сделайте сценарий запускаемым.
- Найдите послеустановочный раздел файла конфигурации Kickstart или AutoYaST.
В Kickstart он обозначается как `%post`. В autoYaST он обозначается как `post-scripts`.
- Измените послеустановочный раздел, чтобы можно было скопировать сценарий в выбранный каталог `/usr/share/gugent/site/workitem` или установить его.

Пользовательские сценарии зачастую выполняются для виртуальных файлов Kickstart и AutoYaST с рабочими элементами SetupOS (чтобы создать подготовку) и CustomizeOS (чтобы клонировать подготовку). Тем не менее, сценарии можно запустить в любой точке рабочего процесса.

Например, чтобы скопировать сценарий `11_addusers.sh` в каталог `/usr/share/gugent/site/Setup05` подготовленного компьютера, можно изменить файл конфигурации, выполнив следующую команду:

```
cp nfs:172.20.9.59/linuxscripts/11_addusers.sh /usr/share/gugent/site/Setup05
```

Результаты

Агент Linux выполняет сценарий в порядке согласно каталогу рабочего элемента и имени файла сценария.

Подготовка к процессу подготовки SCCM

vRealize Automation загружает подготовленный компьютер из образа ISO, после чего управление переходит к указанной последовательности задач SCCM.

Подготовка SCCM поддерживается для развертывания операционных систем Windows. Linux не поддерживается. Распределение и обновления программного обеспечения не поддерживаются.

По умолчанию на компьютере SCCM настроено подтверждение членства в соответствующей коллекции каждые 10 секунд после подготовки. В некоторых случаях этот интервал может стать причиной проблем в процессе регистрации. Для настройки процесса подтверждения доступны два свойства. Первое свойство называется `SCCM refresh collection setting`. По умолчанию для этого свойства задано значение `true`, которое подтверждает, что компьютер выполняет проверку членства. При необходимости можно изменить его на `false`, чтобы компьютер пропускал проверку членства. Второе свойство называется `SCCM machine membership check interval`. Как отмечалось ранее, значение по умолчанию — 10 секунд, но если возникли проблемы с регистрацией, можно задать другое значение, увеличив тем самым окно повторного запуска. Оба эти свойства расположены в разделе глобальных параметров инфраструктуры как услуги, в меню **Инфраструктура > Администрирование > Глобальные параметры**.

Ниже приведен общий обзор шагов, необходимых для подготовки к процессу подготовки SCCM.

1. Для обмена данными с SCCM требуется имя NetBIOS сервера SCCM.

Совместно с администратором сети убедитесь, что, по крайней мере, один Distributed Execution Manager (DEM) может преобразовать полное доменное имя сервера SCCM в свое имя NetBIOS.

Вам не нужно размещать диспетчеры DEM непосредственно в той же сети, что и сервер SCCM, но диспетчеры DEM должны быть способны связываться с сервером SCCM по IP-адресу.

2. Создайте программный пакет, который включает в себя гостевой агент vRealize Automation. См. раздел [Создание пакета программного обеспечения для подготовки SCCM](#).
3. В SCCM создайте желаемую последовательность задач для подготовки компьютера. Заключительным шагом должна быть установка созданного программного пакета, который содержит гостевой агент vRealize Automation. Дополнительные сведения о создании последовательности задач и об установке программных пакетов см. в документации по SCCM.
4. Создайте автономный самоуправляемый образ загрузки ISO для последовательности задач. По умолчанию SCCM создает практически самоуправляемый образ загрузки ISO. Дополнительные сведения о настройке SCCM для автономных самоуправляемых образов ISO см. в документации по SCCM.

5. Скопируйте образ ISO в расположение, которое соответствует требованиям платформы виртуализации. Если соответствующее расположение неизвестно, см. документацию, предоставляемую в гипервизоре.
6. Соберите следующую информацию, чтобы разработчики схем элементов могли добавить ее в схемы элементов:
 - а) имя коллекции, содержащей последовательность задач;
 - б) полное доменное имя сервера SCCM, на котором расположена коллекция, содержащая последовательность задач;
 - в) код сайта сервера SCCM;
 - г) учетные данные с правами администратора для входа на сервер SCCM;
 - д) (Необязательно.) при интеграции SCVMM сведения об образе ISO, виртуальном жестком диске или профиле оборудования, которые будут назначены подготовленному компьютеру.

Создание пакета программного обеспечения для подготовки SCCM

Заключительным шагом в последовательности задач SCCM должна стать установка пакета программного обеспечения, в который входит гостевой агент vRealize Automation.

Процедура

1. Перейдите на страницу консоли управления устройства vRealize Automation.
Например, <https://va-hostname.domain.com>.
2. Выберите **страницу гостевого агента и агента программного обеспечения** в разделе страницы установки компонентов vRealize Automation.
Например, <https://va-hostname.domain.com/software/index.html>.
Откроется страница **Средства установки гостевого агента и агента программного обеспечения** со ссылками, доступными для загрузки.
3. Выберите файлы гостевых агентов Windows (**32-разрядная версия**) или (**64-разрядная версия**) в разделе страницы установки компонентов, чтобы загрузить и сохранить файлы `GuestAgentInstaller.exe` или `GuestAgentInstaller_x64.exe`.
4. Извлеките файлы гостевого агента Windows в расположение, доступное для SCCM.
Будет создан каталог `C:\VRMGuestAgent`. Не переименовывайте этот каталог.
5. Создайте пакет программного обеспечения из файла определения `SCCMPackageDefinitionFile.sms`.
6. Сделайте пакет программного обеспечения доступным для точки распределения.
7. Выберите содержимое извлеченных файлов гостевого агента Windows как исходные файлы.

Подготовка к процессу подготовки WIM

Подготовка компьютера путем его загрузки в среду WinPE и установки операционной системы с помощью образа WIM существующего эталонного компьютера Windows.

Ниже приведен общий обзор шагов, необходимых для подготовки к процессу подготовки WIM.

1. Определите или создайте область промежуточного хранения. Область промежуточного хранения должна быть сетевым каталогом, который можно обозначить в качестве пути UNC или подключить как сетевой накопитель с помощью:
 - эталонного компьютера;
 - системы, в которой создается образ WinPE;
 - узла виртуализации, в котором подготавливаются компьютеры.
2. Убедитесь в наличии сервера DHCP в сети. vRealize Automation может выполнять подготовку компьютеров с помощью образа WIM, только если сервер DHCP доступен.
3. Определите или создайте эталонный компьютер на платформе виртуализации, которая будет использоваться для подготовки. Чтобы узнать больше о требованиях vRealize Automation, см. раздел [Требования к эталонным компьютерам при развертывании образов WIM](#). Чтобы узнать больше о создании эталонного компьютера, см. документацию гипервизора.
4. Используя System Preparation Utility for Windows, подготовьте операционную систему эталонного компьютера для развертывания. См. раздел [Требования к SysPrep для эталонного компьютера](#).
5. Создайте образ WIM эталонного компьютера. Не используйте пробелы в имени WIM-файла образа, иначе подготовка к работе завершится ошибкой.
6. Создайте образ WinPE, который содержит гостевой агент vRealize Automation.
 - (дополнительно) Создайте пользовательские сценарии, которые нужно будет использовать, чтобы настроить подготовленные компьютеры и поместить их в соответствующий каталог рабочих элементов.
 - При использовании VirtIO для сетевых интерфейсов или интерфейсов хранилища нужно убедиться, что в образ WinPE и WIM включены необходимые драйверы. См. раздел [Подготовка к развертыванию образов WIM с помощью драйверов VirtIO](#).

При создании образа WinPE необходимо вручную вставить гостевой агент vRealize Automation. См. раздел [Вставка гостевого агента в образ WinPE вручную](#).
7. Поместите образ WinPE в расположение, соответствующее требованиям вашей платформы виртуализации. Если расположение неизвестно, см. документацию по гипервизору.
8. Соберите следующую информацию, которую необходимо включить в схему элементов:
 - а) Имя и расположение образа ISO WinPE.
 - б) имя WIM-файла, UNC-путь к этому файлу и индекс, необходимый для извлечения образа из WIM-файла;
 - в) имя пользователя и пароль, которые будут использоваться для сопоставления пути к WIM-образу с сетевым диском подготовленного компьютера;
 - г) (дополнительно) если необходимо изменить значение буквы диска по умолчанию (K), с которой сопоставляется путь к WIM-образу на подготовленном компьютере;

- д) для интеграций vCenter Server версию гостевой операционной системы vCenter Server, с помощью которой vCenter Server должен создать компьютер.
- е) (Необязательно.) при интеграции SCVMM сведения об образе ISO, виртуальном жестком диске или профиле оборудования, которые будут назначены подготовленному компьютеру.

Примечание Можно создать группу свойств, чтобы добавить все необходимые сведения.

Использование групп свойств облегчает процесс правильного добавления нужной информации в схемы элементов.

Процедура

1. Требования к эталонным компьютерам при развертывании образов WIM

При развертывании образов WIM создается образ WIM для эталонного компьютера. Эталонный компьютер должен соответствовать основным требованиям образа, чтобы его можно было использовать для подготовки в vRealize Automation

2. Требования к SysPrep для эталонного компьютера

Файл ответов SysPrep содержит несколько необходимых параметров, которые используются для подготовки WIM.

3. Подготовка к развертыванию образов WIM с помощью драйверов VirtIO

При использовании VirtIO для сетевых интерфейсов или интерфейсов хранилища нужно убедиться, что в образ WinPE и WIM включены необходимые драйверы. Как правило, VirtIO обеспечивает лучшую производительность при подготовке с помощью KVM (RHEV).

4. Вставка гостевого агента в образ WinPE вручную

Гостевой агент vRealize Automation должен быть вставлен в образ WinPE вручную.

Требования к эталонным компьютерам при развертывании образов WIM

При развертывании образов WIM создается образ WIM для эталонного компьютера. Эталонный компьютер должен соответствовать основным требованиям образа, чтобы его можно было использовать для подготовки в vRealize Automation

Ниже приведен общий обзор шагов, необходимых для подготовки эталонного компьютера к развертыванию.

1. Если на эталонном компьютере установлена операционная система Windows Server 2008 R2, Windows Server 2012, Windows 7 или Windows 8, при установке по умолчанию на системном жестком диске кроме основного раздела создается еще один небольшой раздел. vRealize Automation не поддерживает использование образов WIM, созданных на таких эталонных компьютерах с несколькими разделами. При установке этот раздел нужно удалить.
2. Установите на эталонном компьютере NET 4.5 и пакет автоматической установки Windows для Windows 7 (с WinPE 3.0).
3. Если на эталонном компьютере установлена операционная система Windows Server 2003 или Windows XP, сбросьте пароль администратора, чтобы поле стало пустым. (В этой системе пароль не используется.)

4. (Необязательно.) Если требуется активировать интеграцию XenDesktop, установите и настройте Citrix Virtual Desktop Agent.
5. (Необязательно.) Агент WMI требуется для сбора определенных данных с компьютера Windows, управляемого с помощью vRealize Automation, например сведений о состоянии Active Directory владельца компьютера. Для успешного управления компьютерами Windows необходимо установить агент WMI (как правило, на узле службы диспетчера) и разрешить ему собирать данные с компьютеров Windows. См. *Установка vRealize Automation*.

Требования к SysPrep для эталонного компьютера

Файл ответов SysPrep содержит несколько необходимых параметров, которые используются для подготовки WIM.

Таблица 1-15. Необходимые параметры для эталонных компьютеров Windows Server или Windows XP

Параметры GuiUnattended	Значение
AutoLogon	Да
AutoLogonCount	1
AutoLogonUsername	имя пользователя (имя_пользователя и пароль являются учетными данными, используемыми для автоматического входа при загрузке вновь подготовленного компьютера в гостевую операционную систему. Как правило используется администратор.)
AutoLogonPassword	пароль, соответствующий AutoLogonUsername.

Таблица 1-16. Необходимые параметры SysPrep для эталонного компьютера, не использующего Windows Server 2003 или Windows XP.

Параметры AutoLogon	Значение
Enabled	Да
LogonCount	1

Таблица 1-16. Необходимые параметры SysPrep для эталонного компьютера, не использующего Windows Server 2003 или Windows XP. (продолжение)

Параметры AutoLogon	Значение
Username	<p><i>имя пользователя</i></p> <p>(<i>имя_пользователя</i> и <i>пароль</i> являются учетными данными, используемыми для автоматического входа при загрузке вновь подготовленного компьютера в гостевую операционную систему. Как правило используется администратор.)</p>
Password	<p><i>пароль</i></p> <p>(<i>имя_пользователя</i> и <i>пароль</i> являются учетными данными, используемыми для автоматического входа при загрузке вновь подготовленного компьютера в гостевую операционную систему. Как правило используется администратор.)</p> <p>Примечание На эталонные компьютеры, использующие более новую платформу Windows, чем Windows Server 2003 или Windows XP, необходимо установить пароль автоматического входа в систему с помощью настраиваемого свойства <code>Sysprep.GuiUnattended.AdminPassword</code>. Удобно для обеспечения этого создать группу свойств, включающую данное настраиваемое свойство, чтобы администраторы арендаторов и менеджеры бизнес-групп смогли корректно добавлять эти сведения в свои схемы элементов.</p>

Подготовка к развертыванию образов WIM с помощью драйверов VirtIO

При использовании VirtIO для сетевых интерфейсов или интерфейсов хранилища нужно убедиться, что в образ WinPE и WIM включены необходимые драйверы. Как правило, VirtIO обеспечивает лучшую производительность при подготовке с помощью KVM (RHEV).

Драйверы Windows для VirtIO входят в состав Red Hat Enterprise Virtualization и находятся в каталоге `/usr/share/virtio-win` в файловой системе диспетчера Red Hat Enterprise Virtualization Manager. Драйверы также входят в состав средств Red Hat Enterprise Virtualization Guest, которые расположены в файле `/usr/share/rhev-guest-tools-iso/rhev-tools-setup.iso`.

Общая процедура для реализации подготовки с использованием образов WIM с помощью драйверов VirtIO выглядит следующим образом.

1. Создайте образ WIM из эталонного компьютера Windows, на котором установлены драйверы VirtIO, или вставьте драйверы в существующий образ WIM.
2. Скопируйте файлы драйверов VirtIO и вставьте драйверы в образ WinPE.
3. Передайте образ ISO WinPE в домены хранения ISO Red Hat Enterprise Virtualization, выполнив команду `rhev-m-iso-uploader`. Для получения дополнительных сведений об управлении образами ISO в RHEV см. документацию по Red Hat.
4. Создайте схему элементов KVM (RHEV) для развертывания образов WIM и выберите параметр WinPE ISO. Для настраиваемого свойства `VirtualMachine.Admin.DiskInterfaceType` необходимо задать значение **VirtIO**. Администратор структуры может добавлять эту информацию в группу свойств для включения в схемы элементов.

Настраиваемые свойства `Image.ISO.Location` и `Image.ISO.Name` не используются для схем элементов KVM (RHEV).

Вставка гостевого агента в образ WinPE вручную

Гостевой агент vRealize Automation должен быть вставлен в образ WinPE вручную.

Необходимые условия

- Выберите систему Windows, в которой доступна подготовленная промежуточная среда и установлены платформа .NET 4.5 и пакет автоматической установки Windows (Automated Installation Kit, AIK) для Windows 7 (в том числе WinPE 3.0).
- Создайте WinPE.

Процедура

1. Установка гостевого агента в WinPE

Необходимо вручную скопировать файлы гостевого агента в образ WinPE.

2. Настройка файла `doagent.bat`

Необходимо вручную настроить файл `doagent.bat`.

3. Настройка файла `doagentc.bat`

Необходимо вручную настроить файл `doagentc.bat`.

4. Настройка файлов свойств гостевого агента

Необходимо вручную настроить файлы свойств гостевого агента.

Процедура

1. Установка гостевого агента в WinPE.

2. Настройка файла `doagent.bat`.

3. Настройка файла `doagentc.bat`.

4. Настройка файлов свойств гостевого агента.

Установка гостевого агента в WinPE

Необходимо вручную скопировать файлы гостевого агента в образ WinPE.

Необходимые условия

- Выберите систему Windows, в которой доступна подготовленная промежуточная среда и установлены платформа .NET 4.5 и пакет автоматической установки Windows (Automated Installation Kit, AIK) для Windows 7 (в том числе WinPE 3.0).
- Создайте WinPE.

Процедура

- ◆ Загрузите и установите гостевой агент vRealize Automation по адресу https://vRealize_VA_Hostname_fqdn/software/index.html.
 - а) Загрузите файл `GugentZip_version` на диск C на эталонном компьютере.

Выберите `GuestAgentInstaller.exe` (32-разрядная версия) или `GuestAgentInstaller_x64.exe` (64-разрядная версия) в зависимости от операционной системы.
 - б) Щелкните файл правой кнопкой мыши и выберите пункт **Свойства**.
 - в) Щелкните **Общие**.
 - г) Щелкните **Разблокировать**.
 - д) Извлеките файлы на диск C:\.

Будет создан каталог C:\VRMGuestAgent. Не переименовывайте этот каталог.

Следующие шаги

[Настройка файла doagent.bat.](#)

Настройка файла doagent.bat

Необходимо вручную настроить файл `doagent.bat`.

Необходимые условия

[Установка гостевого агента в WinPE.](#)

Процедура

1. Перейдите к каталогу `VRMGuestAgent` в образе WinPE.

Например: C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
2. Сделайте копию файла `doagent-template.bat` и назовите копию `doagent.bat`.
3. Откройте файл `doagent.bat` в текстовом редакторе.
4. Замените все экземпляры строки `#Dcas Hostname#` полным доменным именем и номером порта узла службы диспетчера `laaS`.

Параметр	Описание
Если используется подсистема балансировки нагрузки	<p>Введите полное доменное имя и порт подсистемы балансировки нагрузки для службы диспетчера <code>laaS</code>. Пример:</p> <pre>manager_service_LB.mycompany.com:443</pre>
Без подсистемы балансировки нагрузки	<p>Введите полное доменное имя и порт компьютера, на котором установлена служба диспетчера <code>laaS</code>. Пример:</p> <pre>manager_service.mycompany.com:443</pre>

5. Замените все экземпляры строки `#Protocol#` строкой `/ssl`.

6. Замените все экземпляры строки `#Comment#` строкой `REM` (после `REM` должен стоять пробел).
7. (дополнительно) Если используются самозаверяющие сертификаты, раскомментируйте команду `openssl`.

```
echo QUIT | c:\VRMGuestAgent\bin\openssl s_client -connect
```

8. Сохраните файл и закройте его.
9. Измените сценарий `Startnet.cmd`, чтобы среда WinPE включала в себя также файл `doagentc.bat` в качестве настраиваемого сценария.

Следующие шаги

[Настройка файла `doagentc.bat`.](#)

Настройка файла `doagentc.bat`

Необходимо вручную настроить файл `doagentc.bat`.

Необходимые условия

[Настройка файла `doagentc.bat`.](#)

Процедура

1. Перейдите к каталогу `VRMGuestAgent` в образе WinPE.
Например: `C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent`.
2. Сделайте копию файла `doagentsvc-template.bat` и назовите копию `doagentc.bat`.
3. Откройте файл `doagentc.bat` в текстовом редакторе.
4. Удалите все экземпляры строки `#Comment#`.
5. Замените все экземпляры строки `#Dcas Hostname#` полным доменным именем и номером порта узла службы диспетчера.

Используемый по умолчанию порт службы диспетчера — 443.

Параметр	Описание
Если используется подсистема балансировки нагрузки	Введите полное доменное имя и номер порта подсистемы балансировки нагрузки для службы диспетчера. Пример: <code>load_balancer_manager_service.mycompany.com:443</code>
Без подсистемы балансировки нагрузки	Введите полное доменное имя и номер порта службы диспетчера. Пример: <code>manager_service.mycompany.com:443</code>

6. Замените все экземпляры строки `#errorlevel#` символом 1.
7. Замените все экземпляры строки `#Protocol#` строкой `/ssl`.
8. Сохраните файл и закройте его.

Следующие шаги

[Настройка файлов свойств гостевого агента.](#)

Настройка файлов свойств гостевого агента

Необходимо вручную настроить файлы свойств гостевого агента.

Необходимые условия

[Настройка файла doagentc.bat.](#)

Процедура

1. Перейдите к каталогу VRMGuestAgent в образе WinPE.
Например: C:\Program Files (x86)\VMware\Plugins\VRM Agent\VRMGuestAgent.
2. Сделайте копию файла gument.properties и назовите копию gument.properties.template.
3. Сделайте копию файла gument.properties.template и назовите копию gumentc.properties.
4. Откройте файл gument.properties в текстовом редакторе.
5. Замените все экземпляры строки GuestAgent.log строкой X:/VRMGuestAgent/GuestAgent.log.
6. Сохраните файл и закройте его.
7. Откройте файл gumentc.properties в текстовом редакторе.
8. Замените все экземпляры строки GuestAgent.log строкой C:/VRMGuestAgent/GuestAgent.log.
9. Сохраните файл и закройте его.

Подготовка к процессу подготовки образов виртуальных машин

Перед подготовкой экземпляров с помощью OpenStack необходимо получить образы виртуальных машин и версии, настроенные в поставщике OpenStack.

Образы виртуальных машин

Образ виртуальной машины можно выбрать из списка доступных образов при создании схемы элементов для ресурсов OpenStack.

Образ виртуальной машины — это шаблон, в котором содержатся данные конфигурации программного обеспечения, в том числе операционной системы. Образами виртуальных машин управляет поставщик OpenStack. Они импортируются при сборе данных.

Если образ, используемый на схеме элементов, позже удаляется у поставщика OpenStack, он также удаляется со схемы элементов. Если из схемы элементов удалены все образы, эта схема элементов будет деактивирована и ее нельзя будет использовать для запросов компьютеров, пока в нее не добавят хотя бы один образ.

Версии OpenStack

При создании схем элементов OpenStack можно выбрать одну или несколько версий.

Версии OpenStack представляют собой шаблоны виртуального оборудования, по которым определяются спецификации ресурсов компьютера для экземпляров, подготовленных в OpenStack. Версиями управляет поставщик OpenStack. Они импортируются при сборе данных.

Подготовка к процессу подготовки образов компьютеров Amazon

Подготовьте образы компьютера и типы экземпляров Amazon для подготовки в vRealize Automation.

Общие сведения об образах компьютера Amazon

Можно выбрать образ компьютера Amazon из списка доступных образов при создании схемы элементов компьютеров Amazon.

Образ компьютера Amazon — это шаблон, который содержит данные конфигурации программного обеспечения, в том числе операционной системы. Для управления используются учетные записи Amazon Web Services. С помощью vRealize Automation можно управлять типами экземпляров, доступными для подготовки.

Образ компьютера Amazon и тип экземпляра должны быть доступны в области Amazon. В каждой области доступны отдельные типы экземпляров.

Образ компьютера Amazon можно выбрать в Amazon Web Services, сообществе пользователей или на сайте AWS Marketplace. Кроме того, можно создать и, при необходимости, предоставить доступ к своим образам компьютера Amazon другим пользователям. Один образ компьютера Amazon можно использовать для запуска нескольких экземпляров.

При подготовке облачных компьютеров с использованием учетных записей Amazon Web Services следует учитывать следующие особенности работы с образами компьютера Amazon.

- Образ компьютера Amazon должен быть указан в каждой схеме элементов.
Частный образ — это образ компьютера, доступный для определенной учетной записи и всех ее областей. Частный образ компьютера Amazon доступен для всех учетных записей, но только в определенной области каждой из них.
- После создания схемы элементов указанный образ компьютера Amazon выбирается из областей, полученных в результате сбора данных. Если доступно несколько учетных записей Amazon Web Services, у диспетчера бизнес-групп должны быть права на использование всех соответствующих частных образов компьютера Amazon. Возможности выполнения запроса на подготовку ограничиваются резервированиями, соответствующими области образа компьютера Amazon и указанному расположению пользователя.
- Для распределения образов компьютера Amazon в учетных записях Amazon Web Services следует использовать резервирования и политики. Используйте политики, чтобы ограничить набор резервирований для подготовки компьютеров на основе схемы элементов.
- С помощью vRealize Automation нельзя создавать учетные записи пользователей на облачном компьютере. При первом подключении к облачному компьютеру его владельцу необходимо выполнить вход в качестве администратора и добавить свои учетные данные vRealize Automation. Вместо владельца это может сделать администратор. Затем владелец может выполнить вход, используя свои учетные данные vRealize Automation.

Если при каждой загрузке образ компьютера Amazon генерирует пароль администратора, его можно узнать на странице «Запись изменения компьютера». Если пароля нет на странице, его можно найти в учетной записи Amazon Web Services. Генерирование пароля администратора при каждой загрузке можно настроить для всех образов компьютера Amazon. Кроме того, можно указать сведения о пароле администратора в целях поддержки пользователей, которые подготавливают компьютеры для других пользователей.

- Чтобы разрешить выполнение запросов удаленного инструментария управления Microsoft Windows (WMI) на облачных компьютерах, подготовленных в учетных записях Amazon Web Services, предоставьте агенту Microsoft Windows Remote Management (WinRM) возможность сбора данных с компьютеров Windows под управлением vRealize Automation. См. *Установка vRealize Automation*.
- Образ частного компьютера Amazon отображается для всех арендаторов.

Дополнительные сведения см. в разделах документа *Образы компьютера Amazon (Amazon Machine Images, AMI)* в документации Amazon.

Общие сведения о типах экземпляров Amazon

При создании схем элементов Amazon EC2 архитектор инфраструктуры как услуги выбирает один или несколько типов экземпляров Amazon. Администратор инфраструктуры как услуги в свою очередь может добавить или удалить типы экземпляров, чтобы контролировать, какие типы будут доступны для архитекторов.

Экземпляр Amazon EC2 представляет собой виртуальный сервер, на котором могут выполняться приложения в инфраструктуре Amazon Web Services. Экземпляры создаются на основе образа компьютера Amazon при выборе соответствующего типа экземпляра.

Чтобы подготовить компьютер с использованием учетной записи Amazon Web Services, тип экземпляра применяется к указанному образу компьютера Amazon. Список доступных типов экземпляров указывается, когда архитекторы создают схему элементов Amazon EC2. Когда пользователь запрашивает подготовку компьютера, для него доступны типы экземпляров, которые выбрал архитектор. Это может быть как один, так и несколько типов. Типы экземпляров должны поддерживаться в указанной области.

Для получения дополнительной информации см. разделы «*Выбор типов экземпляров*» и «*Сведения об экземпляре Amazon EC2*» в документации Amazon.

Добавление типа экземпляра Amazon

Вместе с vRealize Automation поставляется несколько типов экземпляров, которые предназначены для использования со схемами элементов Amazon. Администратор может добавлять и удалять типы экземпляров.

Типы экземпляров компьютеров, которыми управляют администраторы инфраструктуры как услуги, доступны разработчикам архитектуры схем элементов, когда они создают или изменяют схемы элементов Amazon. Образы компьютеров Amazon и типы экземпляров Amazon делаются доступными с помощью продукта Amazon Web Services.

Необходимые условия

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

Процедура

1. Откройте **Инфраструктура > Администрирование > Типы экземпляров**.
2. Нажмите кнопку **Создать**.
3. Добавьте новый тип экземпляра, указав следующие параметры.

Сведения о доступных типах экземпляров Amazon и значениях, которые можно указать для их параметров, см. в документации по Amazon Web Services в разделе *Типы экземпляров EC2 — Amazon Web Services (AWS)* на сайте aws.amazon.com/ec2 и *Типы экземпляров* на сайте docs.aws.amazon.com.

- Имя
- Имя API
- Имя типа
- Название производительности ввода-вывода
- ЦП
- Память (ГБ)
- Хранилище (ГБ)
- Вычислительные модули

4. Щелкните значок **Сохранить** (✓).

Результаты

Когда разработчики архитектуры инфраструктуры как услуги создают схемы элементов Amazon Web Services, они могут использовать ваши настраиваемые типы экземпляров.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Сценарий: работа с ресурсами vSphere для подготовки компьютера

Администратор vSphere, который создает шаблоны для vRealize Automation, может использовать веб-клиент vSphere для подготовки к клонированию компьютеров CentOS в vRealize Automation.

Можно преобразовать существующий эталонный компьютер CentOS в шаблон vSphere, чтобы вы и разработчики могли создавать схемы элементов для клонирования компьютеров CentOS в vRealize Automation. Для предотвращения каких-либо конфликтов, которые могут возникнуть при развертывании нескольких виртуальных машин с одинаковыми настройками, можно создать общую спецификацию настройки, которую можно использовать при создании схемы элементов для шаблонов Linux.

Необходимые условия

Определите или создайте эталонный компьютер Linux CentOS и установите на нем VMware Tools. Чтобы обеспечить подключение к Интернету, необходимо добавить по крайней мере один сетевой адаптер.

Процедура

1. Сценарий: преобразование эталонного компьютера CentOS в шаблон для Rainpole

С помощью vSphere Client можно преобразовать существующий эталонный компьютер CentOS в шаблон vSphere, на который будут ссылаться разработчики архитектуры инфраструктуры как услуги vRealize Automation в качестве основы для клонов схем элементов.

2. Сценарий: создание спецификации развертывания для клонирования компьютеров Linux

С помощью vSphere Client можно создать стандартную спецификацию настройки для использования разработчиками архитектуры инфраструктуры как услуги vRealize Automation при создании клонов схем элементов для компьютеров Linux.

Сценарий: преобразование эталонного компьютера CentOS в шаблон для Rainpole

С помощью vSphere Client можно преобразовать существующий эталонный компьютер CentOS в шаблон vSphere, на который будут ссылаться разработчики архитектуры инфраструктуры как услуги vRealize Automation в качестве основы для клонов схем элементов.

Процедура

1. Войдите в эталонный компьютер в качестве привилегированного пользователя и подготовьте компьютер к преобразованию.

- а) Удалите правила устойчивости udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- б) Создайте уникальные идентификаторы для компьютеров, клонированных из этого шаблона.

```
/bin/sed -i '/^(HWADDR|UUID)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- в) Выключите компьютер.

```
shutdown -h now
```

2. Войдите в веб-клиент vSphere в качестве администратора.
3. Выберите вкладку **Параметры ВМ**.
4. Щелкните правой кнопкой мыши эталонный компьютер и выберите команду **Изменить параметры**.
5. В текстовом поле **Имя ВМ** введите имя **Rainpole_centos_63_x86**.

6. Даже если на эталонном компьютере установлена гостевая операционная система CentOS, выберите элемент **Red Hat Enterprise Linux 6 (64-разрядная)** в раскрывающемся меню **Версия гостевой ОС**.

Если выбрать CentOS, шаблон и спецификация настройки могут не работать должным образом.

7. В веб-клиенте vSphere щелкните правой кнопкой мыши эталонный компьютер **Rainpole_centos_63_x86** и последовательно выберите **Шаблон > Преобразовать в шаблон**.

Результаты

vCenter Server пометит эталонный компьютер Rainpole_centos_63_x86 как шаблон и отобразит задачу в области «Последние задачи».

Следующие шаги

Для предотвращения каких-либо конфликтов, которые могут возникнуть при развертывании нескольких виртуальных машин с одинаковыми настройками, можно создать общую спецификацию настройки, которую могут использовать вы и архитекторы Rainpole при создании схемы элементов для шаблонов Linux.

Сценарий: создание спецификации развертывания для клонирования компьютеров Linux

С помощью vSphere Client можно создать стандартную спецификацию настройки для использования разработчиками архитектуры инфраструктуры как услуги vRealize Automation при создании клонов схем элементов для компьютеров Linux.

Процедура

1. На домашней странице нажмите **Диспетчер спецификаций настройки**, чтобы открыть мастер.
2. Щелкните значок **Создать**.
3. Укажите свойства.
 - а) В раскрывающемся меню **Целевая операционная система ВМ** выберите пункт **Linux**.
 - б) В текстовом поле **Имя спецификации настройки** введите имя **Linux**.
 - в) В текстовом поле **Описание** введите **Клонирование Rainpole Linux с помощью vRealize Automation**.
 - г) Нажмите кнопку **Далее**.
4. Задайте имя компьютера.
 - а) Выберите элемент **Использовать имя виртуальной машины**.
 - б) В текстовом поле **Доменное имя** введите имя домена, в котором будут подготавливаться клонированные компьютеры.
 - в) Нажмите кнопку **Далее**.
5. Настройте параметры часового пояса.

6. Нажмите кнопку **Далее**.
7. Выберите элемент **Использовать стандартные параметры сети для гостевой операционной системы, включая активацию DHCP на всех сетевых интерфейсах**.
8. Следуйте инструкциям, чтобы ввести оставшуюся необходимую информацию.
9. На странице **Готово к завершению** просмотрите выбранные параметры и нажмите кнопку **Готово**.

Подготовка к процессу подготовки Программное обеспечение

Используйте Программное обеспечение для развертывания приложений и промежуточного программного обеспечения в рамках подготовки компьютеров vSphere, vCloud Director, vCloud Air и Amazon Web Services в vRealize Automation.

Программное обеспечение можно развернуть на компьютерах, если используемая схема элементов поддерживает Программное обеспечение и если до преобразования эталонных компьютеров в шаблоны, моментальные снимки и образы компьютеров на них установлены гостевой агент и агент начальной загрузки программного обеспечения.

Дополнительные сведения о назначении портов на предварительном этапе подготовки компьютеров см. PDF-файл *Эталонная архитектура* в [документации по продукту vRealize Automation](#).

Таблица 1-17. Методы подготовки, которые поддерживают Программное обеспечение

Тип компьютера	Подготовка
vSphere	Клон схемы элементов позволяет создать полную и независимую виртуальную машину на основе шаблона виртуальной машины vCenter Server. Если необходимо, чтобы шаблоны для клонирования поддерживали компоненты Программное обеспечение, установите гостевой агент и агент начальной загрузки программного обеспечения на эталонных компьютерах во время подготовки шаблона для клонирования. См. раздел Контрольный список для подготовки к процессу подготовки путем клонирования .
vSphere	Схема элементов связанного клона используется для подготовки компактной копии компьютера vSphere, созданной на основе моментального снимка. При этом для отслеживания отличий от родительского компьютера применяется цепочка дельта-дисков. Если нужно, чтобы схемы элементов связанных клонов поддерживали компоненты Программное обеспечение, прежде чем создать моментальный снимок, установите на компьютере гостевой агент и агент начальной загрузки программного обеспечения. Если компьютер моментального снимка клонирован из шаблона, который поддерживает Программное обеспечение, необходимые агенты уже установлены.
vCloud Director	Клон схемы элементов позволяет создать полную и независимую виртуальную машину на основе шаблона виртуальной машины vCenter Server. Если необходимо, чтобы шаблоны для клонирования поддерживали компоненты Программное обеспечение, установите гостевой агент и агент начальной загрузки программного обеспечения на эталонных компьютерах во время подготовки шаблона для клонирования. См. раздел Контрольный список для подготовки к процессу подготовки путем клонирования .

Таблица 1-17. Методы подготовки, которые поддерживают Программное обеспечение (продолжение)

Тип компьютера	Подготовка
vCloud Air	Клон схемы элементов позволяет создать полную и независимую виртуальную машину на основе шаблона виртуальной машины vCenter Server. Если необходимо, чтобы шаблоны для клонирования поддерживали компоненты Программное обеспечение, установите гостевой агент и агент начальной загрузки программного обеспечения на эталонных компьютерах во время подготовки шаблона для клонирования. См. раздел Контрольный список для подготовки к процессу подготовки путем клонирования .
Amazon Web Services	<p>Образ компьютера Amazon — это шаблон, который содержит данные конфигурации программного обеспечения, в том числе операционной системы. Если необходимо создать образ компьютера Amazon, поддерживающий Программное обеспечение, установите подключение к работающему экземпляру Amazon Web Services, который использует том EBS для корневого устройства. Установите гостевой агент и агент начальной загрузки программного обеспечения на эталонном компьютере, а затем создайте образ компьютера Amazon на основе экземпляра.</p> <p>Чтобы гостевой агент и агент начальной загрузки программного обеспечения Программное обеспечение работали на подготовленных компьютерах, необходимо настроить связь по схеме «сеть-VPC».</p> <p>Сведения о создании образов AMI на основе Amazon EBS см. в документации по Amazon Web Services.</p>
Microsoft Azure	Дополнительные сведения см. в документах Параметры компонента Программное обеспечение , Создание схемы элементов для Microsoft Azure и документации по Microsoft Azure.

Подготовка к процессу подготовки компьютеров с Программное обеспечение

Чтобы обеспечить поддержку компонентов Программное обеспечение, прежде чем преобразовать в шаблон для клонирования, создать образ компьютера Amazon или сделать моментальный снимок, на эталонном компьютере необходимо установить гостевой агент и агент начальной загрузки Программное обеспечение.

Подготовка эталонного компьютера Windows для поддержки Программное обеспечение

Используйте один сценарий для установки Java Runtime Environment, гостевого агента и агента начальной загрузки Программное обеспечение на эталонном компьютере Windows. С эталонного компьютера можно создать шаблон для клонирования, моментальный снимок или образ машины Amazon, поддерживающий компоненты Программное обеспечение.

В Программное обеспечение поддерживается создание сценариев с помощью Windows CMD и PowerShell 2.0.

Важно! Процесс запуска нельзя прерывать. Настройте виртуальную машину таким образом, чтобы ничто не приостанавливало процесс запуска виртуальной машины до появления запроса на вход в систему. Например, убедитесь, что никакие процессы или сценарии не запрашивают действий пользователя при запуске виртуальной машины.

Необходимые условия

- Определите или создайте эталонный компьютер Windows.

- Установите безопасное доверие между эталонным компьютером и узлом службы диспетчера инфраструктуры как услуги. См. раздел [Настройка в гостевом агенте доверия к серверу](#).
- Если планируется использовать удаленный доступ к компьютеру для устранения неполадок или по другим причинам, установите службы удаленных рабочих столов (RDS).
- Удалите артефакты конфигурации сети из файлов конфигурации сети.

Процедура

1. Войдите на эталонный сервер Windows в качестве администратора.
2. Откройте браузер на странице загрузки программного обеспечения на устройстве vRealize Automation.
`https://vrealize-automation-appliance-FQDN/software`
3. Сохраните ZIP-файл шаблона на сервере Windows.
`prepare_vra_template_windows.zip`
4. Извлеките содержимое ZIP-файла в папку и запустите пакетный файл.
`.\prepare_vra_template.bat`
5. Следуйте подсказкам.
6. После окончания завершите работу виртуальной машины Windows.

Результаты

Сценарий удаляет всех предыдущих гостей или агентов начальной загрузки Программное обеспечение и устанавливает поддерживаемые версии Java Runtime Environment, гостевого агента и агента начальной загрузки Программное обеспечение.

Следующие шаги

Преобразуйте эталонный компьютер в шаблон для клонирования, моментальный снимок или образ машины Amazon, каждый из которых поддерживает Программное обеспечение компоненты, а архитекторы инфраструктуры могут использовать их при создании схем элементов.

Подготовка эталонного компьютера Linux для поддержки Программное обеспечение

Используйте один сценарий для установки Java Runtime Environment, гостевого агента и агента начальной загрузки Программное обеспечение на эталонный компьютер Linux. С эталонного компьютера можно создать шаблон для клонирования, моментальный снимок или образ машины Amazon, поддерживающий компоненты Программное обеспечение.

Служба Программное обеспечение поддерживает сценарии Bash.

Важно! Процесс загрузки нельзя прерывать. Настройте виртуальную машину таким образом, чтобы ничто не приостанавливало процесс загрузки виртуальной машины до появления запроса на вход в систему. Например, убедитесь, что никакие процессы или сценарии не запрашивают действий пользователя при запуске виртуальной машины.

Необходимые условия

- Определение или создание эталонного компьютера Linux.
- Убедитесь, что следующие команды доступны в соответствии с системой Linux:
 - `yum` или `apt-get`
 - `wget` или `curl`
 - `python`
 - `dmidecode` в соответствии с требованиями поставщиков облачных служб
 - Общие требования, например `sed`, `awk`, `perl`, `chkconfig`, `unzip` и `grep`, в зависимости от дистрибутива Linux

Можно также использовать редактор, чтобы просмотреть загруженный сценарий `prepare_vra_template.sh`, который предоставляет используемые команды.

- Если планируется использовать удаленный доступ к компьютеру для устранения неисправностей или по другим причинам, установите OpenSSH.
- Удалите артефакты конфигурации сети из файлов конфигурации сети.

Процедура

1. Войдите на эталонный компьютер в качестве пользователя `root`.
2. Загрузите пакет шаблонов `tar.gz` с устройства vRealize Automation.

```
wget https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template_linux.tar.gz
```

Если в среде используются самозаверяющие сертификаты, может потребоваться параметр `--no-check-certificate`.

```
wget --no-check-certificate https://vrealize-automation-appliance-FQDN/software/download/prepare_vra_template_linux.tar.gz
```

3. Распакуйте пакет.


```
tar -xvf prepare_vra_template_linux.tar.gz
```
4. После распаковки найдите сценарий установщика и сделайте его исполняемым.

```
chmod +x prepare_vra_template.sh
```

5. Запустите сценарий установщика.

```
./prepare_vra_template.sh
```

Если требуется информация о неинтерактивных параметрах и ожидаемых значениях, см. раздел справки по сценарию.

```
./prepare_vra_template.sh --help
```

6. Следуйте подсказкам.

После успешного завершения установки появится подтверждение. Если появятся ошибки или журналы ошибок, устраните ошибки и повторно запустите сценарий.

7. После окончания завершите работу виртуальной машины Linux.**Результаты**

Сценарий удаляет всех предыдущих гостей или агентов начальной загрузки Программное обеспечение и устанавливает поддерживаемые версии Java Runtime Environment, гостевого агента и агента начальной загрузки Программное обеспечение.

Следующие шаги

В гипервизоре или поставщике облачных служб преобразуйте эталонный компьютер в шаблон для клонирования, моментальный снимок или образ машины Amazon, каждый из которых поддерживает Программное обеспечение компоненты, а архитекторы инфраструктуры могут использовать их при создании схем элементов.

Обновление существующих шаблонов виртуальных машин в vRealize Automation

При обновлении шаблонов, образов компьютера Amazon или моментальных снимков до последней версии агента начальной загрузки Программное обеспечение для Windows или при ручном обновлении до последней версии агента начальной загрузки Программное обеспечение для Linux вместо использования сценария `prepare_vra_template.sh`, нужно удалить все существующие версии и удалить все журналы.

Linux

Для эталонных компьютеров Linux запуск сценария `prepare_vra_template.sh` производит сброс агента и удаляет все журналы перед установкой. Тем не менее, для установки вручную необходимо войти на эталонный компьютер в качестве привилегированного пользователя и выполнить команду для сброса и удаления артефактов.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

Windows

Для эталонных компьютеров Windows нужно удалить существующий агент начальной загрузки Программное обеспечение и гостевой агент vRealize Automation 6.0 или более поздней версии и удалить все существующие файлы журналов выполнения. Чтобы удалить агента и артефакты, выполните команды в окне командной строки PowerShell.

```
c:\opt\vmware-appdirector\agent-bootstrap\appd_bootstrap_removal.bat
```

Подготовка шаблона vSphere для клонированного компьютера и схем элементов программных компонентов

Администратору vCenter Server может понадобиться подготовить шаблон vSphere, который разработчики vRealize Automation смогут использовать, например, для клонирования компьютеров Linux CentOS. Для того чтобы убедиться, что шаблон поддерживает схемы элементов с программными компонентами, прежде чем преобразовать эталонный компьютер в шаблон, нужно установить гостевой агент и агент начальной загрузки программного обеспечения.

Необходимые условия

- Определите или создайте эталонный компьютер Linux CentOS и установите на нем VMware Tools. Чтобы обеспечить подключение к Интернету, необходимо добавить по крайней мере один сетевой адаптер, если разработчики схем элементов не добавили эту функцию на уровне схемы. Для получения информации о создании виртуальных машин см. документацию по vSphere.
- Для преобразования виртуальной машины в шаблон требуется подключение к vCenter Server. Невозможно создавать шаблоны, если подключить клиент vSphere непосредственно к узлу vSphere ESXi.

Процедура

1. Сценарий: подготовка эталонного компьютера к настройке гостевого агента и поддержке программных компонентов

Чтобы шаблон поддерживал компоненты программного обеспечения, на эталонном компьютере нужно установить агент начальной загрузки программного обеспечения и необходимый для этого агента компонент — гостевой агент. При наличии агентов разработчики архитектуры vRealize Automation, использующие шаблон, могут включать в свои схемы элементов компоненты программного обеспечения.

2. Сценарий: преобразование эталонного компьютера CentOS в шаблон

После установки гостевого агента и агента начальной загрузки программного обеспечения на эталонном компьютере его необходимо преобразовать в шаблон, который архитекторы vRealize Automation могут использовать, чтобы создавать схемы элементов компьютеров для клонирования.

3. Сценарий: создание спецификации настройки для клонирования vSphere

Создание спецификации настройки для разработчиков схем элементов для использования с шаблоном cpb_centos_63_x84.

Результаты

Из эталонного компьютера был создан шаблон и спецификации настройки, которые могут использоваться разработчиками схем элементов для создания схем элементов vRealize Automation, чтобы клонировать компьютеры Linux CentOS. Так как на эталонном компьютере были установлены агент начальной загрузки Программное обеспечение и гостевой агент, разработчики могут использовать этот шаблон для создания сложных схем элементов каталога, включающих Программное обеспечение компоненты или другие настройки гостевого агента, например запуск сценариев или форматирование дисков. Так как был установлен пакет VMware Tools, разработчики и администраторы каталога могут предоставить пользователям возможность выполнять такие действия с компьютерами, как перенастройка, создание моментальных снимков и перезагрузка.

Следующие шаги

После настройки пользователей, групп и ресурсов vRealize Automation можно использовать шаблон и спецификации настройки для создания схемы элементов компьютера для клонирования. См. раздел [Настройка схемы элементов компьютера](#).

Сценарий: подготовка эталонного компьютера к настройке гостевого агента и поддержке программных компонентов

Чтобы шаблон поддерживал компоненты программного обеспечения, на эталонном компьютере нужно установить агент начальной загрузки программного обеспечения и необходимый для этого агента компонент — гостевой агент. При наличии агентов разработчики архитектуры vRealize Automation, использующие шаблон, могут включать в свои схемы элементов компоненты программного обеспечения.

Чтобы упростить процедуру, загрузите и запустите сценарий vRealize Automation, с помощью которого устанавливаются оба агента. Это избавит от необходимости в загрузке и установке отдельных пакетов.

В рамках сценария также выполняется подключение к экземпляру службы диспетчера и загружается сертификат SSL, который позволяет установить доверие между службой диспетчера и компьютерами, развернутыми с использованием шаблона. Обратите внимание: загрузка сертификата с помощью сценария менее безопасна, чем получение сертификата SSL из службы диспетчера вручную и установка этого сертификата на эталонном компьютере в расположении `/usr/share/gugent/cert.pem`.

Процедура

1. Откройте URL-адрес программного обеспечения устройства vRealize Automation в веб-браузере.
`https://vrealize-automation-appliance-FQDN/software`
2. В разделе установщиков программного обеспечения Linux Загрузите файл с расширением TAR.GZ.
`prepare_vra_template_linux.tar.gz`
3. Переместите TAR-файл во временный каталог эталонного компьютера Linux.

Для передачи файла можно запустить специальное средство, например WinSCP, или использовать любой другой привычный метод.

4. Войдите в командную строку эталонного компьютера Linux, используя учетные данные пользователя root.

Чтобы открыть терминал, можно запустить из vRealize Automation удаленную консоль на компьютере или использовать любой другой привычный способ.

5. Распакуйте TAR-файл из временного каталога.

```
gunzip prepare_vra_template_linux.tar.gz
```

6. Извлеките содержимое TAR-файла.

```
tar xvf prepare_vra_template_linux.tar
```

7. Перейдите в каталог сценария.

```
cd prepare_vra_template_linux
```

8. Запустите сценарий и следуйте отображаемым инструкциям.

```
./prepare_vra_template.sh
```

Если нужна неинтерактивная информация о параметрах и значениях, введите ./prepare_vra_template.sh --help.

Результаты

После завершения установки появится сообщение с подтверждением. Если появятся сообщения об ошибках или журналы ошибок, устраните проблемы и еще раз запустите сценарий.

Сценарий: преобразование эталонного компьютера CentOS в шаблон

После установки гостевого агента и агента начальной загрузки программного обеспечения на эталонном компьютере его необходимо преобразовать в шаблон, который архитекторы vRealize Automation могут использовать, чтобы создавать схемы элементов компьютеров для клонирования.

После преобразования эталонного компьютера в шаблон его можно редактировать и включать только после обратного преобразования шаблона в виртуальную машину.

Процедура

1. Войдите в эталонный компьютер в качестве привилегированного пользователя и подготовьте компьютер к преобразованию.

- а) Удалите правила устойчивости udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- б) Создайте уникальные идентификаторы для компьютеров, клонированных из этого шаблона.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- в) Если после установки агента начальной загрузки программного обеспечения вы перезагружали или перенастраивали эталонный компьютер, сбросьте агент.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- г) Выключите компьютер.

```
shutdown -h now
```

2. Войдите в веб-клиент vSphere в качестве администратора.
3. Щелкните правой кнопкой мыши эталонный компьютер и выберите команду **Изменить параметры**.
4. В текстовом поле **Имя ВМ** введите имя **cpb_centos_63_x84**.
5. Даже если на эталонном компьютере установлена гостевая операционная система CentOS, выберите элемент **Red Hat Enterprise Linux 6 (64-разрядная)** в раскрывающемся меню **Версия гостевой ОС**.

Если выбрать CentOS, шаблон и спецификация настройки могут не работать должным образом.

6. В веб-клиенте vSphere щелкните правой кнопкой мыши эталонный компьютер и последовательно выберите элементы **Шаблон > Преобразовать в шаблон**.

Результаты

vCenter Server пометит эталонный компьютер cpb_centos_63_x84 как шаблон и отобразит задачу в области «Последние задачи». Если среда уже находится vSphere под управлением vRealize Automation, шаблон будет обнаружен во время следующего автоматического сбора данных. Если ПО vRealize Automation еще не настроено, шаблон появится во время настройки.

Сценарий: создание спецификации настройки для клонирования vSphere

Создание спецификации настройки для разработчиков схем элементов для использования с шаблоном cpb_centos_63_x84.

Процедура

1. Войдите в веб-клиент vSphere в качестве администратора.
2. На домашней странице нажмите **Диспетчер спецификаций настройки**, чтобы открыть мастер.
3. Щелкните значок **Создать**.
4. Щелкните значок **Создать**.
5. Укажите свойства.
 - а) В раскрывающемся меню **Целевая операционная система ВМ** выберите пункт **Linux**.
 - б) В текстовом поле **Имя спецификации настройки** введите имя **Customspecs**.
 - в) В текстовом поле **Описание** введите **Клонирование cpb_centos_63_x84 с помощью vRealize Automation**.
 - г) Нажмите кнопку **Далее**.

6. Задайте имя компьютера.
 - а) Выберите элемент **Использовать имя виртуальной машины**.
 - б) В текстовом поле **Доменное имя** введите имя домена, в котором будут подготавливаться клонированные компьютеры.
 - в) Нажмите кнопку **Далее**.
7. Настройте параметры часового пояса.
8. Нажмите кнопку **Далее**.
9. Выберите элемент **Использовать стандартные параметры сети для гостевой операционной системы, включая активацию DHCP на всех сетевых интерфейсах**.

Администраторы структуры и архитекторы инфраструктуры настраивают параметры сети для подготовленного компьютера, создавая и используя профили сетей в vRealize Automation.
10. Следуйте инструкциям, чтобы ввести оставшуюся необходимую информацию.
11. На странице **Готово к завершению** просмотрите выбранные параметры и нажмите кнопку **Готово**.

Результаты

Сценарий: подготовка к импорту схемы элементов образца приложения Dukes Bank для vSphere

В качестве администратора vCenter Server вам необходимо подготовить шаблон vSphere CentOS 6.x Linux и спецификацию настройки, которые затем можно использовать для подготовки образца приложения vRealize Automation Dukes Bank.

Чтобы шаблон поддерживал программные компоненты образца приложения, необходимо установить гостевой агент и агент начальной загрузки программного обеспечения в эталонный компьютер Linux, прежде чем преобразовать его в шаблон и создать спецификацию настройки. Деактивируйте SELinux на эталонном компьютере и убедитесь, что шаблон поддерживает реализацию MySQL, используемую в образце приложения Dukes Bank.

Необходимые условия

- Выберите или создайте эталонный компьютер CentOS 6.x Linux и установите на нем VMware Tools. Для получения информации о создании виртуальных машин см. документацию по vSphere.

- Для преобразования виртуальной машины в шаблон требуется подключение к vCenter Server. Невозможно создавать шаблоны, если подключить клиент vSphere непосредственно к узлу vSphere ESXi.

Процедура

1. Сценарий: подготовка эталонного компьютера для образца приложения Dukes Bank vSphere

Чтобы шаблон поддерживал образец приложения Dukes Bank, на эталонном компьютере нужно установить гостевой агент и агент начальной загрузки программного обеспечения, чтобы решение vRealize Automation могло подготовить программные компоненты. Чтобы упростить процесс, вместо загрузки и установки пакетов по отдельности загрузите и запустите сценарий vRealize Automation, по которому гостевой агент и агент начальной загрузки программного обеспечения устанавливаются одновременно.

2. Сценарий: преобразование эталонного компьютера в шаблон для приложения Dukes Bank vSphere

После установки гостевого агента и агента начальной загрузки программного обеспечения на эталонном компьютере деактивируйте SELinux и убедитесь, что шаблон поддерживает реализацию MySQL, используемую в образце приложения Dukes Bank. Эталонный компьютер превращается в шаблон, который можно использовать для подготовки образца приложения Dukes Bank vSphere.

3. Сценарий: создание спецификации настройки для клонирования компьютеров образца приложения Dukes Bank vSphere

Предусматривает создание спецификации настройки для использования с шаблоном компьютера Dukes Bank.

Результаты

Теперь на основе эталонного компьютера, который поддерживает образец приложения Dukes Bank vRealize Automation, созданы шаблон и спецификация настройки.

Сценарий: подготовка эталонного компьютера для образца приложения Dukes Bank vSphere

Чтобы шаблон поддерживал образец приложения Dukes Bank, на эталонном компьютере нужно установить гостевой агент и агент начальной загрузки программного обеспечения, чтобы решение vRealize Automation могло подготовить программные компоненты. Чтобы упростить процесс, вместо загрузки и установки пакетов по отдельности загрузите и запустите сценарий vRealize Automation, по которому гостевой агент и агент начальной загрузки программного обеспечения устанавливаются одновременно.

Процедура

1. Войдите в эталонный компьютер в качестве привилегированного пользователя.
2. Загрузите сценарий установки с устройства vRealize Automation.

```
wget https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

Если в вашей среде используются самозаверяющие сертификаты, возможно, придется использовать параметр `wget --no-check-certificate`. Пример:

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn/software/download/prepare_vra_template.sh
```

3. Сделайте сценарий `prepare_vra_template.sh` исполняемым.

```
chmod +x prepare_vra_template.sh
```

4. Выполните сценарий установщика `prepare_vra_template.sh`.

```
./prepare_vra_template.sh
```

Для получения информации о неинтерактивных параметрах и ожидаемых значениях можно запустить команду вывода справки `./prepare_vra_template.sh --help`.

5. Следуйте указаниям, чтобы завершить установку.

После успешного завершения установки отобразится сообщение с подтверждением. При появлении сообщения об ошибке и журналов в консоли устраните ошибки и выполните сценарий установщика снова.

Результаты

Вы установили агент начальной загрузки программного обеспечения и гостевой агент, необходимый для его установки, чтобы убедиться, что образец приложения Dukes Bank успешно подготавливает программные компоненты. В рамках сценария выполнено подключение к экземпляру службы диспетчера и загружен сертификат SSL, чтобы установить доверие между службой диспетчера и компьютерами, развернутыми с использованием вашего шаблона. Это менее безопасный подход, чем при получении сертификата SSL службы диспетчера и установке его вручную на эталонном компьютере в каталоге `/usr/share/gugent/cert.pem`. И если вам важна безопасность, этот сертификат можно заменить вручную.

Сценарий: преобразование эталонного компьютера в шаблон для приложения Dukes Bank vSphere

После установки гостевого агента и агента начальной загрузки программного обеспечения на эталонном компьютере деактивируйте SELinux и убедитесь, что шаблон поддерживает реализацию MySQL, используемую в образце приложения Dukes Bank. Эталонный компьютер превращается в шаблон, который можно использовать для подготовки образца приложения Dukes Bank vSphere.

После преобразования эталонного компьютера в шаблон его можно редактировать и включать только после обратного преобразования шаблона в виртуальную машину.

Процедура

1. Войдите в эталонный компьютер в качестве привилегированного пользователя.

- a) Измените файл `/etc/selinux/config`, чтобы деактивировать SELinux.

```
SELINUX=disabled
```

Если не деактивировать SELinux, программный компонент MySQL образца приложения Dukes Bank может работать неправильно.

- b) Удалите правила устойчивости udev.

```
/bin/rm -f /etc/udev/rules.d/70*
```

- v) Создайте уникальные идентификаторы для компьютеров, клонированных из этого шаблона.

```
/bin/sed -i '/^\(HWADDR\|UUID\)=/d'  
/etc/sysconfig/network-scripts/ifcfg-eth0
```

- г) Если после установки агента начальной загрузки программного обеспечения вы перезагружали или перенастраивали эталонный компьютер, сбросьте агент.

```
/opt/vmware-appdirector/agent-bootstrap/agent_reset.sh
```

- д) Выключите компьютер.

```
shutdown -h now
```

2. Войдите в веб-клиент vSphere в качестве администратора.
3. Щелкните правой кнопкой мыши эталонный компьютер и выберите команду **Изменить параметры**.
4. В текстовом поле **Имя ВМ** введите имя **dukes_bank_template**.
5. Даже если на эталонном компьютере установлена гостевая операционная система CentOS, выберите элемент **Red Hat Enterprise Linux 6 (64-разрядная)** в раскрывающемся меню **Версия гостевой ОС**.

Если выбрать CentOS, шаблон и спецификация настройки могут не работать должным образом.

6. Нажмите кнопку **ОК**.
7. В веб-клиенте vSphere щелкните правой кнопкой мыши эталонный компьютер и последовательно выберите элементы **Шаблон > Преобразовать в шаблон**.

Результаты

vCenter Server пометит эталонный компьютер как шаблон и отобразит задачу в области «Последние задачи». Если среда уже находится vSphere под управлением vRealize Automation, шаблон будет обнаружен во время следующего автоматического сбора данных. Если ПО vRealize Automation еще не настроено, шаблон появится во время настройки.

Сценарий: создание спецификации настройки для клонирования компьютеров образа приложения Dukes Bank vSphere

Предусматривает создание спецификации настройки для использования с шаблоном компьютера Dukes Bank.

Процедура

1. Войдите в веб-клиент vSphere в качестве администратора.
2. На домашней странице нажмите **Диспетчер спецификаций настройки**, чтобы открыть мастер.
3. Щелкните значок **Создать**.
4. Укажите свойства.
 - а) В раскрывающемся меню **Целевая операционная система ВМ** выберите пункт **Linux**.
 - б) В текстовом поле **Имя спецификации настройки** введите имя **Customspecs_sample**.
 - в) В текстовом поле **Описание** введите **Спецификация настройки Dukes Bank**.
 - г) Нажмите кнопку **Далее**.
5. Задайте имя компьютера.
 - а) Выберите элемент **Использовать имя виртуальной машины**.
 - б) В текстовом окне **Имя домена** введите имя домена, на котором нужно подготовить образец приложения Dukes Bank.
 - в) Нажмите кнопку **Далее**.
6. Настройте параметры часового пояса.
7. Нажмите кнопку **Далее**.
8. Выберите элемент **Использовать стандартные параметры сети для гостевой операционной системы, включая активацию DHCP на всех сетевых интерфейсах**.

Администраторы структуры и архитекторы инфраструктуры настраивают параметры сети для подготовленного компьютера, создавая и используя профили сетей в vRealize Automation.
9. Следуйте инструкциям, чтобы ввести оставшуюся необходимую информацию.
10. На странице **Готово к завершению** просмотрите выбранные параметры и нажмите кнопку **Готово**.

Результаты

Теперь созданный шаблон и настройки спецификации можно использовать для подготовки образа приложения Dukes Bank.

Следующие шаги

1. Создайте внешний профиль сети, задав шлюз и диапазон IP-адресов. См. [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#).

2. Сопоставьте профиль внешней сети с резервированием vSphere. См. [Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer](#). Образец приложения нельзя успешно подготовить без внешнего профиля сети.
3. Импортируйте образец приложения Dukes Bank в свою среду. См. [Сценарий: импорт образца приложения Dukes Bank для vSphere и его настройка для среды](#).

Приготовление арендатора и ресурса для подготовки схемы элементов

2

Можно настроить несколько сред арендаторов, задав для каждой из них свои группы пользователей и уникальные права доступа к ресурсам, для управления которыми используется vRealize Automation.

В эту главу входят следующие разделы:

- [Настройка параметров арендатора](#)
- [Настройка ресурсов](#)
- [Параметры пользователя для уведомлений и делегатов](#)

Настройка параметров арендатора

Администраторы арендатора настраивают параметры арендатора, например проверку подлинности пользователей, и управляют ролями пользователей и бизнес-группами. Системные администраторы и администраторы арендатора настраивают параметры, например почтовые серверы, для обработки уведомлений и фирменной символики для консоли vRealize Automation.

Чтобы получить общее представление о последовательности шагов, которые необходимо выполнить для настройки параметров арендатора, воспользуйтесь контрольным списком для настройки параметров арендатора.

Таблица 2-1. Контрольный список для настройки параметров арендатора

Задача	Роль vRealize Automation	Сведения
<input type="checkbox"/> Создает учетные записи локальных пользователей и назначает администратора арендатора.	Системный администратор	Настройка доступа к арендатору по умолчанию
<input type="checkbox"/> Настройте управление каталогами, чтобы задать параметры управления удостоверениями арендаторов и доступом.	Администратор арендатора	Выбор вариантов настройки службы управления каталогами
<input type="checkbox"/> Создает бизнес-группы и настраиваемые группы, а также предоставляет пользователям права доступа к консоли vRealize Automation.	Администратор арендатора	Настройка групп и ролей пользователей

Таблица 2-1. Контрольный список для настройки параметров арендатора (продолжение)

Задача	Роль vRealize Automation	Сведения
<input type="checkbox"/> (Необязательно). Создайте дополнительные арендаторы, чтобы пользователи могли получать доступ к соответствующим приложениям и ресурсам, необходимым для выполнения своих рабочих заданий.	Системный администратор	Создание дополнительных арендаторов
<input type="checkbox"/> (Необязательно). Настройте фирменную символику для страниц входа арендатора и приложения в консоли vRealize Automation.	<ul style="list-style-type: none"> ■ Системный администратор ■ Администратор арендатора 	Настройка пользовательской фирменной символики
<input type="checkbox"/> (Необязательно). В vRealize Automation можно настроить отправку уведомлений пользователям при наступлении определенных событий.	<ul style="list-style-type: none"> ■ Системный администратор ■ Администратор арендатора 	Контрольный список для настройки уведомлений
<input type="checkbox"/> (Необязательно). Настройте vRealize Orchestrator для поддержки Все как услуга и других возможностей расширения	<ul style="list-style-type: none"> ■ Системный администратор ■ Администратор арендатора 	Настройка vRealize Orchestrator
<input type="checkbox"/> (Необязательно). Создайте настраиваемые файлы протокола удаленного рабочего стола. Эти файлы архитекторы инфраструктуры как услуги используют в схемах элементов для настройки параметров RDP.	Системный администратор	Создание настраиваемого RDP-файла для поддержки подключений RDP для подготовленных компьютеров
<input type="checkbox"/> (Необязательно). Определите расположение центра обработки данных, который администраторы структуры и архитекторы инфраструктуры как услуги смогут использовать, чтобы разрешить пользователям выбирать подходящее место для подготовки при отправке запроса компьютера.	Системный администратор	Примеры по добавлению расположений в центре обработки данных см. в разделе Сценарий: добавление данных о расположении центра обработки данных при развертываниях в нескольких регионах .

Выбор вариантов настройки службы управления каталогами

Для настройки канала связи с Active Directory в соответствии с требованиями к проверке подлинности пользователей можно использовать службу управления каталогами vRealize Automation.

Служба управления каталогами позволяет реализовать различные настраиваемые варианты проверки подлинности пользователей.

Таблица 2-2. Выбор вариантов настройки службы управления каталогами

Вариант настройки	Процедура
Настройте канал связи с Active Directory	<ol style="list-style-type: none"> 1 Настройте канал связи с Active Directory См. раздел Настройка ссылки Active Directory по LDAP/IWA. 2 Если настроено обеспечение высокой доступности для vRealize Automation, см. раздел Настройка службы управления каталогами для обеспечения высокой доступности.
(Необязательно). Повышение безопасности канала связи с каталогом при использовании идентификатора пользователя и пароля путем настройки двунаправленной интеграции со службами федерации Active Directory.	Настройка двунаправленных отношений доверия между vRealize Automation и Active Directory
(Необязательно). Добавление пользователей и групп к существующему каналу связи с Active Directory.	Добавление пользователей или групп к подключению Active Directory.
(Необязательно). Редактирование политики по умолчанию для применения настраиваемых правил для канала связи с Active Directory.	Управление политикой доступа пользователей.
(Необязательно). Настройка сетевых диапазонов для ограничения IP-адресов, через которые пользователи могут входить в систему, управлять ограничениями на вход в систему (время ожидания, количество попыток входа в систему перед блокировкой).	Добавление или изменение сетевого диапазона.

Общие сведения об управлении каталогами

Администраторы арендатора могут настраивать функции управления учетными данными арендатора и контроля доступа с помощью параметров функции управления каталогами на консоли приложения vRealize Automation.

На вкладке **Администрирование > Управление каталогами** можно управлять следующими параметрами.

Таблица 2-3. Параметры управления каталогами

Параметр	Описание
Каталоги	<p>На странице «Каталоги» можно создавать и управлять каналами связи с Active Directory для поддержки процесса проверки подлинности и авторизации пользователей арендатора в vRealize Automation. Необходимо создать один или несколько каталогов, а затем синхронизировать их со своим развертыванием Active Directory. На этой странице отображаются количество групп и пользователей, синхронизируемых с каталогом, и время последней операции синхронизации. Для запуска вручную синхронизации каталогов щелкните Синхронизация.</p> <p>См. раздел Использование функции управления каталогами для создания ссылки на Active Directory.</p> <p>Если щелкнуть каталог и затем нажать кнопку Параметры синхронизации, можно отредактировать параметры синхронизации, перейти на страницу «Поставщики удостоверений» и просмотреть журнал синхронизации.</p> <p>На странице параметров синхронизации каталогов можно указать частоту синхронизации, просмотреть список доменов, связанных с этим каталогом, изменить сопоставленный список атрибутов, обновить список пользователей и групп, для которого выполняется синхронизация, а также задать параметры защиты.</p>
Соединители	<p>На странице «Соединители» приведен список развернутых соединителей для корпоративной сети. Соединитель синхронизирует пользовательские и групповые данные между Active Directory и службой управления каталогами и проверяет подлинность пользователей в службе при использовании в качестве поставщика удостоверений. Каждое устройство vRealize Automation содержит соединитель по умолчанию. См. раздел Управление соединителями и кластерами соединителей.</p>
Атрибуты пользователя	<p>На странице «Атрибуты пользователя» отображаются атрибуты пользователя по умолчанию, которые синхронизируются в каталоге. Здесь можно добавлять другие атрибуты, которые можно сопоставлять с атрибутами Active Directory. См. раздел Выбор атрибутов для синхронизации с каталогом.</p>
Сетевые диапазоны	<p>На этой странице отображаются сетевые диапазоны, которые настроены для вашей системы. Сетевой диапазон должен быть настроен, чтобы пользователи могли получать доступ через указанные IP-адреса. Можно добавлять дополнительные сетевые диапазоны, а также редактировать существующие диапазоны. См. раздел Добавление или изменение сетевого диапазона.</p>
Поставщики удостоверений	<p>На странице «Поставщики удостоверений» отображаются поставщики удостоверений, доступные в вашей системе. Системы vRealize Automation содержат соединитель, который служит поставщиком удостоверений по умолчанию и удовлетворяет многие потребности пользователей. Можно добавить экземпляры стороннего поставщика удостоверений или иметь комбинацию поставщиков обоих типов.</p> <p>См. раздел Настройка подключения стороннего поставщика удостоверений.</p>
Политики	<p>На странице «Политики» отображаются политика доступа по умолчанию и любые другие политики доступа к веб-приложениям, созданные вами. Политики представляют собой набор правил, указывающих критерии, которым должны соответствовать пользователи, чтобы получать доступ к порталам приложений или запускать разрешенные веб-приложения. Политика по умолчанию должна подходить для большинства развертываний vRealize Automation, но, при необходимости, ее можно редактировать. См. раздел Управление политикой доступа пользователей.</p>

Важные понятия, связанные с Active Directory

Существует несколько понятий, связанных с Active Directory, которые важны для понимания того, как Directories Management интегрируется со средой Active Directory.

Соединитель

Компонент службы соединитель выполняет следующие функции.

- Синхронизация данных о пользователях и группах между Active Directory и службой.
- Проверка подлинности пользователей в службе при использовании в качестве поставщика удостоверений.

соединитель является поставщиком удостоверений по умолчанию. Список поддерживаемых соединитель способов проверки подлинности см. в разделе *Администрирование VMware Identity Manager*. Также можно использовать сторонних поставщиков удостоверений, которые поддерживают протокол SAML 2.0. Используйте стороннего поставщика удостоверений для типов проверки подлинности, которые не поддерживаются соединитель, а также для поддерживаемых соединитель типов проверки подлинности, если согласно политике безопасности организации сторонний поставщик удостоверений является предпочтительным.

Примечание Даже при использовании сторонних поставщиков удостоверений необходимо настроить соединитель для синхронизации данных о пользователях и группах.

Каталог

Служба Directories Management основана на собственной концепции каталога, согласно которой для определения пользователей и групп используются атрибуты и параметры Active Directory. Необходимо создать один или несколько каталогов, а затем синхронизировать эти каталоги в среде Active Directory. В службе можно создать следующие типы каталогов.

- Active Directory через LDAP. Этот тип каталога создается, если планируется подключение к среде Active Directory с одним доменом. В случае использования типа каталога Active Directory через LDAP соединитель связывается с Active Directory, используя простую привязку проверки подлинности.
- Active Directory, встроенная проверка подлинности Windows. Этот тип каталога создается, если планируется подключение к среде Active Directory с несколькими доменами или несколькими лесами. соединитель связывается с Active Directory, используя встроенную проверку подлинности Windows.

Тип и количество создаваемых каталогов варьируется в зависимости от среды Active Directory (один домен или нескольких доменов) и от вида используемых отношений доверия между доменами. В большинстве сред создается один каталог.

Служба не имеет прямого доступа к Active Directory. Только соединитель имеет прямой доступ к Active Directory. Таким образом, каждый каталог, созданный в службе, связывается с экземпляром соединитель.

Рабочий процесс

При связывании каталога с экземпляром соединительсоединитель создает раздел для связанного каталога, который называется «рабочий процесс». Экземпляр соединитель может иметь несколько рабочих процессов, связанных с ним. Каждый рабочий процесс выступает в качестве поставщика удостоверений. Для каждого рабочего процесса определяются и настраиваются способы проверки подлинности.

соединитель синхронизирует данные о пользователях и группах между Active Directory и службой с помощью одного или нескольких рабочих процессов.

Для типа «встроенная проверка подлинности Windows» может быть только один рабочий процесс на одном экземпляре соединитель.

Среды Active Directory

Службу можно интегрировать в среду Active Directory, которая состоит из одного домена Active Directory, нескольких доменов в одном лесу Active Directory или нескольких доменов в нескольких лесах Active Directory.

Среда с одним доменом Active Directory

Одиночное развертывание Active Directory позволяет синхронизировать пользователей и группы из одного домена Active Directory.

См. [Настройка ссылки Active Directory по LDAP/IWA](#). Для этой среды при добавлении каталога в службу выберите параметр «Active Directory по LDAP».

Среда Active Directory в нескольких доменах и одном лесу

Развертывание Active Directory в нескольких доменах и одном лесу позволяет синхронизировать пользователей и группы из нескольких доменов Active Directory в пределах одного леса.

Для этой среды Active Directory службу можно настроить как одиночную службу Active Directory, тип каталога «Встроенная проверка подлинности Windows», а также как тип каталога «Active Directory по LDAP», настроенный с функциями глобального каталога.

- Рекомендуемый вариант — создание одной службы Active Directory с типом каталога «Встроенная проверка подлинности Windows».

См. [Настройка ссылки Active Directory по LDAP/IWA](#). При добавлении каталога для этой среды выберите параметр «Active Directory (встроенная проверка подлинности Windows)».

Среда Active Directory в нескольких лесах с отношениями доверия

Развертывание Active Directory в нескольких лесах с отношениями доверия позволяет синхронизировать пользователей и группы из нескольких доменов Active Directory в нескольких лесах, где между доменами существуют двусторонние отношения доверия.

См. [Настройка ссылки Active Directory по LDAP/IWA](#). При добавлении каталога для этой среды выберите параметр «Active Directory (встроенная проверка подлинности Windows)».

Среда Active Directory в нескольких лесах без отношений доверия

Развертывание Active Directory в нескольких лесах без отношений доверия позволяет синхронизировать пользователей и группы из нескольких доменов Active Directory в нескольких лесах, где между доменами нет двусторонних отношений доверия. В этой среде вы создаете в службе несколько каталогов, по одному каталогу для каждого леса.

См. [Настройка ссылки Active Directory по LDAP/IWA](#). Тип каталогов, которые вы создаете в службе, зависит от леса. Для лесов с несколькими доменами выберите параметр «Active Directory (встроенная проверка подлинности Windows)». Для леса с одним доменом выберите параметр «Active Directory по LDAP».

Использование функции управления каталогами для создания ссылки на Active Directory

После создания арендаторов vRealize Automation необходимо войти в системную консоль в качестве администратора арендатора и создать ссылку на Active Directory для поддержки проверки подлинности пользователей.

Эти три параметра коммуникационного протокола Active Directory доступны при настройке подключения к Active Directory с использованием функции управления каталогами.

- «Active Directory по LDAP» — протокол «Active Directory по LDAP» по умолчанию поддерживает функцию поиска места расположения службы DNS.
- Active Directory (встроенная проверка подлинности Windows) — с помощью Active Directory (встроенная проверка подлинности Windows) настраивается домен, к которому нужно присоединиться. Active Directory по LDAP подходит для развертываний отдельных доменов. Используйте Active Directory (встроенная проверка подлинности Windows) для всех развертываний с несколькими доменами и несколькими лесами.
- OpenLDAP — можно использовать версию LDAP с открытым кодом для поддержки проверки подлинности пользователей с помощью функции управления каталогами.

После выбора коммуникационного протокола и настройки ссылки на Active Directory можно указать, какие домены должны использоваться при данной конфигурации Active Directory, а затем выбрать пользователей и группы для синхронизации с заданной конфигурацией.

Настройка ссылки Active Directory по LDAP/IWA

Вы можете настроить ссылку Active Directory по LDAP/IWA для выполнения проверки подлинности пользователя с помощью функции Directories Management путем определения ссылки на Active Directory для выполнения проверки подлинности пользователей всех арендаторов, а также выбора пользователей и групп для синхронизации с каталогом Directories Management.

Сведения и инструкции относительно использования OpenLDAP со службой управления каталогами см. в разделе [Настройка подключения к каталогу OpenLDAP](#).

Для Active Directory (встроенная проверка подлинности Windows), если у вас есть настроенная служба Active Directory в нескольких лесах и локальная группа домена содержит участников из доменов в различных лесах, убедитесь, что пользователь привязки добавлен в группу администраторов домена, в котором находится локальная группа домена. Если этого не сделать, данных участников не будет в локальной группе домена.

Примечание Сначала настройте каталоги Active Directory по IWA для арендатора по умолчанию, а затем добавьте их к другим арендаторам.

Необходимые условия

- На странице «Атрибуты пользователя» выберите обязательные атрибуты по умолчанию и добавьте дополнительные атрибуты. См. раздел [Выбор атрибутов для синхронизации с каталогом](#).

- Список групп и пользователей Active Directory, которые нужно синхронизировать из Active Directory.
- Если для Active Directory необходим доступ по протоколу SSL или STARTTLS, требуется сертификат корневого центра сертификации контроллера домена Active Directory.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Щелкните элемент **Добавить каталог** и выберите пункт **Добавить Active Directory по LDAP/IWA**.
3. На странице «Добавить каталог» укажите IP-адрес для сервера Active Directory в текстовом поле **Имя каталога**.
4. Выберите соответствующий коммуникационный протокол Active Directory с помощью переключателей под текстовым полем **Имя каталога**.

Параметр	Описание
проверка подлинности Windows	Выберите Active Directory (встроенная проверка подлинности Windows) . Для встроенной проверки подлинности Windows в Active Directory необходимо указать такую информацию, как адрес и пароль UPN пользователя привязки домена.
LDAP	Выберите Active Directory по LDAP . Для подключения к Active Directory по протоколу LDAP необходимо указать такую информацию, как базовое имя домена, имя домена привязки и пароль имени домена привязки.

5. Настройте соединитель, синхронизирующий пользователей Active Directory с каталогом VMware Directories Management в разделе «Синхронизация каталогов и проверка подлинности».

Параметр	Описание
Соединитель синхронизации	<p>Выберите соответствующий соединитель для использования в системе. Каждое устройство vRealize Automation содержит соединитель по умолчанию. Если вам требуется помощь при выборе соединителя, обратитесь к системному администратору.</p>
Проверка подлинности	<p>Нажмите соответствующий переключатель, чтобы обозначить, выполняет ли выбранный соединитель проверку подлинности.</p> <p>При использовании Active Directory (встроенной проверки подлинности Windows) со сторонним поставщиком удостоверений для проверки подлинности пользователей щелкните Нет. После настройки подключения Active Directory для синхронизации пользователей и групп перейдите на страницу «Поставщики удостоверений», чтобы добавить стороннего поставщика удостоверений для проверки подлинности.</p> <p>Для получения дополнительных сведений об использовании адаптеров проверки подлинности, например PasswordIpddAdapter, SecuriDAdapter и RadiusAuthAdapter, см. <i>Руководство по администрированию VMware Identity Manager</i>.</p>
Атрибут поиска каталогов	<p>Выберите соответствующий атрибут учетной записи, который содержит имя пользователя. VMware рекомендует использовать атрибут sAMAccount вместо атрибута userPrincipalName. Если для операций синхронизации используется атрибут userPrincipalName, то при интеграции со сторонним программным обеспечением, для которой требуется указать имя пользователя, могут возникать ошибки.</p> <p>Примечание Если при работе с глобальным каталогом, который указан путем установки флажка Этот каталог содержит глобальный каталог в области «Расположение сервера», выбран атрибут sAMAccountName, то пользователи не смогут выполнить вход в систему.</p>

6. Введите соответствующую информацию в текстовом поле «Расположение сервера», если выбран протокол Active Directory по LDAP, или в текстовом поле «Сведения о присоединении к домену», если выбран протокол Active Directory (встроенная проверка подлинности Windows).

Параметр	Описание
Поле «Расположение сервера» отображается, когда выбран параметр «Active Directory по LDAP»	<ul style="list-style-type: none"> ■ Если необходимо использовать функцию поиска места расположения службы DNS для размещения доменов Active Directory, установите флажок Этот каталог поддерживает расположение службы DNS. <p>Примечание При выборе этого варианта нельзя изменить назначение порта 636.</p> <p>Вместе с каталогом создается файл <code>domain_krb.properties</code>, в который автоматически вносится список контроллеров домена. См. раздел Выбор контроллеров домена.</p> <p>Если для Active Directory требуется шифрование STARTTLS, в разделе «Сертификаты» установите флажок Все подключения объектов, входящих в данный каталог, выполняются с использованием протокола STARTTLS, а также скопируйте и вставьте сертификат корневого центра сертификации Active Directory в поле Сертификат SSL.</p> <ul style="list-style-type: none"> ■ Если указанная служба Active Directory не использует функцию поиска места расположения службы DNS, снимите флажок рядом с полем Этот каталог поддерживает расположение службы DNS в поле «Расположение сервера» и введите имя узла сервера Active Directory, а также номер порта в соответствующих текстовых полях. <p>Установите флажок Этот каталог содержит глобальный каталог, если связанный экземпляр Active Directory использует глобальный каталог. Глобальный каталог содержит представление всех объектов в каждом из доменов в лесу доменов Active Directory.</p> <p>Сведения о том, как настроить каталог в качестве глобального каталога, см. в разделе «Среда Active Directory с несколькими доменами и одним лесом» в Среды Active Directory.</p> <p>Если для Active Directory требуется доступ по SSL, установите флажок Этому каталогу требуются все подключения для использования SSL под заголовком «Сертификаты» и предоставьте сертификат SSL для Active Directory.</p> <p>При выборе этого варианта порт 636 используется автоматически и его нельзя изменить.</p> <p>Убедитесь, что сертификат находится в формате PEM и содержит строки BEGIN CERTIFICATE и END CERTIFICATE.</p>
Поле «Сведения о присоединении к домену» отображается, когда выбран параметр «Active Directory (встроенная проверка подлинности Windows)»	<p>Введите соответствующие учетные данные в текстовых полях Имя домена, Имя администратора домена и Пароль администратора домена.</p> <p>Если для Active Directory требуется шифрование STARTTLS, в разделе «Сертификаты» установите флажок Все подключения объектов, входящих в данный каталог, выполняются с использованием протокола STARTTLS, а также скопируйте и вставьте сертификат корневого центра сертификации Active Directory в поле Сертификат SSL.</p> <p>Убедитесь, что сертификат находится в формате PEM и содержит строки BEGIN CERTIFICATE и END CERTIFICATE.</p>

Параметр	Описание
	Если в каталоге используется несколько доменов, добавьте сертификаты корневого центра сертификации для всех доменов по отдельности.
	Примечание Если для Active Directory требуется протокол STARTTLS, а сертификат не предоставлен, создать каталог невозможно.

7. В разделе «Сведения о привязке пользователя» введите соответствующие учетные данные, чтобы упростить синхронизацию каталогов.

Для Active Directory по LDAP:

Параметр	Описание
Базовое имя домена	Введите базовое различающееся имя для поиска пользователя. Например, cn=users,dc=corp,dc=local .
Имя домена привязки	Введите различающееся имя для привязки. Например, cn=fritz infra,cn=users,dc=corp,dc=local

Для Active Directory (встроенная проверка подлинности Windows):

Параметр	Описание
Имя UPN пользователя привязки домена	Введите имя участника-пользователя для пользователя, который может выполнить проверку подлинности домена. Например, UserName@example.com .
Пароль имени домена привязки	Введите пароль пользователя привязки.

8. Щелкните **Проверить подключение**, чтобы проверить подключение к настроенному каталогу.

Эта кнопка не появляется, если выбрана опция «Active Directory (встроенная проверка подлинности Windows)».

9. Нажмите **Сохранить и Далее**.

Появляется страница «Выбрать домены» со списком доменов.

10. Просмотрите и обновите домены, перечисленные для подключения Active Directory.

- Для Active Directory (встроенная проверка подлинности Windows) выберите домены, которые необходимо связать с этим подключением к Active Directory.
- Доступный домен для Active Directory по LDAP отмечен галочкой.


Примечание В случае добавления доверенного домена после создания каталога новый доверенный домен служба автоматически не обнаруживает. Чтобы служба смогла обнаружить домен, соединитель соединитель должен отсоединиться от домена, а затем снова присоединиться к нему. После того как соединитель снова присоединится к домену, доверенный домен появится в списке.

11. Щелкните **Далее**.

12. Убедитесь, что имена атрибутов каталога Directories Management сопоставляются с нужными атрибутами Active Directory.

Если имена атрибутов каталога отображаются неправильно, выберите нужный атрибут Active Directory в раскрывающемся меню.

13. Нажмите кнопку **Далее**.

14. Щелкните , чтобы выбрать группы, которые должны синхронизироваться из Active Directory с каталогом.

Если при добавлении группы из Active Directory ее участников нет в списке пользователей, они будут добавлены. При синхронизации группы все пользователи, для которых группа «Пользователи домена» в Active Directory не является основной, не синхронизируются.

Примечание Система проверки подлинности пользователей Directories Management импортирует данные из Active Directory при добавлении групп и пользователей, при этом быстродействие системы ограничивается возможностями Active Directory. В результате операции импорта могут продолжаться очень долго в зависимости от количества добавляемых пользователей и групп. Для уменьшения вероятности появления задержек или проблем сократите количество групп и пользователей и выберите только те из них, которые требуются для работы системы vRealize Automation.


При уменьшении производительности системы или возникновении ошибок закройте все ненужные приложения и убедитесь, что для службы Active Directory в системе выделен соответствующий объем памяти. Если проблема не исчезает, увеличьте соответствующим образом объем памяти, выделенной для Active Directory. Для систем с большим количеством пользователей и групп может понадобиться увеличить объем памяти, выделенной Active Directory, до 24 ГБ.

15. Щелкните **Далее**.

16. Щелкните , чтобы добавить дополнительных пользователей.

Допустимыми являются следующие значения.

- Один пользователь: **CN=username,CN=Users,OU=Users,DC=myCorp,DC=com**
- Несколько пользователей: **OU=Users,OU=myUnit,DC=myCorp,DC=com**

Для исключения пользователей щелкните , чтобы создать фильтр для исключения некоторых типов пользователей. Вы выбираете атрибут пользователя для фильтрации, правило запроса и значение.

17. Щелкните **Далее**.

18. Посмотрите на странице, сколько пользователей и групп синхронизируются с каталогом.

Если нужно изменить пользователей и группы, щелкните ссылки «Изменить».

Примечание Необходимо указать различающиеся имена пользователей, которые включены в базовое различающееся имя, заданное ранее. Если различающееся имя пользователя не соответствует базовому различающемуся имени, данные пользователей с этим различающимся именем будут синхронизироваться, но сами пользователи не смогут выполнить вход.

19. Щелкните **Отправить в Workspace**, чтобы начать синхронизацию с каталогом.

Результаты

Подключение к Active Directory установлено, а выбранные пользователи и группы добавлены в каталог. Теперь можно назначить пользователям и группам соответствующие роли vRealize Automation, выбрав **Администрирование > Пользователи и группы > Пользователи и группы каталога**. Дополнительные сведения см. в разделе [Назначение ролей пользователям или группам](#).

Следующие шаги

Если среда vRealize Automation настроена для обеспечения высокой доступности, необходимо специально настроить управление каталогами для обеспечения высокой доступности. См. раздел [Настройка службы управления каталогами для обеспечения высокой доступности](#).

- Настройте методы проверки подлинности. После синхронизации пользователей и групп с каталогом, если для проверки подлинности также используется соединитель, в нем можно настроить дополнительные методы проверки подлинности. Если поставщиком удостоверений для проверки подлинности является сторонняя организация, настройте этого поставщика в соединителе.
- Проанализируйте политику доступа по умолчанию. Политика доступа по умолчанию настроена так, чтобы все устройства во всех сетевых диапазонах могли получать доступ к веб-браузеру с заданным временем ожидания сеанса (восемь часов) или получать доступ к клиентскому приложению с временем ожидания сеанса 2160 часов (или 90 дней). Политику доступа по умолчанию можно изменить, а при добавлении веб-приложений в каталог можно создать новые политики доступа.
- Примените пользовательскую фирменную символику на консоли администрирования, на страницах пользовательского портала и на экране входа в систему.

Настройка подключения к каталогу OpenLDAP

Настроить подключение к каталогу OpenLDAP можно с помощью службы управления каталогами.

Несмотря на то что существует несколько разных протоколов LDAP, только протокол OpenLDAP был протестирован и утвержден для использования службой управления каталогами vRealize Automation.

Для интеграции каталога LDAP необходимо создать соответствующий каталог Directories Management и синхронизировать пользователей и группы из каталога LDAP с каталогом Directories Management. Для последующих обновлений можно настроить регулярное расписание синхронизации.

Кроме того, следует выбрать атрибуты LDAP, которые нужно синхронизировать для пользователей, и сопоставить их с атрибутами Directories Management.

Конфигурация каталогов LDAP может быть настроена на основе схем по умолчанию или пользовательских схем. Можно также определить пользовательские атрибуты. Чтобы дать Directories Management возможность запрашивать каталог LDAP и получать объекты пользователей или групп, необходимо указать поисковые фильтры и имена атрибутов LDAP, применимых к каталогу LDAP.

В частности, необходимо указать следующие сведения.

- Поисковые фильтры LDAP для получения групп и пользователей, а также пользователя подключения.

- Имена атрибутов LDAP для членства в группе, идентификатора UUID и различающегося имени

Примечание Служба управления каталогами использует для запросов LDAP размер страницы по умолчанию, равный 1500. При настройке подключения к каталогу OpenLDAP необходимо включить простое расширение для контроля результатов на странице для OpenLDAP, чтобы ограничить количество отображаемых результатов. Неправильное использование этого расширения может привести к ошибкам синхронизации пользователей и групп.

Необходимые условия

- Проверьте конфигурацию на странице атрибутов пользователя и добавьте дополнительные атрибуты, которые нужно синхронизировать. При создании каталога атрибуты Directories Management будут сопоставлены с каталогом LDAP. Эти атрибуты будут синхронизированы для пользователей в каталоге.

Примечание При изменении атрибутов пользователя учтите влияние на другие каталоги в службе. Если планируется добавить каталоги Active Directory и LDAP, не отмечайте никакие атрибуты в качестве обязательных (кроме **userName**). Параметры на странице «Атрибуты пользователя» применяются ко всем каталогам службы. Если атрибут обозначен как обязательный, пользователи без этого атрибута не будут синхронизироваться со службой Directories Management.

- Учетная запись пользователя с различающимся именем для подключения. Рекомендуется использовать учетную запись пользователя различающегося имени для подключения с паролем без срока действия.
- В каталоге LDAP универсальный уникальный идентификатор объекта пользователей и групп должен быть указан в текстовом формате.
- В каталоге LDAP для всех пользователей и групп должен быть указан атрибут domain.
Этот атрибут сопоставляется с атрибутом **domain** в Directories Management при создании каталога Directories Management.
- В именах пользователей не должно быть пробелов. Если имя пользователя содержит пробел, пользователь синхронизируется, но права для него становятся недоступны.
- При использовании проверки подлинности с помощью сертификата пользователи должны указать значения для атрибута userPrincipalName, а также атрибуты адреса электронной почты.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Выберите команду **Добавить каталог**, затем — **Добавить каталог LDAP**.

3. Введите необходимые сведения на странице «Добавить каталог LDAP».

Параметр	Описание
Имя каталога	Введите имя для каталога Directories Management.
Синхронизация службы каталогов и проверка подлинности	<p>а) В поле Синхронизируйте соединитель выберите соединитель, который необходимо использовать для синхронизации пользователей и групп каталога LDAP с каталогом Directories Management.</p> <p>Компонент соединителя всегда доступен в службе Directories Management по умолчанию. Этот соединитель отображается в раскрывающемся списке. Если для высокой доступности установлены несколько устройств Directories Management, компонент соединителя каждого из них будет в этом списке.</p> <p>В отдельном соединителе для каталога LDAP нет необходимости. Соединитель может поддерживать несколько каталогов, будь то каталоги Active Directory или LDAP.</p> <p>б) Если необходимо использовать этот каталог LDAP для проверки подлинности пользователей, в поле Проверка подлинности выберите значение Да.</p> <p>Если для проверки подлинности пользователей необходимо применять сторонний поставщик удостоверений, выберите Нет. После подключения к каталогу для синхронизации пользователей и групп перейдите на страницу Администрирование > Управление каталогами > Поставщики удостоверений, чтобы добавить сторонний поставщик удостоверений для проверки подлинности.</p> <p>в) Для большинства конфигураций следует оставить выбранный по умолчанию вариант Пользовательский в текстовом поле Атрибут поиска каталога. В поле Пользовательский атрибут поиска каталога укажите атрибут каталога LDAP, который будет использоваться в качестве имени пользователя и группы. Этот атрибут позволяет идентифицировать объекты, например пользователей и группы, на сервере LDAP. Например, cn.</p> <p>г) Если необходимо использовать поиск расположения служб DNS для Active Directory, установите следующие параметры.</p> <ul style="list-style-type: none"> ■ В разделе «Расположение сервера» (Server Location) установите флажок Данный каталог поддерживает поиск размещения службы DNS. <p>Служба управления каталогами найдет и использует оптимальные контроллеры домена. Если не требуется использовать выбор оптимизированных контроллеров домена, переходите к шагу е.</p> <ul style="list-style-type: none"> ■ Если для Active Directory требуется шифрование STARTTLS, в разделе «Сертификаты» (Certificates) установите флажок Все подключения объектов, входящих в данный каталог, выполняются с использованием протокола SSL, а также скопируйте и вставьте сертификат корневого центра сертификации Active Directory в текстовом поле «Сертификат SSL» (SSL Certificate). <p>Убедитесь, что сертификат создан в формате PEM и содержит строки BEGIN CERTIFICATE и END CERTIFICATE.</p> <p>Примечание Если для Active Directory требуется протокол STARTTLS, а сертификат не предоставлен, создать каталог невозможно.</p> <p>д) Если не требуется использовать поиск расположения служб DNS для Active Directory, установите следующие параметры.</p> <ul style="list-style-type: none"> ■ Убедитесь, что в разделе «Расположение сервера» (Server Location) не установлен флажок Данный каталог поддерживает поиск размещения

Параметр	Описание
	<p>службы DNS, и введите имя узла сервера и номер порта Active Directory. Сведения о том, как настроить каталог в качестве глобального каталога, см. в разделе «Среда Active Directory с несколькими доменами и одним лесом» (Multi-Domain Single-Forest Active Directory) в Среды Active Directory.</p> <ul style="list-style-type: none"> ■ Если для Active Directory требуется доступ по протоколу SSL, в разделе «Сертификаты» (Certificates) установите флажок Все подключения объектов, входящих в данный каталог, выполняются с использованием протокола SSL, а также скопируйте и вставьте сертификат корневого центра сертификации Active Directory в поле «Сертификат SSL» (SSL Certificate). <p>Убедитесь, что сертификат создан в формате PEM и содержит строки BEGIN CERTIFICATE и END CERTIFICATE.</p> <p>Примечание Если для Active Directory требуется протокол STARTTLS, а сертификат не предоставлен, создать каталог невозможно.</p>
Расположение сервера	<p>Введите имя узла и номер порта узла сервера каталога LDAP. В качестве узла сервера можно указать полное доменное имя или IP-адрес. Например, myLDAPserver.example.com или 100.00.00.0.</p> <p>При наличии серверного кластера за средством балансировки нагрузки введите вместо этого сведения о средстве балансировки нагрузки.</p>
Настройка LDAP	<p>Укажите фильтры и атрибуты поиска LDAP, которые Directories Management следует использовать для создания запроса каталога LDAP. Значения по умолчанию указываются, исходя из данных основной схемы LDAP.</p> <p>Запросы с фильтрацией</p> <ul style="list-style-type: none"> ■ Группы: поисковый фильтр для получения объектов группы. <p>Например, (objectClass=group).</p> <ul style="list-style-type: none"> ■ Пользователь подключения: поисковый фильтр для получения объекта пользователя подключения, то есть пользователя, который может подключаться к каталогу. <p>Например, (objectClass=person).</p> <ul style="list-style-type: none"> ■ Пользователи: поисковый фильтр для получения данных пользователей, которые необходимо синхронизировать. <p>Например, (&(objectClass=user)(objectCategory=person)).</p> <p>Атрибуты</p> <ul style="list-style-type: none"> ■ Состав: атрибут, который используется в каталоге LDAP для определения участников группы. <p>Например, member.</p> <ul style="list-style-type: none"> ■ Универсальный уникальный идентификатор объекта: атрибут, который используется в каталоге LDAP для определения универсального уникального идентификатора пользователя и группы. <p>Например, entryUUID.</p> <ul style="list-style-type: none"> ■ Различающееся имя: атрибут, который используется в каталоге LDAP для определения различающегося имени пользователя или группы. <p>Например, entryDN.</p>

Параметр	Описание
Сертификаты	<p>Если для каталога LDAP требуется доступ с использованием SSL, установите флажок Все подключения объектов, входящих в данный каталог, выполняются с использованием протокола SSL. Затем скопируйте сертификат SSL из корневого центра сертификации, настроенного для сервера каталога LDAP, и вставьте в текстовое поле Сертификат SSL. Убедитесь, что сертификат находится в формате PEM и содержит строки BEGIN CERTIFICATE и END CERTIFICATE.</p> <p>Если в каталоге есть несколько доменов, поочередно добавляйте сертификаты корневого центра сертификации для всех доменов.</p> <p>Далее убедитесь, что в поле Порт сервера в разделе «Расположение сервера» на данной странице правильно указан номер порта.</p>
Сведения о пользователе подключения	<p>Базовое различающееся имя: введите различающееся имя, с которого будет начинаться поиск. Например, cn=users,dc=example,dc=com.</p> <p>Все соответствующие пользователи должны относиться к базовому различающемуся имени. В противном случае пользователь не сможет войти в систему, даже если он является членом группы, которая относится к базовому различающемуся имени.</p> <p>Различающееся имя для подключения — введите различающееся имя, которое следует использовать для подключения к каталогу LDAP. Можно вводить и имена пользователей, однако для большинства развертываний наиболее подходящим вариантом является различающееся имя.</p> <hr/> <p>Примечание Рекомендуется использовать учетную запись пользователя различающегося имени для подключения с паролем без срока действия.</p> <hr/> <p>Пароль для базового различающегося имени — введите пароль для пользователя с различающимся именем для подключения.</p>

- Чтобы проверить подключение к серверу каталога LDAP, щелкните **Протестировать соединение**.

Если не удастся установить подключение, проверьте введенные сведения и внесите соответствующие изменения.

- Нажмите **Сохранить и Далее**.
- Проверьте, правильно ли указан домен на странице «Выбор доменов», затем щелкните элемент **Далее**.
- На странице «Сопоставление атрибутов» убедитесь, что атрибуты Directories Management сопоставлены с правильными атрибутами LDAP.

Эти атрибуты будут синхронизированы для пользователей.

Важно! Необходимо указать сопоставление для атрибута **domain**.

На странице «Атрибуты пользователя» можно добавить атрибуты в список.

- Нажмите кнопку **Далее**.
- Щелкните знак **+**, чтобы выбрать группы для синхронизации между каталогом LDAP и каталогом Directories Management на странице «Выбор групп (пользователей) для синхронизации».

Если в каталоге LDAP есть несколько групп с одинаковыми именами, на странице групп необходимо указать для них уникальные имена.

Если при добавлении группы из Active Directory ее участников нет в списке пользователей, они будут добавлены. При синхронизации группы все пользователи, для которых группа «Пользователи домена» в Active Directory не является основной, не синхронизируются.

Параметр **Синхронизировать участников вложенных групп** включен по умолчанию. Когда этот параметр включен, все пользователи, которые принадлежат непосредственно к выбранной группе, а также к вложенным группам этой группы, синхронизируются. Обратите внимание, что синхронизируются не вложенные группы, а только пользователи, принадлежащие к ним. В каталоге Directories Management эти пользователи будут участниками группы верхнего уровня, выбранной для синхронизации. Иерархические элементы ниже выбранной группы удаляются, а пользователи всех уровней отображаются в Directories Management в составе выбранной группы.

Если этот параметр деактивирован, то при указании группы для синхронизации все пользователи, которые непосредственно к ней относятся, синхронизируются. Пользователи, которые принадлежат к вложенным группам этой группы, не синхронизируются. Отключение этого параметра полезно для больших конфигураций каталога, где навигация по дереву групп требует значительных объемов ресурсов и времени. Но перед тем как его деактивировать, убедитесь, что выбраны все группы, пользователей которых необходимо синхронизировать.

Примечание Система проверки подлинности пользователей Directories Management импортирует данные из Active Directory при добавлении групп и пользователей, при этом быстродействие системы ограничивается возможностями Active Directory. В результате операции импорта могут продолжаться очень долго в зависимости от количества добавляемых пользователей и групп. Для уменьшения вероятности появления задержек или проблем сократите количество групп и пользователей и выберите только те из них, которые требуются для работы системы vRealize Automation.

При снижении производительности системы или возникновении ошибок закройте все ненужные приложения и убедитесь, что для службы управления каталогами в системе выделен соответствующий объем памяти. Если проблема не исчезает, увеличьте соответствующим образом объем памяти, выделенной для данной службы. Если в системе много пользователей и групп, возможно, понадобится увеличить этот объем до 24 ГБ.

10. Нажмите кнопку **Далее**.

11. Щелкните **+**, чтобы добавить дополнительных пользователей. Например, введите **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Здесь можно добавлять как организационные единицы, так и отдельных пользователей.

Можно создать фильтр, чтобы исключить отдельные типы пользователей. Выберите атрибут пользователя для фильтрации, правило запроса и значение.

12. Нажмите кнопку **Далее**.

13. На этой странице можно просмотреть расписание синхронизации по умолчанию и узнать, сколько пользователей и групп будет синхронизироваться с каталогом.

Чтобы внести изменения в список пользователей и групп или интервал синхронизации, щелкните ссылки **Изменить**.

14. Щелкните команду **Синхронизировать каталог**, чтобы запустить синхронизацию каталогов.

Результаты

Устанавливается подключение к каталогу LDAP, а пользователи и группы каталога LDAP синхронизируются с каталогом Directories Management.

Теперь можно назначить пользователям и группам соответствующие роли vRealize Automation, выбрав **Администрирование > Пользователи и группы > Пользователи и группы каталога**. Дополнительные сведения см. в разделе [Назначение ролей пользователям или группам](#).

Ограничения интеграции каталогов LDAP

Существует несколько важных ограничений, связанных с подключением каталога LDAP к системе «Управление каталогами».

- Интегрировать можно только среду каталогов LDAP одного домена.
Чтобы интегрировать несколько доменов из каталога LDAP, необходимо создать дополнительные каталоги Directories Management (по одному для каждого домена).
- Следующие методы проверки подлинности не поддерживаются каталогами LDAP в Directories Management.
 - проверка подлинности с помощью Kerberos
 - Адаптивная проверка подлинности RSA
 - ADFS в качестве стороннего поставщика удостоверений.
 - SecurID
 - Проверка подлинности Radius с использованием Vasco и сервера SMS Passcode.
- Нельзя присоединиться к домену LDAP.
- Интеграция с помощью View или опубликованных ресурсов Citrix для каталогов LDAP в Directories Management не поддерживается.
- В именах пользователей не должно быть пробелов. Если имя пользователя содержит пробел, пользователь синхронизируется, но права для него становятся недоступны.
- Если планируется добавить каталоги Active Directory и LDAP, не отмечайте никакие атрибуты в качестве обязательных на странице «Атрибуты пользователя» (кроме userName, который можно отметить в качестве обязательного). Параметры на странице «Атрибуты пользователя» применяются ко всем каталогам службы. Если атрибут обозначен как обязательный, пользователи без этого атрибута не будут синхронизироваться со службой Directories Management.
- Если в каталоге LDAP есть несколько групп с одинаковыми именами, в службе Directories Management необходимо указать для них уникальные имена. Указать имена можно при выборе групп для синхронизации.
- Параметр, с помощью которого можно разрешить пользователям сбросить просроченные пароли, недоступен.
- Файл domain_krb.properties не поддерживается.

Настройка службы управления каталогами для обеспечения высокой доступности

Службу управления каталогами можно использовать для настройки подключения к Active Directory с высокой доступностью в vRealize Automation.

Каждое устройство vRealize Automation содержит соединитель, который поддерживает проверку подлинности пользователей, хотя для обеспечения синхронизации каталога обычно настроен только один соединитель. В качестве соединителя синхронизации можно выбрать любой соединитель. Для поддержки высокой доступности службы управления каталогами необходимо вручную настроить второй соединитель, соответствующий второму устройству vRealize Automation, который подключается к поставщику удостоверений и указывает на ту же самую службу Active Directory. При использовании такой конфигурации, если одно устройство выходит из строя, второе принимает на себя управление процессом проверки подлинности пользователей.

В среде с высокой доступностью все узлы должны обслуживать один и тот же набор каталогов Active Directory, пользователей, методов проверки подлинности и т. д. Наиболее простым способом реализации такой конфигурации является применение поставщика удостоверений в кластере путем настройки узла подсистемы балансировки нагрузки в качестве узла поставщика удостоверений. Благодаря такой конфигурации все запросы на проверку подлинности направляются в подсистему балансировки нагрузки, которая затем отправляет их на один из соединителей.

Соединитель также используется для синхронизации пользователей. Но для синхронизации каталогов настроен только один соединитель. Синхронизированные пользователи сохраняются в базе данных устройств, информацию в которой считывают все кластерные узлы. В случае сбоя соединителя, отвечающего за синхронизацию каталогов, данный процесс синхронизации перестанет работать. Для восстановления нормального режима работы администратор арендатора должен вручную предложить другому соединителю выполнить синхронизацию каталогов с помощью пользовательского интерфейса vRealize Automation. См. раздел [Включение синхронизации каталогов на дополнительном соединителе](#).

Дополнительные сведения о работе с соединителями см. в разделе [Управление соединителями и кластерами соединителей](#).

Необходимые условия

- Настройте развертывание vRealize Automation как минимум с двумя экземплярами устройства vRealize Automation.
- Установите vRealize Automation в режиме Enterprise, функционирующем в одном домене с двумя экземплярами устройства vRealize Automation.
- Установите и настройте соответствующую подсистему балансировки нагрузки для работы с развертыванием vRealize Automation.
- Настройте арендаторов и службу управления каталогами, используя один из соединителей, предоставляемых с установленными экземплярами устройства vRealize Automation. Сведения о настройке арендатора см. в разделе [Настройка параметров арендатора](#).

Процедура

1. Войдите в подсистему балансировки нагрузки для развертывания vRealize Automation в качестве администратора арендатора.

URL-адрес подсистемы балансировки нагрузки — <адрес подсистемы балансировки нагрузки>/*vcac/org/tenant_name*.
2. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.
3. Щелкните поставщика удостоверений, который в настоящее время используется для вашей системы.

Появляются существующий каталог и соединитель, которые обеспечивают базовое управление учетными данными для вашей системы.
4. На странице свойств поставщика удостоверений щелкните раскрывающийся список **Добавить соединитель** и выберите соединитель, который соответствует дополнительному устройству vRealize Automation.
5. Введите соответствующий пароль в текстовом поле **Пароль имени домена привязки**, которое появляется при выборе соединителя.
6. Щелкните **Добавить соединитель**.
7. В текстовом поле **Имя узла поставщика удостоверений** по умолчанию появляется основной соединитель. Измените имя узла для указания на подсистему балансировки нагрузки.

Включение синхронизации каталогов на дополнительном соединителе

В случае сбоя основного соединителя проверка подлинности выполняется автоматически другим экземпляром соединителя. В случае сбоя для синхронизации каталогов необходимо изменить параметры каталога в службе управления каталогами, чтобы она использовала соответствующий экземпляр дополнительного соединителя. В данный момент времени синхронизация каталогов может выполняться только на одном соединителе.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**
2. Выберите каталог, который был связан с исходным экземпляром соединителя.

Примечание Эту информацию можно просмотреть на странице **Каталоги > Соединители**.

3. В разделе «Синхронизация каталогов и проверка подлинности» на странице «Каталог» выберите другой экземпляр соединителя в раскрывающемся списке **Синхронизировать соединитель**.
4. В разделе «Сведения о привязке пользователя» введите пароль учетной записи для подключения Active Directory в текстовом поле **Пароль привязки DN**.
5. Нажмите кнопку **Сохранить**.

Настройка двунаправленных отношений доверия между vRealize Automation и Active Directory

Можно повысить уровень системной безопасности обычного подключения vRealize Automation Active Directory с помощью настройки двунаправленных отношений доверия между поставщиком удостоверений и службами федерации Active Directory.

Для настройки двунаправленных отношений доверия между vRealize Automation и Active Directory необходимо создать специального поставщика удостоверений и добавить в него метаданные Active Directory. Кроме того, необходимо изменить политику по умолчанию, используемую развертыванием vRealize Automation. Наконец, следует настроить Active Directory для распознавания поставщика удостоверений.

Необходимые условия

- Убедитесь, что вы настроили арендаторов для развертывания vRealize Automation и создали соответствующий канал связи с Active Directory для поддержки обычной проверки подлинности по идентификатору пользователя Active Directory и паролю.
- Служба Active Directory установлена и настроена для использования в вашей сети.
- Получите соответствующие метаданные служб федерации Active Directory (ADFS).
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Получите файл Federation Metadata.

Этот файл можно загрузить по ссылке <https://servername.domain/FederationMetadata/2007-06/FederationMetadata.xml>

2. Найдите слово «logout» (выход из системы) и измените расположение каждого экземпляра так, чтобы был указан адрес <https://servername.domain/adfs/ls/logout.aspx>

Например,

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/ "/>
```

необходимо изменить на

```
SingleLogoutService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Location="https://servername.domain/adfs/ls/logout.aspx"/>
```

3. Создайте нового поставщика удостоверений для развертывания.

- а) Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.
- б) Щелкните **Добавить поставщика удостоверений** и заполните поля соответствующим образом.

Параметр	Описание
Имя поставщика удостоверений	Введите имя нового поставщика удостоверений.
Метаданные поставщика удостоверений (URL-адрес или XML)	Вставьте содержимое файла метаданных служб федерации Active Directory здесь.
Политика идентификатора имени в запросе SAML (необязательно)	При необходимости введите имя для запроса политики удостоверений SAML.
Пользователи	Выберите домены, для доступа к которым необходимо предоставить пользователям привилегии.
IDP-метаданные процесса	Щелкните, чтобы обработать добавленный файл метаданных.
Сеть	Выберите диапазоны сети, доступ к которым необходимо предоставить пользователям.
Способы проверки подлинности	Введите имя способа проверки подлинности, который использует этот поставщик удостоверений.
Контекст SAML	Выберите подходящий контекст для системы.
Сертификат подписи SAML	Перейдите по ссылке рядом с заголовком «Метаданные SAML», чтобы загрузить метаданные службы управления каталогами.

- в) Сохраните файл метаданных службы управления каталогами как `sp.xml`.
- г) Нажмите кнопку **Добавить**.

4. Добавьте правило в политику по умолчанию.

- а) Выберите **Администрирование > Управление каталогами > Политики**.
- б) Щелкните имя политики по умолчанию.
- в) Для добавления нового правила щелкните значок **+** под заголовком **Правила политики**.

Для создания правила, указывающего соответствующие основной и дополнительный методы проверки подлинности для конкретного сетевого диапазона и устройства, используйте параметры на странице «Добавить правило политики».

Например, если сетевой диапазон пользователя — **«Мой компьютер»**, и пользователю нужно получать доступ к содержимому из **«Всех типов устройств»**, то для типового развертывания проверка подлинности этого пользователя должна выполняться с помощью следующего метода: **Имя пользователя ADFS и пароль**.

- г) Щелкните **ОК**, чтобы сохранить измененную политику.
- д) На странице «Политика по умолчанию» перетащите новое правило в верхнюю часть таблицы, чтобы оно имело более высокий приоритет, чем существующие правила.

5. С помощью консоли управления службами федерации Active Directory или другого соответствующего средства установите отношения доверия между проверяющей стороной и поставщиком удостоверений vRealize Automation.

Для установки таких отношений доверия необходимо импортировать предварительно загруженные метаданные службы управления каталогами. Дополнительные сведения о настройке консоли служб федерации Active Directory для двунаправленных отношений доверия см. в документации по Microsoft Active Directory. В рамках этого процесса необходимо выполнить следующие действия.

- Установите отношения доверия с проверяющей стороной. При этом необходимо импортировать XML-файл метаданных поставщика услуг VMware Identity Provider, который вы скопировали и сохранили.
- Создайте правило утверждения, которое преобразует атрибуты, полученные из LDAP в правиле Get Attributes (Получение атрибутов) в требуемый формат SAML. После создания правила измените его, добавив следующий текст:

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType, Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/
format"] = "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress", Properties["http://
schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"] =
"vmwareidentity.domain.com");
```

Настройка федерации SAML между Directories Management и SSO2

Между vRealize Automation Directories Management и системами, в которых для поддержки единого входа используется SSO2, можно установить федерацию SAML.

Установите федерацию между Directories Management и SSO2 путем создания подключения SAML между двумя этими объектами. В настоящее время единственным поддерживаемым сквозным потоком является поток, где SSO2 действует как поставщик удостоверений (IdP), а Directories Management — как поставщик услуг (SP).

Для проверки подлинности пользователя SSO2 должна существовать одинаковая учетная запись в Directories Management и SSO2. По крайней мере имя UserPrincipalName (UPN) пользователя должно совпадать. Другие атрибуты могут отличаться, так как они требуются для идентификации субъекта SAML.

Для локальных пользователей в SSO2, например `admin@vsphere.local`, в Directories Management также должны существовать соответствующие учетные записи (по крайней мере с совпадающими именами UPN пользователей). Создайте эти учетные записи вручную или с помощью сценария, в котором используются интерфейсы API для создания локального пользователя Directories Management.

При настройке SAML между SSO2 и Directories Management выполняется настройка компонентов управления каталогами и службы единого входа.

Таблица 2-4. Конфигурация компонента федерации SAML

Компонент	Конфигурация
Управление каталогами	Настройте SSO2 в качестве стороннего поставщика удостоверений в разделе Directories Management и обновите политику проверки подлинности по умолчанию. Для настройки Directories Management можно создать автоматизированный сценарий.
Компонент SSO2	Настройте Directories Management в качестве поставщика услуг, выполнив импорт файла Directories Managementsp.xml. Этот файл позволяет настроить SSO2 для использования Directories Management в качестве поставщика услуг (SP).

Необходимые условия

- Настройте арендаторов для развертывания vRealize Automation. См. раздел [Создание дополнительных арендаторов](#).
- Задайте подходящую ссылку Active Directory для поддержки стандартной проверки подлинности идентификатора и пароля пользователя Active Directory.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Загрузите метаданные поставщика удостоверений SSO2 через интерфейс пользователя SSO2.
 - а) Войдите в vCenter в качестве администратора по адресу `https://<cloudvm-hostname>/`.
 - б) Щелкните ссылку **Вход в vSphere Web Client**.
 - в) На панели навигации слева выберите **Администрирование > Single Sign On > Конфигурация**.
 - г) Щелкните **Загрузить** рядом с заголовком «Метаданные для поставщика услуг SAML».

Должен начать загружаться файл `vsphere.local.xml`.
 - д) Скопируйте содержимое файла `vsphere.local.xml`.
2. На странице «Поставщики удостоверений управления каталогами vRealize Automation» создайте новый поставщик удостоверений.
 - а) Войдите в vRealize Automation в качестве **администратора арендатора**.
 - б) Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

- в) Щелкните **Добавить поставщика удостоверений** и предоставьте сведения конфигурации.

Параметр	Действие
Имя поставщика удостоверений	Введите имя нового поставщика удостоверений.
Текстовое поле Метаданные поставщика удостоверений (URI или XML)	Вставьте содержимое файла метаданных SSO2 idp.xml в текстовое поле и нажмите кнопку Обработать метаданные пост. удост.
Политика идентификатора имени в запросе SAML (необязательно)	Введите <code>http://schemas.xmlsoap.org/claims/UPN</code> .
Пользователи	Выберите домены, для доступа к которым необходимо предоставить пользователям привилегии.
Сеть	Выберите диапазоны сети, в которых пользователям необходимо предоставить привилегии доступа. Если нужно проверять подлинность пользователей с IP-адресов, выберите Все диапазоны .
Способы проверки подлинности	Введите имя способа проверки подлинности. Затем используйте раскрывающееся меню Контекст SAML справа для сопоставления способа проверки подлинности с <code>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</code> .
Сертификат подписи SAML	Перейдите по ссылке рядом с заголовком «Метаданные SAML», чтобы загрузить метаданные службы управления каталогами.

- г) Сохраните файл метаданных службы управления каталогами как `sp.xml`.
- д) Щелкните **Добавить**.
- 3.** Обновите соответствующую политику проверки подлинности на странице «Политики управления каталогами» для перенаправления проверки подлинности на стороннего поставщика удостоверений SSO2.
- а) Выберите **Администрирование > Управление каталогами > Политики**.
- б) Щелкните имя политики по умолчанию.
- в) Щелкните способ проверки подлинности под заголовком **Правила политики** для редактирования существующего правила проверки подлинности.
- г) На странице «Изменить правило политики» установите другой способ проверки подлинности (не по паролю).
- В этом случае должен быть метод SSO2.
- д) Щелкните **Сохранить**, чтобы сохранить внесенные изменения в политике.
- 4.** На панели навигации слева выберите **Администрирование > Single Sign On > Конфигурация** и щелкните **Обновить**, чтобы передать файл `sp.xml` в vSphere.

Добавление пользователей или групп к подключению Active Directory

К существующему подключению Active Directory можно добавлять пользователей и группы.

При добавлении групп и пользователей функция проверки подлинности пользователей в системе управления каталогами импортирует данные из Active Directory. Скорость передачи данных ограничивается возможностями Active Directory. В связи с этим для выполнения действий может потребоваться значительное время, которое зависит от количества добавляемых групп и пользователей. Чтобы свести к минимуму проблемы, добавьте только пользователей и группы, которые необходимы для выполнения действия vRealize Automation. В случае возникновения проблем закройте ненужные приложения и проверьте, выделен ли для Active Directory в текущем развертывании достаточный объем памяти. Если проблемы сохраняются, увеличьте объем выделенной памяти для Active Directory. Для развертываний с большим количеством пользователей и групп может потребоваться увеличить объем памяти, выделенной для Active Directory, до 24 ГБ.

Когда развертывание vRealize Automation синхронизируется с большим количеством пользователей и групп, могут возникать задержки при отображении данных в журнале SyncLog. Метка времени, присвоенная журналу, может отличаться от времени завершения, отображаемого в консоли.

Если участники группы не включены в список «Пользователи», то при добавлении такой группы из Active Directory ее участники включаются в этот список. При синхронизации группы все пользователи, для которых группа «Пользователи домена» в Active Directory не является основной, не синхронизируются.

Примечание Отменить запущенную операцию синхронизации невозможно.

Необходимые условия

- Соединитель Соединитель установлен, и код активации активирован. На странице «Атрибуты пользователя» выберите обязательные атрибуты по умолчанию и добавьте дополнительные атрибуты.
- Список групп и пользователей Active Directory, которые нужно синхронизировать из Active Directory.
- Для подключения к Active Directory по протоколу LDAP необходимо указать такую информацию, как базовое имя домена, имя домена привязки и пароль имени домена привязки.
- Для встроенной проверки подлинности Windows в Active Directory необходимо указать такую информацию, как адрес и пароль UPN пользователя привязки домена.
- Если доступ к Active Directory устанавливается по SSL, необходима копия сертификата SSL.
- Если используется Active Directory с несколькими лесами и интегрированной проверкой подлинности Windows, а в локальную группу домена входят участники из различных лесов, выполните указанные ниже действия. Добавьте пользователя привязки в список администраторов локальной группы домена. В противном случае эти участники не будут включены в локальную группу домена.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Щелкните нужное имя каталога.

3. Нажмите кнопку **Настройки синхронизации**, чтобы открыть диалоговое окно с параметрами синхронизации.
4. Щелкните соответствующий значок в зависимости от того, чью конфигурацию нужно изменить (пользователя или группы).

Чтобы изменить конфигурацию группы, сделайте следующее:

- Чтобы добавить группы, щелкните значок **+**, добавьте строку для определений имен доменов группы и введите соответствующее имя домена группы.
- Если нужно удалить определение имени домена группы, щелкните значок **X** возле нужного имени домена группы.

Чтобы изменить конфигурацию пользователя, сделайте следующее:

- ◆ Чтобы добавить пользователей, щелкните значок **+**, добавьте строку для определения имени домена пользователя и введите соответствующее имя домена пользователя.

Если нужно удалить определение имени домена пользователя, щелкните значок **X** возле нужного имени домена пользователя.

5. Нажмите кнопку **Сохранить**, чтобы сохранить изменения без запуска синхронизации. Нажмите кнопку **Сохранить и синхронизировать**, чтобы сохранить и синхронизировать изменения.

Выбор атрибутов для синхронизации с каталогом

При настройке каталога Directories Management для синхронизации с Active Directory указываются атрибуты пользователя, которые должны синхронизироваться с каталогом. Перед настройкой каталога на странице «Атрибуты пользователя» можно указать, какие атрибуты требуются по умолчанию и, при желании, добавить дополнительные атрибуты, которые нужно сопоставить атрибутам Active Directory.

При настройке перед созданием каталога на странице «Атрибуты пользователя» можно изменить обязательные атрибуты по умолчанию на необязательные, отметить атрибуты как обязательные и добавить пользовательские атрибуты.

Для получения списка сопоставленных атрибутов по умолчанию см. [Управление атрибутами пользователя, синхронизируемыми из Active Directory](#).

После создания каталога можно изменить обязательный атрибут на необязательный и удалить пользовательские атрибуты. Нельзя изменить атрибут, чтобы он стал быть обязательным атрибутом.

При добавлении других атрибутов для синхронизации каталога после его создания перейдите на страницу каталога «Сопоставленные атрибуты» для сопоставления этих атрибутов атрибутам Active Directory.

Процедура

1. Войдите в службу vRealize Automation от имени системного администратора или администратора арендатора.
2. Откройте вкладку «Администрирование».
3. Выберите **Управление каталогами > Атрибуты пользователя**
4. В разделе «Атрибуты по умолчанию» нужно проверить список обязательных атрибутов и внести соответствующие изменения, чтобы указать, какие атрибуты должны быть обязательными.

5. В разделе «Атрибуты» в список необходимо добавить имя атрибута каталога Directories Management.
6. Нажмите кнопку **Сохранить**.
Состояние атрибута по умолчанию обновится, и новые атрибуты будут добавлены в список сопоставленных атрибутов каталога.
7. После создания каталога перейдите на страницу «Хранилища удостоверений» и выберите каталог.
8. Нажмите **Настройки синхронизации > Сопоставленные атрибуты**.
9. В раскрывающемся меню для добавленных атрибутов выберите атрибут Active Directory для сопоставления.
10. Нажмите кнопку **Сохранить**.

Результаты

Каталог обновится в следующий раз при синхронизации с Active Directory.

Добавление памяти в службу управления каталогами

При наличии подключений к Active Directory с большим количеством пользователей или групп может потребоваться выделение дополнительного объема памяти для Directories Management.

По умолчанию службе Directories Management выделены 4 Гбайт памяти. Этого достаточно для большинства малых и средних развертываний. Если у вас есть подключение Active Directory для большого числа пользователей или групп, возможно, потребуется увеличить этот объем памяти. Выделение дополнительной памяти необходимо для систем с более чем 100 000 пользователями. Каждая система может содержать от 30 до 750 групп. Для таких систем VMware рекомендует увеличить объем выделенной памяти для Directories Management до 6 Гбайт.

Объем памяти для службы управления каталогами рассчитывается на основе общего объема памяти, выделенного для устройства vRealize Automation. В следующей таблице указана выделенная память для соответствующих компонентов.

Таблица 2-5. Выделенная память для устройства vRealize Automation

Память виртуального устройства	Память службы vRA	Память службы vIDM
18 Гбайт	3,3 Гбайт	4 Гбайт
24 Гбайт	4,9 Гбайт	6 Гбайт
30 Гбайт	7,4 Гбайт	9,1 Гбайт

Примечание Указанный объем памяти предполагает, что все службы по умолчанию включены и выполняются на виртуальном устройстве. Если некоторые службы будут остановлены, размер памяти может измениться.

Необходимые условия

- Соответствующее подключение Active Directory настроено и функционирует в развернутой системе vRealize Automation.

Процедура

1. Остановите каждый компьютер, на котором работает устройство vRealize Automation.
2. Увеличьте объем выделенной памяти виртуального устройства на каждом компьютере.

Если вы используете выделенную память по умолчанию размером 18 Гбайт, VMware рекомендует увеличить размер выделенной памяти до 24 Гбайт.

3. Перезапустите компьютеры с устройством vRealize Automation.

Настройка моментальной регистрации пользователей

Можно настроить моментальную регистрацию для поддержки добавления пользователей без синхронизации с Active Directory.

Для поддержки моментальной регистрации необходимо добавить стороннего поставщика удостоверений, а затем настроить подключение к нему в рамках развертывания vRealize Automation для интеграции управления каталогами с другими поставщиками SSO по протоколу SAML. Кроме того, необходимо создать новый каталог с соответствующим именем, например каталог моментальной регистрации.

При включении моментальной регистрации можно добавить динамически добавляемых пользователей в назначенную настраиваемую группу. Чтобы обеспечить поддержку этой функции, создайте настраиваемую группу с соответствующими участниками. См. раздел [Динамическое добавление пользователей с настраиваемыми группами и правилами](#).

Примечание Рекомендуется не настраивать моментальную регистрацию в арендаторе по умолчанию vsphere.local.

Необходимые условия

Настройте соответствующего стороннего поставщика удостоверений для использования при моментальной регистрации.

Процедура

1. Создайте поставщика удостоверений для моментальной регистрации.

- а) Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.
- б) Щелкните **Добавить поставщика удостоверений** и измените параметры экземпляра поставщика удостоверений соответствующим образом.
 - Для моментальной регистрации создайте стороннего поставщика удостоверений.
 - В разделе «Создание каталога моментальной регистрации» введите имена для каталога и одного или нескольких доменов.
 - Необходимо выбрать сеть для конфигурации стороннего поставщика удостоверений.
 - Если используется внешний экземпляр VMware Identity Manager в качестве стороннего поставщика удостоверений и для проверки подлинности пользователей используется userPrincipleName, необходимо изменить конфигурацию сопоставления идентификаторов имен для userPrincipleName со значения по умолчанию x509SubjectName на unspecified.

Дополнительные сведения о создании поставщиков удостоверений см. в разделе [Настройка подключения стороннего поставщика удостоверений](#).

2. Настройте SAML для поставщика удостоверений, используемого для динамической регистрации.

- а) Скопируйте метаданные с поставщика удостоверений.
- б) В vRealize Automation выберите поставщика удостоверений и вставьте его метаданные в текстовом поле **Метаданные поставщика удостоверений (URL-адрес или XML)**.
- в) Нажмите кнопку **Сохранить**.
- г) В раскрывающемся меню **Политика идентификаторов имени в запросах SAML (Необязательно)** выберите нужный формат.

Например, при использовании адреса электронной почты в качестве уникального идентификатора пользователя можно выбрать urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress.

- д) Выберите соответствующий каталог в разделе «Пользователи».
- е) Выберите сети, которые будут использоваться этим поставщиком удостоверений, в разделе «Сеть».
- ж) Укажите соответствующее имя в текстовом поле **Методы проверки подлинности**.
- з) В раскрывающемся списке **Контекст SAML** выберите urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport.
- и) Щелкните правой кнопкой мыши ссылку **Метаданные поставщика услуг** и откройте ее в отдельной вкладке браузера.
- к) Используйте эти метаданные для настройки подключения SAML к поставщику удостоверений. При использовании VMware Identity Manager подробные инструкции по настройке SAML см. в документации по VMware Identity Manager.

3. Нажмите кнопку *Добавить*.

Новый каталог создается с помощью предоставленного имени каталога.

4. Настройте политику доступа к vRealize Automation.

- а) Выберите **Администрирование > Политики**.
- б) Щелкните зеленый значок «+» в верхнем правом углу таблицы правил политик.
- в) Настройте правило политики, чтобы применить соответствующие диапазоны и типы устройств.
- г) Выберите метод проверки подлинности, созданный при настройке стороннего поставщика удостоверений для моментальной регистрации для метода проверки подлинности.

Управление атрибутами пользователя, синхронизируемыми из Active Directory

На странице «Управление каталогами», «Атрибуты пользователя» перечислены атрибуты пользователя, которые синхронизируются с помощью подключения к Active Directory.

Изменения, внесенные и сохраненные на странице «Атрибуты пользователя», добавляются на страницу «Сопоставленные атрибуты» в каталоге Directories Management. Изменения атрибутов вносятся в каталог при следующей синхронизации с Active Directory.

На странице «Атрибуты пользователя» перечислены атрибуты каталога по умолчанию, которые можно сопоставить с атрибутами Active Directory. Выберите необходимые атрибуты, также можно добавить прочие атрибуты Active Directory, которые нужно синхронизировать с каталогом.

Таблица 2-6. Атрибуты Active Directory по умолчанию для синхронизации с каталогом

Имя атрибута каталога	Сопоставление с атрибутом Active Directory по умолчанию
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeid	employeeID
Домен	canonicalName. Добавляет полное доменное имя объекта.
отключено (внешний пользователь отключен)	userAccountControl. Помечено как UF_Account_Disable. Пользователи с отключенными учетными записями не могут получить доступ к своим приложениям и ресурсам. Ресурсы, на доступ к которым у пользователей имелись права, не удаляются из учетной записи, поэтому в случае снятия пометки с учетной записи пользователи смогут войти и получить доступ к ресурсам в соответствии с правами.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
Имя пользователя	sAMAccountName

На странице «Атрибуты пользователя» перечислены атрибуты каталога по умолчанию, которые можно сопоставить с атрибутами Active Directory. Выберите необходимые атрибуты, также можно добавить прочие атрибуты Active Directory, которые нужно синхронизировать с каталогом.

Таблица 2-7. Атрибуты Active Directory по умолчанию для синхронизации с каталогом

Имя атрибута каталога	Сопоставление с атрибутом Active Directory по умолчанию
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
Домен	canonicalName. Добавляет полное доменное имя объекта.
отключено (внешний пользователь отключен)	userAccountControl. Помечено как UF_Account_Disable. Пользователи с отключенными учетными записями не могут получить доступ к своим приложениям и ресурсам. Ресурсы, на доступ к которым у пользователей имелись права, не удаляются из учетной записи, поэтому в случае снятия пометки с учетной записи пользователи смогут войти и получить доступ к ресурсам в соответствии с правами.
phone	telephoneNumber
lastName	sn
firstName	givenName
email	mail
Имя пользователя	sAMAccountName

Управление соединителями и кластерами соединителей

На странице «Соединители» приведен список развернутых соединителей для корпоративной сети. Соединитель синхронизирует пользовательские и групповые данные между Active Directory и службой управления каталогами и проверяет подлинность пользователей в службе при использовании в качестве поставщика удостоверений.

В vRealize Automation каждое устройство Устройство vRealize Automation содержит собственный соединитель, и эти соединители подходят для большинства развертываний.

При связывании каталога с экземпляром соединителя, он создает раздел для связанного каталога, который называется «рабочий процесс». С экземпляром соединителя может быть связано несколько рабочих процессов. Каждый рабочий процесс выступает в качестве поставщика удостоверений. Соединитель синхронизирует пользовательские и групповые данные между Active Directory и службой с помощью одного или нескольких рабочих процессов. Для каждого рабочего процесса определяются и настраиваются способы проверки подлинности.

На странице «Соединители» можно управлять различными аспектами связи с Active Directory. На этой странице имеется таблица и несколько кнопок, которые позволяют выполнять различные задачи по управлению.

- В столбце «Рабочий процесс» выберите рабочий процесс, чтобы просмотреть подробные сведения о соединителе, и перейдите на страницу «Адаптеры проверки подлинности», чтобы увидеть состояние доступных способов проверки подлинности. Дополнительные сведения о проверке подлинности см. в разделе [Интеграция альтернативных продуктов для проверки подлинности пользователей с управлением каталогами](#).
- В столбце «Поставщик удостоверений» выберите поставщика удостоверений для просмотра, изменения или деактивации. См. раздел [Настройка подключения стороннего поставщика удостоверений](#).
- В столбце «Связанный каталог» можно получить доступ к связанному с этим рабочим процессом каталогу.
- Нажмите кнопку **Присоединить к домену**, чтобы присоединить соединитель к определенному домену Active Directory. Например, при настройке проверки подлинности с помощью Kerberos необходимо присоединиться к домену Active Directory, который либо содержит пользователей, либо имеет доверительные отношения с доменами, содержащими пользователей.
- При настройке каталога со встроенной проверкой подлинности Windows Active Directory соединитель присоединяется к домену в соответствии с данными конфигурации.

Соединители в кластерной среде

В распределенном развертывании vRealize Automation все доступные соединители выполняют все необходимые процедуры по авторизации пользователей, а отдельно назначенный соединитель занимается синхронизацией всех конфигураций. Как правило, синхронизация включает в себя процедуры добавления, удаления или изменения конфигураций пользователей и выполняется автоматически, если доступны все соединители. Существует ряд специфических ситуаций, когда автоматическая синхронизация может не выполняться.

Если изменения касаются конфигурации каталогов, например, базового различающегося имени, vRealize Automation попытается автоматически разослать обновления на все соединители в кластере. Если соединитель не функционирует или по какой-то причине недостижим, он не получит обновление, даже если продолжает работу в сети. Чтобы применить изменения в конфигурации к соединителям, которые не получили эти изменения автоматически, системные администраторы должны вручную сохранить эти изменения на всех соответствующих соединителях.

Если изменения касаются профилей синхронизации каталогов, vRealize Automation также попытается автоматически разослать обновления на все соединители. Если соединитель синхронизации функционирует, обновление сохраняется и рассылается всем доступным соединителям авторизации. Если один или несколько соединителей недостижимы, системный администратор получит предупреждение о том, что не все соединители были обновлены. Если соединитель синхронизации не функционирует,

обновление не выполняется и возникает ошибка. Если системный администратор изменяет соединитель, работавший в качестве соединителя синхронизации, на другой, то новый соединитель синхронизации получает самую актуальную информацию о профилях и отправляет эту информацию всем соответствующим доступным соединителям.

Присоединение компьютера соединителя к домену

В некоторых случаях может понадобиться присоединить к домену компьютер, на котором содержится соединитель управления каталогами.

После создания каталогов Active Directory через LDAP можно выполнить присоединение к домену. Для каталогов Active Directory (со встроенной проверкой подлинности Windows) соединитель автоматически присоединяется к домену при создании каталога. В обоих случаях необходимо указать соответствующие учетные данные.

Чтобы присоединиться к домену, необходимы учетные данные Active Directory с правом присоединения компьютера к домену AD. Это можно настроить в Active Directory, используя следующие права:

- Create Computer Objects
- «Создание объектов-компьютеров».

При присоединении к домену объект-компьютер создается в Active Directory в папке по умолчанию.

Если нет прав на присоединение к домену или согласно политике компании для компьютера необходимо указать настраиваемое расположение, необходимо попросить администратора создать объект компьютера, а затем присоединить компьютер соединителя к домену.

Процедура

1. Попросите администратора Active Directory создать объект-компьютер в расположении, предусмотренном политикой компании. Необходимо указать имя узла соединителя. Укажите полное доменное имя, например `server.example.com`.

Имя узла можно найти в колонке «Имя узла» на странице «Соединители» в консоли администрирования. Выберите **Администрирование > Управление каталогами > Соединители**.
2. Когда объект-компьютер будет создан, на странице «Соединители» выполните команду **Подключение к домену**, чтобы присоединить компьютер к домену, используя любую доменную учетную запись, доступную в управлении каталогами.

Выбор контроллеров домена

В службе управления каталогами хранится динамический список контроллеров домена, для которых не требуется конфигурация пользователя.

Служба управления каталогами регулярно обновляется, повторно находит контроллеры домена с помощью проверки связи LDAP, изменяет их порядок и сохраняет их в файле `domain_krb.properties` и в пользовательском файле `krb5.conf`. Наиболее подходящий контроллер домена указывается первым и используется для выполнения всех операций, таких как проверка подлинности и синхронизация. Если этот контроллер домена не отвечает в течение 10 мс, список контроллеров домена обновляется повторно. Благодаря этому служба управления каталогами всегда использует оптимальные контроллеры домена, даже в случае сбоев контроллера домена.

Управление политиками доступа

Политики Directories Management представляют собой набор правил, определяющих критерии, которым должны соответствовать пользователи для предоставления им доступа к portalу приложений или запуска указанных веб-приложений.

Можно создать правило как часть политики. Для каждого правила в политике можно указать следующие сведения.

- Диапазон сети, в котором пользователи могут входить в систему, например, внутри или снаружи корпоративной сети.
- Тип устройства, с помощью которого можно получить доступ через эту политику.
- Порядок, в котором применяются задействованные способы проверки подлинности.
- Количество часов, в течение которых проверка подлинности является действительной.
- Пользовательское сообщение об отказе в доступе.

Примечание Политики не контролируют продолжительность времени сеанса веб-приложения. Они контролируют количество времени, в течение которого пользователи должны запустить веб-приложение.

Служба Directories Management включает в себя политику по умолчанию, которую можно редактировать. Эта политика управляет доступом к службе в целом. См. раздел [Применение политики доступа по умолчанию](#). Для управления доступом к определенным веб-приложениям можно создать дополнительные политики. Политика по умолчанию применяется если не применена политика веб-приложения.

Настройка параметров политики доступа

Политика содержит одно или несколько правил доступа. Каждое правило имеет параметры, которые можно настраивать для управления доступом пользователей как к portalам приложений, так и к указанным веб-приложениям.

Диапазон сети

Для каждого правила нужно определить пользовательскую базу, указав диапазон сети. Диапазон сети состоит из одного или более диапазонов IP-адресов. Диапазоны сети создаются на вкладке «Управление учетными данными и доступом» страницы «Настройка» > «Диапазоны сети» до настройки наборов политик доступа.

Тип устройства

Выберите тип устройства, которым управляет правило. Возможны следующие типы клиентов: веб-браузер, клиентское приложение Identity Manager, iOS, Android и все типы устройств.

Добавить группы

Можно использовать различные политики проверки подлинности в зависимости от членства пользователей в различных группах. Чтобы назначить для групп пользователей конкретную процедуру проверки подлинности при входе в систему, можно добавить группы в правило политики доступа. Можете синхронизировать группы из каталога организации или локальные группы, создаваемые в консоли администрирования. Имена групп должны быть уникальными в пределах домена.

Чтобы использовать группы в правилах политики доступа, необходимо настроить новую политику на странице "Управление каталогами" > "Политики" и выбрать для нее нужные группы. Политику необходимо указать на странице «Атрибуты пользователя», а затем синхронизировать с нужным каталогом.

Если в правиле политики доступа используются группы, процедура входа пользователя изменяется. Вместо запроса на выбор пользователем домена и ввод учетных данных отображается страница с запросом на ввод уникального идентификатора. Directories Management выполняет поиск пользователя во внутренней базе данных по уникальному идентификатору и отображает страницу проверки подлинности, которая настроена в этом правиле.

Если группа не выбрана, правило политики доступа будет применяться ко всем пользователям. При настройке правил политики доступа, которые содержат правила на основе групп и правило для всех пользователей, необходимо убедиться в том, что правилом, которое назначено всем пользователям, является последнее правило в списке, приведенном в разделе политики «Правила политики».

Дополнительные сведения о применении правил для пользователей см. в документации VMware Identity Manager по входу в систему с использованием уникального идентификатора.

Способы проверки подлинности

Установите приоритет способов проверки подлинности для правила политики. Способы проверки подлинности применяются в порядке их перечисления. Выбираются первые экземпляры поставщика удостоверений, соответствующие способу проверки подлинности, и конфигурация диапазона сети в выбранной политике; запрос проверки подлинности пользователя перенаправляется в экземпляр поставщика удостоверений для проверки подлинности. Если проверка подлинности завершается ошибкой, выбирается следующий способ проверки подлинности по списку. Если используется проверка подлинности с помощью сертификата, этот способ должен быть первым в списке способом проверки подлинности.

Можно настроить правила политики доступа, которые потребуют, чтобы пользователи передавали учетные данные, используя два способа проверки подлинности, прежде чем они могут войти в систему. Если один или оба способа проверки подлинности завершаются отказом и настроены резервные способы, пользователям будет предложено ввести свои учетные данные для следующих настроенных способов проверки подлинности. Следующие два сценария описывают возможные цепочки процессов проверки подлинности.

- В первом сценарии правило политики доступа настроено на требование проверки подлинности пользователей с использованием их паролей и учетных данных Kerberos. Резервная проверка

подлинности настроена на запрос пароля и учетных данных RADIUS для проверки подлинности. Пользователь вводит правильный пароль, но не вводит правильные учетные данные Kerberos для проверки подлинности. Так как пользователь ввел правильный пароль, резервная проверка подлинности запрашивает только учетные данные RADIUS. Пользователю не нужно повторно вводить пароль.

- Во втором сценарии правило политики доступа настроено на требование проверки подлинности пользователей с использованием их паролей и учетных данных Kerberos. Резервная проверка подлинности настроена на требование RSA SecurID и RADIUS для проверки подлинности. Пользователь вводит правильный пароль, но не вводит правильные учетные данные Kerberos для проверки подлинности. Резервная проверка подлинности настроена на запрос как учетных данных RSA SecurID, так и учетных данных RADIUS для проверки подлинности.

Длительность сеанса проверки подлинности

Для каждого правила устанавливается период времени, в течение которого проверка подлинности является действительной. Значение определяет максимальное количество времени, которое есть у пользователей с момента последнего события проверки подлинности для доступа на портал или запуска определенного веб-приложения. Например, если установлено значение 4 в правиле веб-приложения, то пользователям предоставляется четыре часа, чтобы запустить веб-приложение, пока они не инициировали еще одно событие проверки подлинности, увеличивающее время сеанса.

Пользовательское сообщение об ошибке типа «отказ в доступе»

Если пользователь пытается войти в систему и ему это не удастся из-за недействительных учетных данных, неправильной конфигурации или системной ошибки, появляется сообщение об отказе в доступе. Сообщение по умолчанию:

«В доступе отказано, поскольку не был найден ни один действительный метод проверки подлинности».

Можно создать пользовательское сообщение об ошибке для каждого правила политики доступа, которое переопределяет сообщение по умолчанию. Пользовательское сообщение может включать текст и ссылку на сообщение с призывом к действию. Например, если пользователь пытается войти с незарегистрированного устройства, в правилах политики для мобильных устройств, которыми нужно управлять, может появиться следующее пользовательское сообщение об ошибке:

«Щелкните ссылку в конце данного сообщения и зарегистрируйте устройство, чтобы получить доступ к корпоративным ресурсам. Если устройство уже зарегистрировано, обратитесь в службу поддержки».

Пример политики по умолчанию

Следующая политика служит примером настройки политики по умолчанию для управления доступом к portalу приложений. См. раздел [Управление политикой доступа пользователей](#).

Правила политики оцениваются в указанном порядке. Можно изменить порядок политики путем перетаскивания правила в разделе «Правила политики».

В следующем примере использования данная политика применяется ко всем приложениям.

Имя политики default_access_policy_set ПОЛИТИКА ПО УМОЛЧАНИЮ

Описание Default access policy set

Распространяется на Все приложения

Правила политики

Можно создать список правил для доступа к данным веб-приложениям. Для каждого правила необходимо указать диапазон IP-сети, тип устройств, которым разрешен доступ к соответствующим приложениям, методы и порядок проверки подлинности и максимальное время использования приложения (в часах), после которого пользователям необходимо пройти повторную проверку подлинности.

Сетевые диапазоны	Тип устройств	Метод проверки подлинности	Интервал повторной проверки подлинности	
ВСЕ ДИАПАЗОНЫ	Веб-браузер	Password	8 ч.	✗ +
ВСЕ ДИАПАЗОНЫ	Клиент Identity Manager	Password	2160 ч.	✗ +

- Для внутренней сети (внутренний диапазон сети) для правила настроены два способа проверки подлинности: с помощью Kerberos и с помощью пароля в качестве резервного способа. Для доступа к portalу приложений из внутренней сети служба сначала пытается проверить подлинность пользователей с помощью Kerberos, так как этот способ проверки подлинности указан в правиле первым по списку. Если это не удастся, пользователям предлагается ввести свой пароль в Active Directory. Пользователи, используя браузер, входят в систему и получают доступ к своим portalам на период восьмичасового сеанса.
 - Для доступа из внешней сети (все диапазоны) настроен только один способ проверки подлинности — RSA SecurID. Для доступа к portalу приложений из внешней сети пользователи должны войти с помощью SecurID. Пользователи, используя браузер, входят в систему и получают доступ к своим portalам приложений на период четырехчасового сеанса.
- Когда пользователь пытается получить доступ к ресурсу (за исключением веб-приложений, охватываемых исключением конкретной политики), применяется политика доступа на портал по умолчанию.

Например, время повторной проверки подлинности для таких ресурсов соответствует времени повторной проверки подлинности правила политики доступа по умолчанию. Если время сеанса для пользователя, который зайдет на портал приложений, составляет восемь часов в соответствии с правилом политики доступа по умолчанию, то когда пользователь пытается запустить ресурс во время действия сеанса, приложение запускается, не требуя от пользователя повторной проверки подлинности.

Настройте политику доступа на основе групп

Можно настроить политику доступа на основе групп, чтобы управлять правами входа в систему в зависимости от членства в группах.

Управление каталогами содержит политики доступа по умолчанию, которые поддерживают все группы и все сетевые диапазоны. Можно изменять эти политики, чтобы установить более строгие ограничения, или создавать новые политики, если политик входа в систему должно быть несколько.

Процедура

- Добавьте группы в требуемую политику.
 - Выберите **Администрирование > Управление каталогами > Политики**.
 - Можно открыть политику доступа по умолчанию или создать новую.

- в) Измените правило политики, в котором в качестве типа устройства указан веб-браузер.

Чтобы изменить политику, нажмите ее метод проверки подлинности. По умолчанию существуют два правила политики, которые применяются для всех IP-адресов и всех пользователей.

Откроется страница изменения правила выбранной политики. В правиле политики можно изменять различные параметры, такие как сетевой диапазон, тип устройства, методы проверки подлинности и т.д.

- г) Нажмите **Изменить группы** на странице «Изменить правило политики», чтобы просмотреть список групп, для которых можно использовать эту политику.

На этой странице отображаются все группы, связанные с данным арендатором.

- д) Выберите группы, которые необходимо связать с данной политикой.

- е) Нажмите кнопку **ОК**.

Выбранные группы отображаются на странице «Изменить правило политики».

- ж) Нажмите кнопку **ОК** на странице «Изменить правило политики», чтобы сохранить изменения данного правила.

Появится страница «Политики» с указанием количества групп, выбранных для данной политики.

- з) На странице «Политики» нажмите кнопку **Сохранить**.

2. Настройте сетевой диапазон для данной групповой политики.

- а) Выберите **Администрирование > Управление каталогами > Сетевые диапазоны**.

По умолчанию предварительно определяется значение **All Ranges**, которое включает все IP-адреса для всех сетевых диапазонов. Можно создать новый сетевой диапазон или изменить один из существующих.

- б) Нажмите **Добавить сетевой диапазон**.

Откроется страница «Изменить сетевой диапазон».

- в) Введите **Имя** для нового сетевого диапазона и при необходимости добавьте **Описание**.

Результаты

При входе vRealize Automation необходимо выбрать домен и ввести допустимое имя пользователя и пароль. Если группа указана в соответствующей политике, соответствующие ей пользователи все равно должны вводить имя пользователя и пароль.

Управление политиками веб-приложений

При добавлении веб-приложений в каталог можно создать особые политики доступа для веб-приложения. Например, можно создать политику с правилами для веб-приложения, задающую IP-адреса, которые имеют доступ к приложению, используемые способы проверки подлинности и период повторного запроса проверки подлинности.

Следующая политика только для веб-приложений представляет собой пример политики, которую можно создавать для управления доступом к определенным веб-приложениям.

Пример 1. Строгая политика только для веб-приложений

В этом примере создается новая политика и применяется к веб-приложению особой категории.

The screenshot shows the configuration page for a policy named "Sensitive Web Application". At the top, there is a description: "To be applied to Web application that should have limited access." and a red button labeled "Удалить политику" (Delete policy). Below this, there are fields for "Имя политики" (Policy name) and "Описание" (Description), both containing the same text as the title. Under the "Распространяется на" (Applies to) section, a list of applications is shown, including "AirWatch" and "Content Locker", with a button "Изменить приложения" (Change applications). The "Правила политики" (Policy rules) section contains a table with two rules. The first rule is for "Internal Network" with a "Веб-браузер" (Web browser) type, using "Kerberos" authentication, with an interval of 8 hours. The second rule is for "ВСЕ ДИАПАЗОНЫ" (All ranges) with a "Веб-браузер" type, using "SecurID" authentication, with an interval of 4 hours. Both rules have a "Все пользователи" (All users) group. At the bottom, there are "Сохранить" (Save) and "Отмена" (Cancel) buttons.

Сетевые диапа...	Тип устройств	Метод проверки...	Интервал повт...	Группы
Internal Network	Веб-браузер	Сначала используйте: Kerberos и еще 1 возврата(-ов) в основную среду...	8 ч	Все пользователи
ВСЕ ДИАПАЗОНЫ	Веб-браузер	SecurID	4 ч	Все пользователи

1. Для доступа к услуге за пределами корпоративной сети пользователь должен войти в систему с использованием RSA SecurID. Пользователь входит в систему с помощью браузера и получает доступ к portalу приложений на протяжении четырехчасового сеанса, что предусмотрено правилом доступа по умолчанию.
2. По истечении четырех часов, пользователь пытается запустить веб-приложение, к которому применен набор политик для веб-приложений особой категории.
3. Служба проверяет правила в политике и применяет политику для диапазона сети ВСЕ ДИАПАЗОНЫ, так как запрос пользователя приходит из веб-браузера и диапазона сети ВСЕ ДИАПАЗОНЫ.

Пользователь входит в систему с использованием способа проверки подлинности RSA SecurID, однако время сеанса только что истекло. Пользователь перенаправляется для повторной проверки подлинности. После повторной проверки подлинности пользователю предоставляется еще один сеанс на четыре часа и возможность запуска приложения. В течение следующих четырех часов пользователь может продолжать запускать приложение без повторной проверки подлинности.

Пример 2. Более строгая политика только для веб-приложений

Чтобы применить более строгое правило к веб-приложениям очень высокой важности, можно потребовать проведение повторной проверки подлинности с использованием SecureID на любом устройстве по истечении 1 часа. Ниже приведен пример того, как реализуются правила политики доступа, относящиеся к этому типу.

1. Пользователь входит в систему внутри корпоративной сети, используя проверку подлинности с помощью пароля.

После этого пользователь имеет доступ к portalу приложений на протяжении восьми часов (в соответствии с тем, что задано в примере 1).

2. Пользователь сразу же пытается запустить веб-приложение, к которому применено правило политики из примера 2, которое требует проверки подлинности с помощью RSA SecurID.
3. Пользователь перенаправляется к поставщику удостоверений, который обеспечивает проверку подлинности с помощью RSA SecurID.
4. После того как пользователь успешно входит в систему, служба запускает приложение и сохраняет событие проверки подлинности.

Пользователь может продолжать запускать это приложение в течение одного часа, но по истечении этого времени будет запрошена повторная проверка подлинности, как это задано правилом политики.

Управление политикой доступа пользователей

vRealize Automation поставляется с политикой доступа пользователей по умолчанию, которую можно использовать в готовом виде или редактировать по мере необходимости, чтобы управлять доступом арендатора к приложениям.

vRealize Automation поставляется с политикой доступа пользователей по умолчанию, а новые политики добавлять нельзя. Существующую политику можно редактировать, чтобы добавлять правила.

Необходимые условия

- Выберите или настройте соответствующих поставщиков удостоверений для развертывания. См. [Настройка подключения стороннего поставщика удостоверений](#).
- Настройте соответствующие сетевые диапазоны для развертывания. См. [Добавление или изменение сетевого диапазона](#).
- Настройте соответствующие методы проверки подлинности для развертывания. См. [Интеграция альтернативных продуктов для проверки подлинности пользователей с управлением каталогами](#).
- Если вы планируете отредактировать политику по умолчанию (для управления доступом пользователей к службе в целом), настройте ее до того, как создать специальную политику для веб-приложения.
- Добавьте веб-приложения в каталог. Веб-приложения должны быть перечислены на странице «Каталог» до того, как можно будет добавить политику.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Политики**.
2. Щелкните **Изменить политику** для добавления новой политики.
3. Добавьте имя и описание политики в соответствующих текстовых полях.
4. В разделе «Применимо к» щелкните **Выбрать**. Появляется страница, на которой следует выбрать веб-приложения, связанные с этой политикой.

5. В разделе «Правила политики» щелкните **+** для добавления правила.

Появляется страница «Добавить правило политики».

- а) Выберите сетевой диапазон, который будет применен к этому правилу.
- б) Выберите тип устройства, которое может получать доступ к веб-приложениям для этого правила.
- в) Выберите методы проверки подлинности для использования в заданном порядке.
- г) Укажите продолжительность (в часах) открытого сеанса веб-приложения.
- д) Нажмите кнопку **Сохранить**.

6. Настройте необходимые дополнительные правила.

7. Нажмите кнопку **Сохранить**.

Настройка подключений дополнительных поставщиков удостоверений

Можно настроить подключения дополнительных поставщиков удостоверений, необходимые для поддержки сценариев управления различными удостоверениями, включая дополнительных встроенных и сторонних поставщиков удостоверений.

Можно создать три типа подключений поставщиков удостоверений с помощью управления каталогами.

- Создание стороннего поставщика удостоверений. Используйте этот элемент для создания подключения к внешнему стороннему поставщику удостоверений. Проверьте наличие следующих сведений перед добавлением экземпляра стороннего поставщика удостоверений.
 - Убедитесь, что сторонние экземпляры совместимы с SAML 2.0 и что служба может подключиться к стороннему экземпляру.
 - Получите соответствующие сведения о метаданных сторонних производителей, которые следует добавить при настройке поставщика удостоверений на консоли администрирования. Сведениями о метаданных, которые вы получаете из стороннего экземпляра, является URL-адрес метаданных или сами метаданные.
- Создание поставщика удостоверений рабочей области. При включении соединителя для проверки подлинности пользователей во время настройки управления каталогами в качестве поставщика удостоверений создается поставщик удостоверений рабочей области и включается проверка подлинности с помощью пароля. Можно настроить дополнительных поставщиков удостоверений рабочей области за пределами различных подсистем балансировки нагрузки.
- Создание встроенного поставщика удостоверений. Встроенные поставщики удостоверений используют внутренние механизмы управления каталогами для поддержки проверки подлинности. Можно

настроить встроенных поставщиков удостоверений для использования методов проверки подлинности, не требующих использования на локальном соединителе. Настройка встроенного поставщика подразумевает привязку методов проверки подлинности, которые будут использоваться для данного поставщика.

- **Настройка подключения стороннего поставщика удостоверений**

vRealize Automation поставляется с экземпляром подключения поставщика удостоверений по умолчанию. Пользователям может потребоваться создать дополнительные подключения поставщиков удостоверений для выполнения моментальной регистрации пользователей или настройки других пользовательских параметров.

- **Настройка дополнительных поставщиков удостоверений рабочей области**

При настройке соединителя управления каталогами для проверки подлинности пользователей, создается поставщик удостоверений рабочей области и включается проверка подлинности с помощью пароля.

- **Настройка подключения встроенных поставщиков удостоверений**

Можно настроить несколько встроенных поставщиков удостоверений и назначить для них методы проверки подлинности.

Настройка подключения стороннего поставщика удостоверений

vRealize Automation поставляется с экземпляром подключения поставщика удостоверений по умолчанию. Пользователям может потребоваться создать дополнительные подключения поставщиков удостоверений для выполнения моментальной регистрации пользователей или настройки других пользовательских параметров.

vRealize Automation поставляется с поставщиком удостоверений по умолчанию. В большинстве случаев для удовлетворения потребностей заказчика достаточно иметь поставщика удостоверений по умолчанию. Однако при использовании существующего корпоративного решения по управлению учетными данными можно настроить специального поставщика удостоверений для перенаправления пользователей в существующее решение.

Если используется пользовательский поставщик удостоверений, то функция управления каталогами будет использовать метаданные SAML, предоставленные поставщиком, чтобы установить с ним отношения доверия. После установления отношений доверия функция управления каталогами сопоставляет пользователей из утверждения SAML со списком внутренних пользователей vRealize Automation по идентификаторам имен субъектов.

Необходимые условия

- Настройте сетевые диапазоны, которые требуется направлять в этот экземпляр поставщика удостоверений для проверки подлинности. См. раздел [Добавление или изменение сетевого диапазона](#).
- Получите доступ к документу с метаданными стороннего поставщика. Это может быть URL-адрес метаданных или фактические метаданные.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

На этой странице отображаются все настроенные поставщики удостоверений.

2. Щелкните **Добавить поставщика удостоверений**.

Откроется меню с параметрами поставщика удостоверений.

3. Выберите **Создать стороннего поставщика удостоверений**.

4. Введите соответствующие сведения для настройки поставщика удостоверений.

Параметр	Описание
Имя поставщика удостоверений	Введите имя этого экземпляра поставщика удостоверений.
Метаданные SAML	<p>Добавьте XML-документ с метаданными сторонних поставщиков удостоверений для установления отношения доверия с поставщиком удостоверений.</p> <ol style="list-style-type: none"> 1 Введите в текстовое поле URL-адрес метаданных SAML или xml-содержимое. 2 Щелкните Обработать метаданные пост. удост. Форматы идентификаторов имен, поддерживаемые поставщиком удостоверений, извлекаются из метаданных и добавляются в таблицу «Форматы идентификаторов имен». 3 В столбце значений идентификаторов имен выберите атрибут пользователя в службе для сопоставления с отображаемыми форматами идентификаторов. Можно добавлять настраиваемые форматы идентификаторов имен сторонних производителей и сопоставлять их со значениями атрибутов пользователей в службе. 4 (Необязательно) Выберите формат строки идентификатора ответа NameIDPolicy.
Пользователи	Выберите каталоги пользователей Directories Management, которые могут проходить проверку подлинности с помощью этого поставщика удостоверений.
Моментальная регистрация пользователей	<p>Выберите соответствующие параметры для выполнения моментальной регистрации пользователей с использованием соответствующего стороннего поставщика удостоверений.</p> <p>Введите Имя каталога для моментальной регистрации.</p> <p>Введите один или несколько доменов, существующих в системе внешнего поставщика удостоверений, который будет использоваться для моментальной регистрации.</p>
Сеть	<p>Перечисляются существующие сетевые диапазоны, настроенные в службе.</p> <p>Выберите сетевые диапазоны для пользователей на основе их IP-адресов, которые вы хотите направлять в этот экземпляр поставщика удостоверений для проверки подлинности.</p>
Способы проверки подлинности	Добавьте способы проверки подлинности, поддерживаемые сторонним поставщиком удостоверений. Выберите класс контекста проверки подлинности SAML, который поддерживает соответствующий способ проверки подлинности.
Сертификат подписи SAML	Щелкните Метаданные поставщика услуг (SP) , чтобы увидеть URL-адрес для метаданных поставщика услуг SAML Directories Management. Скопируйте и сохраните URL-адрес. Этот URL-адрес указывается при редактировании оператора контроля SAML в стороннем поставщике удостоверений для сопоставления с пользователями Directories Management.
Hostname	Если отображается поле Hostname , введите имя узла, куда перенаправляется поставщик удостоверений для проверки подлинности. Если используется нестандартный порт, отличный от 443, его можно указать как Hostname:Port. Например, myco.example.com:8443.

5. Нажмите кнопку **Добавить**.

Следующие шаги

- Скопируйте и сохраните метаданные поставщика услуг Directories Management, которые требуются для настройки экземпляра стороннего поставщика удостоверений. Это метаданные доступны в разделе «Сертификат подписи SAML» на странице «Поставщик удостоверений».
- Добавьте метод проверки подлинности поставщика удостоверений в политику служб по умолчанию.

Сведения о добавлении и настройке ресурсов, добавляемых в каталог, см. в руководстве *Настройка ресурсов в Directories Management*.

Настройка дополнительных поставщиков удостоверений рабочей области

При настройке соединителя управления каталогами для проверки подлинности пользователей, создается поставщик удостоверений рабочей области и включается проверка подлинности с помощью пароля.

Можно настроить дополнительные соединители для работы за пределами нескольких подсистем балансировки нагрузки. Если в развертывании находится несколько подсистем балансировки нагрузки, в конфигурации каждой подсистемы балансировки нагрузки можно настроить дополнительных поставщиков удостоверений рабочей области для проверки подлинности.

Процедура

1. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

На этой странице отображаются все настроенные поставщики удостоверений.

2. Щелкните **Добавить поставщика удостоверений**.

Откроется меню с параметрами поставщика удостоверений.

3. Выберите **Создать поставщика удостоверений рабочей области**.

4. Введите соответствующие сведения для настройки поставщика удостоверений.

Параметр	Описание
Имя поставщика удостоверений	Введите имя экземпляра встроенного поставщика удостоверений.
Пользователи	Выберите пользователей для проверки подлинности. Отобразится список настроенных каталогов.
Пользователи	Выберите группу пользователей, которые могут проходить проверку подлинности с помощью этого поставщика удостоверений.
Сеть	Перечисляются существующие сетевые диапазоны, настроенные в службе. Выберите диапазон сетевых адресов для пользователей на основе IP-адресов, трафик с которых необходимо направлять в этот экземпляр поставщика удостоверений для проверки подлинности.
Способы проверки подлинности	Отобразятся методы проверки подлинности, которые настроены в службе. Установите флажок для методов проверки подлинности, которые необходимо назначить для поставщика удостоверений. Для совместимости устройств и пароля с AirWatch и соединителя этот параметр должен быть включен на странице конфигурации AirWatch.

5. Нажмите кнопку **Добавить**.

Настройка подключения встроенных поставщиков удостоверений

Можно настроить несколько встроенных поставщиков удостоверений и назначить для них методы проверки подлинности.

Необходимые условия

Если используется встроенная проверка подлинности Kerberos, загрузите сертификат издателя KDC, который будет использоваться в конфигурации AirWatch профиля управления устройствами iOS.

Процедура

1. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

На этой странице отображаются все настроенные поставщики удостоверений.

2. Щелкните **Добавить поставщика удостоверений**.

Откроется меню с параметрами поставщика удостоверений.

3. Выберите **Создать встроенного поставщика удостоверений**.

4. Введите соответствующие сведения для настройки поставщика удостоверений.

Параметр	Описание
Имя поставщика удостоверений	Введите имя экземпляра встроенного поставщика удостоверений.
Пользователи	Выберите пользователей для проверки подлинности. Отобразится список настроенных каталогов.
Сеть	Перечисляются существующие сетевые диапазоны, настроенные в службе. Выберите диапазон сетевых адресов для пользователей на основе IP-адресов, трафик с которых необходимо направлять в этот экземпляр поставщика удостоверений для проверки подлинности.
Способы проверки подлинности	Отобразятся методы проверки подлинности, которые настроены в службе. Установите флажок для методов проверки подлинности, которые необходимо назначить для поставщика удостоверений. Для совместимости устройств и пароля с AirWatch и соединителя соответствующий параметр должен быть включен на странице конфигурации AirWatch.

5. Нажмите кнопку **Добавить**.

Интеграция альтернативных продуктов для проверки подлинности пользователей с управлением каталогами

Как правило, при начальной настройке модуля управления каталогами используются соединители, поставляемые вместе с существующей инфраструктурой vRealize Automation, чтобы создать соединение Active Directory для проверки подлинности с помощью идентификатора пользователя и пароля, а также для управления ими. С другой стороны, модуль управления каталогами можно интегрировать с другими решениями для проверки подлинности, например Kerberos или RSA SecurID.

Экземпляром поставщика удостоверений может быть экземпляр Directories Managementсоединитель, экземпляр стороннего поставщика удостоверений или их комбинация.

Экземпляр поставщика удостоверений, который используется с помощью службы Directories Management, создает сетевой центр федерации, который обменивается данными со службой с помощью подтверждений SAML 2.0.

При первоначальном развертывании службы Directories Management соединитель является первоначальным поставщиком удостоверений для службы. Существующая инфраструктура Active Directory используется для проверки подлинности пользователей и управления.

Поддерживаются следующие способы проверки подлинности. Данные способы проверки подлинности можно включить в консоли администрирования.

Таблица 2-8. Типы проверки подлинности пользователей, поддерживаемые модулем управления каталогами

Типы проверки подлинности	Описание
Пароль (локальное развертывание)	Directories Management поддерживает проверку подлинности с помощью пароля Active Directory без дополнительной конфигурации. Это способ проверки подлинности пользователей непосредственно из Active Directory.
Kerberos для настольных компьютеров	Проверка подлинности Kerberos предоставляет пользователям домена доступ с выполнением единого входа к порталам их приложений. Пользователям не требуется еще раз выполнять вход после выполнения входа в сеть.
Сертификат (локальное развертывание)	<p>Чтобы проверять подлинность клиентов с помощью сертификатов на настольных компьютерах и мобильных устройствах или использовать адаптеры смарт-карт для проверки подлинности, может быть настроена проверка подлинности на основе сертификата.</p> <p>Проверка подлинности на основе сертификата базируется на сведениях, которые есть у пользователя и которые ему известны. Сертификат X.509 использует стандарт открытой инфраструктуры ключей для проверки того, что публичный ключ, который содержится в сертификате, принадлежит пользователю.</p>
RSA SecurID (локальное развертывание)	После настройки проверки подлинности с помощью RSA SecurID компонент Directories Management настраивается в качестве агента проверки подлинности на сервере RSA SecurID. Для проверки подлинности с помощью RSA SecurID требуется, чтобы пользователи использовали систему проверки подлинности на основе маркеров. RSA SecurID является способом проверки подлинности для пользователей, получающих доступ к Directories Management за пределами корпоративной сети.
RADIUS (локальное развертывание)	Проверка подлинности с помощью RADIUS предоставляет варианты двухуровневой проверки подлинности. Необходимо настроить сервер RADIUS, доступный службе Directories Management. Когда пользователи входят в систему с помощью имени пользователя и пароля, для проверки подлинности на сервер RADIUS отправляется запрос на доступ.
Адаптивная проверка подлинности RSA (локальное развертывание)	Проверка подлинности RSA обеспечивает более надежную многоуровневую проверку подлинности, чем проверка подлинности с использованием только имени пользователя и пароля из Active Directory. Если включена адаптивная проверка подлинности RSA, показатели риска, указанные в политике рисков, настраиваются в приложении управления политикой RSA. Настройка службы адаптивной проверки подлинности Directories Management используется для определения требуемых сообщений о проверке подлинности.

Таблица 2-8. Типы проверки подлинности пользователей, поддерживаемые модулем управления каталогами (продолжение)

Типы проверки подлинности	Описание
Mobile SSO (для ОС iOS)	Mobile SSO для проверки подлинности в ОС iOS используется для проверки подлинности с выполнением единого входа для устройств iOS под управлением AirWatch. Проверка подлинности Mobile SSO (для ОС iOS) использует центр распределения ключей (Key Distribution Center, KDC), который является частью службы Directories Management. Необходимо активировать службу KDC в службе VMware Identity Manager перед включением этого способа проверки подлинности.
Mobile SSO (для ОС Android)	Mobile SSO для проверки подлинности в ОС Android используется для проверки подлинности с выполнением единого входа для устройств Android под управлением AirWatch. Прокси-служба настраивается между службой Directories Management и AirWatch для получения сертификата от AirWatch для проверки подлинности.
Пароль (AirWatch Connector)	Приложение AirWatch Cloud Connector можно интегрировать в службу Directories Management для проверки подлинности пароля пользователя. Служба Directories Management настраивается для синхронизации пользователей из каталога AirWatch.

Проверка подлинности пользователей выполняется на основе настроенных способов проверки подлинности, правил политики доступа по умолчанию, сетевых диапазонов и экземпляра поставщика удостоверений. После настройки способов проверки подлинности создаются правила политики доступа, в которых указывается, какие способы проверки подлинности используются в зависимости от типа устройства.

■ [Настройка SecurID для Directories Management](#)

При настройке сервера RSA SecurID необходимо добавить данные о службах Directories Management как агенте проверки подлинности на сервере RSA SecurID и настроить сведения о сервере RSA SecurID в службе Directories Management.

■ [Настройка RADIUS для Directories Management](#)

Directories Management можно настроить так, чтобы пользователи были обязаны использовать проверку подлинности с помощью RADIUS. Вы настраиваете сведения о сервере RADIUS в службе Directories Management.

■ [Настройка сертификата или адаптера смарт-карты для использования со службой управления каталогами.](#)

Вы можете настроить проверку подлинности сертификатов x509, чтобы клиенты могли проверять подлинность с помощью сертификатов на своих компьютерах и мобильных устройствах или использовать адаптеры смарт-карт для проверки подлинности. Проверка подлинности на базе сертификатов основана на том, что имеет пользователь (закрытый ключ или смарт-карту) и что знает человек (пароль для закрытого ключа или ПИН-код для смарт-карты). Сертификат X.509 использует стандарт инфраструктуры открытых ключей (PKI) для проверки того, что открытый ключ, который находится внутри сертификата, принадлежит пользователю. В случае проверки подлинности с помощью смарт-карты пользователь подключает смарт-карту к компьютеру и вводит ПИН-код.

- **Настройка экземпляра стороннего поставщика удостоверений для проверки подлинности пользователей**

Стороннего поставщика удостоверений можно настроить таким образом, чтобы использовать его для проверки подлинности пользователей в службе Directories Management.

- **Управление способами проверки подлинности, применяемыми для пользователей**

Служба Directories Management пытается проверить подлинность пользователей, используя настроенные способы проверки подлинности, политики доступа по умолчанию, сетевые диапазоны и экземпляры поставщика удостоверений.

- **Настройка Kerberos для Directories Management**

Проверка подлинности с помощью Kerberos позволяет пользователям, которые успешно вошли в свой домен Active Directory, получать доступ к portalу приложений без дополнительных запросов учетных данных. Во время проверки подлинности Windows обеспечивается применение протокола Kerberos для защиты передачи данных между браузерами пользователей и службой Directories Management. Чтобы реализовать функцию Kerberos для своего развертывания, саму службу Active Directory настраивать не нужно.

Настройка SecurID для Directories Management

При настройке сервера RSA SecurID необходимо добавить данные о службах Directories Management как агенте проверки подлинности на сервере RSA SecurID и настроить сведения о сервере RSA SecurID в службе Directories Management.

При настройке SecurID для обеспечения дополнительной безопасности необходимо убедиться, что сеть правильно настроена для развертывания Directories Management. В частности, для SecurID следует убедиться, что соответствующий порт открыт, благодаря чему SecurID может проверять подлинность пользователей за пределами вашей сети.

После запуска мастера установки Directories Management и настройки подключения Active Directory у вас будут данные, необходимые для подготовки сервера RSA SecurID. После подготовки сервера RSA SecurID для Directories Management выключите SecurID на консоли администрирования.

- **Подготовка сервера RSA SecurID**

Сервер RSA SecurID должен быть настроен с информацией об устройстве Directories Management как агенте проверки подлинности. Требуются такие данные как имя узла и IP-адреса для сетевых интерфейсов.

- **Настройка проверки подлинности с помощью RSA SecurID**

После того как модуль управления каталогами настроен как агент проверки подлинности на сервере RSA SecurID, в соединитель необходимо добавить сведения о конфигурации RSA SecurID.

Подготовка сервера RSA SecurID

Сервер RSA SecurID должен быть настроен с информацией об устройстве Directories Management как агенте проверки подлинности. Требуются такие данные как имя узла и IP-адреса для сетевых интерфейсов.

Необходимые условия

- Убедитесь, что в корпоративной сети установлена и функционирует одна из следующих версий диспетчера проверки подлинности RSA: RSA AM 6.1.2, 7.1 SP2 и более поздние версии, а также 8.0 и более поздние версии. Сервер Directories Management использует AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), который поддерживает только предыдущие версии диспетчера проверки подлинности RSA (сервер RSA SecurID). Сведения об установке и настройке диспетчера проверки подлинности RSA (сервера RSA SecurID) см. в документации по RSA.

Процедура

1. В поддерживаемой версии сервера RSA SecurID в качестве агента проверки подлинности добавьте Directories Management Connector. Введите следующие данные.

Параметр	Описание
Имя узла	Имя узла для Directories Management.
IP-адрес	IP-адрес для Directories Management.
Альтернативный IP-адрес	Если трафик из соединителя проходит через устройство преобразования сетевых адресов (NAT), чтобы попасть на сервер RSA SecurID, введите частный IP-адрес этого устройства.

2. Загрузите сжатый файл конфигурации и извлеките файл `sdconf.rec`.

Будьте готовы передать этот файл позже при настройке RSA SecurID в Directories Management.

Следующие шаги

Перейдите на консоль администрирования и на вкладке «Управление учетными данными и доступом» на странице настройки выберите соединитель, а на странице «AuthAdapters» настройте SecurID.

Настройка проверки подлинности с помощью RSA SecurID

После того как модуль управления каталогами настроен как агент проверки подлинности на сервере RSA SecurID, в соединитель необходимо добавить сведения о конфигурации RSA SecurID.

Необходимые условия

- Убедитесь, что диспетчер проверки подлинности RSA (сервер RSA SecurID) установлен и правильно настроен.
- Загрузите сжатый файл с сервера RSA SecurID и распакуйте файл конфигурации сервера.

Процедура

1. В качестве администратора арендатора выберите **Администрирование > Управление каталогами > Соединители**
2. На странице «Соединители» выберите ссылку «Рабочий процесс» для соединителя, настраиваемого для RSA SecurID.

3. Нажмите **Адаптеры проверки подлинности**, а затем нажмите **SecurIDIdpAdapter**.

Вы будете перенаправлены на страницу входа диспетчера удостоверений.

4. На странице «Адаптеры проверки подлинности» выберите строку SecurIDIdpAdapter и нажмите **Изменить**.

5. Настройте страницу адаптера проверки подлинности с помощью SecurID.

При настройке параметров страницы SecurID потребуется используемая информация и файлы, созданные на сервере RSA SecurID.

Параметр	Действие
Имя	Имя должно быть задано. По умолчанию используется имя SecurIDIdpAdapter. Его можно изменить.
Включить SecurID	Установите этот флажок, чтобы включить проверку подлинности с помощью SecurID.
Разрешенное количество попыток проверки подлинности	Введите максимальное количество неудачных попыток входа в систему с использованием маркера RSA SecurID. По умолчанию дается пять попыток.
Адрес соединителя	Введите IP-адрес экземпляра соединителя. Введенное значение должно соответствовать значению, которое использовалось при добавлении устройства соединителя в качестве агента проверки подлинности на сервере RSA SecurID. Если сервер RSA SecurID имеет значение, присвоенное строке альтернативного IP-адреса, введите это значение в качестве IP-адреса соединителя. Если альтернативный IP-адрес не назначен, введите значение из строки IP-адреса.
IP-адрес агента	Введите значение, присвоенное в строке IP-адрес на сервере RSA SecurID.
Конфигурация сервера	Загрузите файл конфигурации сервера RSA SecurID. Сначала необходимо загрузить сжатый файл с сервера RSA SecurID и извлечь файл конфигурации сервера, который по умолчанию называется <code>sdconf.rec</code> .
Секретный ключ узла	Если поле для секретного ключа узла оставить незаполненным, то он будет создан автоматически. Рекомендуется очистить файл с секретным ключом узла на сервере RSA SecurID и намеренно не загружать этот файл. Убедитесь, что файлы с секретным ключом узла на сервере RSA SecurID и на экземпляре соединителя сервера совпадают. При изменении секретного ключа узла в одном месте, измените его и в другом месте.

6. Нажмите кнопку **Сохранить**.

Следующие шаги

Добавьте метод проверки подлинности в политику доступа по умолчанию. Откройте **Администрирование > Управление каталогами > Политики** и выберите **Изменить политику по умолчанию**, чтобы отредактировать правила политики по умолчанию для добавления метода проверки подлинности SecurID в правило в нужном порядке.

Настройка RADIUS для Directories Management

Directories Management можно настроить так, чтобы пользователи были обязаны использовать проверку подлинности с помощью RADIUS. Вы настраиваете сведения о сервере RADIUS в службе Directories Management.

RADIUS обеспечивает возможность применения различных альтернативных вариантов проверки подлинности на основе двухуровневых маркеров. Так как решения двухуровневой проверки подлинности, например RADIUS, работают с диспетчерами проверки подлинности, установленными на отдельных серверах, необходимо иметь настроенный сервер RADIUS, доступный для службы диспетчера удостоверений.

Когда пользователи входят на портал «Мои приложения» и проверка подлинности RADIUS включена, в браузере появляется специальное диалоговое окно входа в систему. В этом окне пользователь вводит свое имя пользователя и пароль для проверки подлинности с помощью RADIUS. Если сервер RADIUS отправляет вызов на доступ, служба диспетчера удостоверений отображает диалоговое окно, где запрашивается второй пароль. В настоящее время поддержка таких вызовов в RADIUS ограничена и заключается в запросе ввода текстовых данных.

После того как пользователь введет учетные данные в диалоговом окне, сервер RADIUS может отправить SMS-сообщение, электронное письмо или текстовое сообщение, где будет указан код, с помощью какого либо иного внешнего механизма на сотовый телефону пользователя. Пользователь может ввести этот текст и код в диалоговом окне входа в систему для завершения операции проверки подлинности.

Если сервер RADIUS позволяет импортировать пользователей из Active Directory, то перед запросом имени пользователя и пароля для проверки подлинности с помощью RADIUS конечные пользователи могут сначала получать запрос на ввод учетных данных для Active Directory.

Подготовка сервера RADIUS

Необходимо установить сервер RADIUS, а затем настроить его для принятия запросов RADIUS от службы Directories Management.

Для получения информации о настройке сервера RADIUS см. руководства по настройке поставщика RADIUS. Запишите информацию о конфигурации RADIUS, она потребуется при настройке RADIUS в службе. Чтобы узнать, какая информация RADIUS необходима для настройки Directories Management, см. [Настройка проверки подлинности RADIUS в управлении каталогами](#).

Для обеспечения высокой доступности можно настроить вторичный сервер проверки подлинности RADIUS. Если первичный сервер RADIUS не отвечает в течение времени ожидания ответа сервера, настроенного для проверки подлинности RADIUS, запрос направляется на вторичный сервер. Когда основной сервер не отвечает, вторичный сервер получает все последующие запросы проверки подлинности.

Настройка проверки подлинности RADIUS в управлении каталогами

Программное обеспечение RADIUS запускается на сервере диспетчера проверки подлинности. Для включения проверки подлинности с помощью RADIUS выполните указания, приведенные в документации по конфигурации от поставщика.

Необходимые условия

Установите и настройте программное обеспечение RADIUS на сервере диспетчера проверки подлинности. Для включения проверки подлинности с помощью RADIUS выполните указания, приведенные в документации по конфигурации от поставщика.

Чтобы настроить RADIUS в службе, необходимо знать следующую информацию о сервере RADIUS.

- IP-адрес или DNS-имя сервера RADIUS.

- Номер порта проверки подлинности. Номер порта проверки подлинности, как правило, равен 1812.
- Тип проверки подлинности. Типы проверки подлинности включают PAP (Password Authentication Protocol), CHAP (Challenge Handshake Authentication Protocol), MSCHAP1, MSCHAP2 (Microsoft Challenge Handshake Authentication Protocol, версии 1 и 2).
- Общий секретный ключ RADIUS, который используется для шифрования и расшифровки сообщений протокола RADIUS.
- Определенные значения времени ожидания и повтора, необходимые для проверки подлинности с помощью RADIUS.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Соединители**.
2. На странице «Соединители» выберите ссылку «Рабочий процесс» для соединителя, настраиваемого для проверки подлинности с помощью RADIUS.
3. Нажмите **Адаптеры проверки подлинности**, а затем нажмите **RadiusAuthAdapter**.
Вы будете перенаправлены на страницу входа диспетчера удостоверений.
4. Нажмите **Изменить** для настройки данных полей на странице адаптера проверки подлинности.

Параметр	Действие
Имя	Имя должно быть задано. По умолчанию используется имя RadiusAuthAdapter. Его можно изменить.
Включить адаптер Radius	Установите этот флажок, чтобы включить проверку подлинности с помощью RADIUS.
Разрешенное количество попыток проверки подлинности	Введите максимальное количество неудачных попыток входа в систему с помощью RADIUS. По умолчанию дается пять попыток.
Количество попыток обращения к серверу Radius	Укажите общее количество повторных попыток. Если первичный сервер не отвечает, служба ждет истечения заданного времени перед повторной попыткой.
Имя узла или адрес сервера Radius	Введите имя узла или IP-адрес сервера RADIUS.
Порт проверки подлинности	Введите номер порта проверки подлинности Radius. Он, как правило, равен 1812.
Порт учета	Введите 0 в качестве номера порта. Порт учета в настоящее время не используется.
Тип проверки подлинности	Введите протокол проверки подлинности, который поддерживается сервером RADIUS. Значение PAP, CHAP, MSCHAP1 ИЛИ MSCHAP2.

Параметр	Действие
Общий секрет	Введите общий секрет, который используется сервером RADIUS и службой VMware Identity Manager.
Время ожидания сервера в секундах	Введите время ожидания сервера RADIUS в секундах, по истечении которого отправляется повторный запрос, если сервер RADIUS не отвечает.
Префикс области	(Необязательно) Место расположения учетной записи пользователя называется «область». Если указать строку префикса области, строка помещается в начале имени пользователя при его передаче на сервер RADIUS. Например, если введено имя пользователя jdoe и указан префикс области DOMAIN-A\, на сервер RADIUS будет отправлено имя пользователя DOMAIN-A\jdoe. Если не настраивать эти поля, то будет отправляться только введенное имя пользователя.
Суффикс области	(Необязательно) Если указать суффикс области, то эта строка размещается в конце имени пользователя. Например, если указать суффикс @myco.com, на сервер RADIUS будет отправлено имя пользователя jdoe@myco.com.
Подсказка для парольной фразы на странице входа в систему	Введите текстовую строку для отображения в сообщении на странице входа, чтобы пользователи вводили правильный пароль для Radius. Например, если это поле настроено как Сначала пароль AD, затем код доступа из SMS , то сообщение на странице входа будет иметь вид: Введите пароль AD, а затем код доступа из SMS . Текстовая строка по умолчанию — Пароль RADIUS .

5. Для обеспечения высокой доступности можно задействовать дополнительный сервер RADIUS.

Настройка дополнительного сервера осуществляется, как описано в шаге 4.

6. Нажмите кнопку **Сохранить**.

Следующие шаги

Добавьте метод проверки подлинности с помощью RADIUS в политику доступа по умолчанию. Откройте **Администрирование > Управление каталогами > Политики** и выберите **Изменить политику по умолчанию**, чтобы отредактировать правила политики по умолчанию для добавления метода проверки подлинности с помощью RADIUS в правило в нужном порядке.

Настройка сертификата или адаптера смарт-карты для использования со службой управления каталогами.

Вы можете настроить проверку подлинности сертификатов x509, чтобы клиенты могли проверять подлинность с помощью сертификатов на своих компьютерах и мобильных устройствах или использовать адаптеры смарт-карт для проверки подлинности. Проверка подлинности на базе сертификатов основана на том, что имеет пользователь (закрытый ключ или смарт-карту) и что знает человек (пароль для закрытого ключа или ПИН-код для смарт-карты). Сертификат X.509 использует стандарт инфраструктуры открытых ключей (PKI) для проверки того, что открытый ключ, который находится внутри сертификата, принадлежит пользователю. В случае проверки подлинности с помощью смарт-карты пользователь подключает смарт-карту к компьютеру и вводит ПИН-код.

Сертификаты смарт-карт копируются в локальное хранилище сертификатов на компьютере пользователя. Сертификаты в локальном хранилище сертификатов доступны почти для всех браузеров на компьютере пользователя.

Примечание При настроенной проверке подлинности на основе сертификата и установленным за подсистемой балансировки нагрузки устройством службы убедитесь, что соединитель настроен на сквозное подключение SSL через подсистему балансировки нагрузки и не замыкается на нее. Эта конфигурация гарантирует, что для передачи сертификата соединителю подтверждение сеанса связи по протоколу SSL проходит между соединителем и клиентом. Можно настроить дополнительные соединители за другой подсистемой балансировки нагрузки, которая настроена с использованием сквозного подключения по SSL, а также включить и настроить проверку подлинности на основе сертификатов на этих соединителях.

Использование основного имени пользователя для проверки подлинности с помощью сертификатов

В Active Directory можно использовать сопоставление сертификатов. При входе с помощью сертификатов и смарт-карт для проверки учетных записей пользователя используется основное имя пользователя (UPN) из Active Directory. Учетные записи пользователей Active Directory, которые пытаются пройти проверку подлинности в службе Directories Management, должны иметь действительное имя UPN, соответствующее UPN в сертификате.

Можно настроить Directories Management, чтобы использовать адрес электронной почты для проверки учетной записи пользователя в том случае, если UPN в сертификате отсутствует.

Также можно включить использование альтернативного типа UPN.

Центр сертификации, необходимый для проверки подлинности

Для отслеживания проверки подлинности с помощью сертификата корневые сертификаты и промежуточные сертификаты должны быть загружены в Directories Management.

Сертификаты будут скопированы в локальное хранилище сертификатов на компьютере пользователя. Сертификаты в локальном хранилище сертификатов доступны (с некоторыми исключениями) для всех браузеров, работающих на компьютере пользователя и, следовательно, доступны экземпляру Directories Management в браузере.

Для проверки подлинности с помощью смарт-карт, когда пользователь инициирует подключение к экземпляру Directories Management, служба Directories Management отправляет в браузер список доверенных центров сертификации (ЦС). Браузер проверяет имеющиеся пользовательские сертификаты на вхождение в список доверенных центров сертификации, выбирает подходящий сертификат, а затем предлагает пользователю ввести ПИН-код смарт-карты. Если доступны несколько действительных сертификатов пользователя, браузер предлагает пользователю выбрать сертификат.

Если пользователь не может проверить подлинность, то возможно неправильно настроены корневой ЦС и промежуточный ЦС, или служба не была перезапущена после загрузки на сервер корневых и промежуточных ЦС. В таких случаях браузер не может отобразить установленные сертификаты, пользователь не может выбрать правильный сертификат, и проверка подлинности с помощью сертификата не удастся.

Использование проверки отзыва сертификатов

Чтобы пользователи с отозванными пользовательскими сертификатами не могли пройти проверку подлинности, можно настроить проверку отзыва сертификатов. Как правило, сертификаты отзываются, когда пользователь покидает организацию, теряет смарт-карту или переходит из одного отдела в другой.

Поддерживается проверка отзыва сертификатов с использованием списков отозванных сертификатов (CRL) и протокола Online Certificate Status Protocol (OCSP). Список CRL представляет собой список отозванных сертификатов, опубликованный центром сертификации, который выпустил сертификаты. OCSP — протокол проверки сертификатов, который используется для получения статуса отзыва сертификата.

При настройке проверки подлинности с использованием сертификата можно настроить проверку отзыва сертификата в консоли администрирования на странице «Соединители» > «Адаптеры проверки подлинности» > CertificateAuthAdapter.

В одной конфигурации адаптера проверки подлинности сертификата можно настроить как CRL, так и OCSP. При настройке обоих типов проверки отзыва сертификатов и установке флажка «Использовать CRL в случае отказа проверки OCSP», сначала для проверки используется OCSP, а в случае ошибки OCSP происходит возврат к проверке с помощью CRL. В случае отказа при проверке отзыва с помощью CRL, возврат к проверке с помощью OCSP не происходит.

Вход в систему с использованием проверки CRL

При включении проверки отзыва сертификата сервер Directories Management читает CRL, чтобы определить состояние отзыва сертификата пользователя.

Если сертификат отозван, проверка подлинности с его использованием завершится отказом.

Вход в систему с использованием проверки сертификатов по OCSP

При настройке проверки отзыва по протоколу состояния сертификата (OCSP), Directories Management посылает запрос к ответчику по протоколу OCSP, чтобы определить состояние отзыва сертификата определенного пользователя. Сервер Directories Management использует сертификат подписи OCSP чтобы убедиться, что ответы, которые он получает от ответчика OCSP, являются подлинными.

Если сертификат отозван, проверка подлинности завершится отказом.

Можно настроить возврат проверки подлинности к проверке CRL, если не будет получен ответ от ответчика OCSP или если ответ неверен.

Настройка проверки подлинности сертификата для управления каталогами

Вы включаете и настраиваете проверку подлинности сертификата с помощью функции управления каталогами на консоли администрирования vRealize Automation.

Примечание Системному администратору необходимо настроить внешний соединитель для развертывания vRealize Automation при использовании сторонних поставщиков удостоверений, таких как Kerberos, или проверки подлинности с помощью смарт-карты.

Необходимые условия

- Получение корневого сертификата и промежуточных сертификатов от центра сертификации (ЦС), который подписал сертификаты, представленные пользователями.

- (Необязательно) Список идентификаторов объекта (OID) с действительными политиками сертификатов для проверки подлинности с помощью сертификата.
- Расположение файла CRL и URL-адрес сервера OCSP для проверки отзыва.
- (Необязательно) Расположение файла ответа OCSP на подписание сертификата.
- Содержимое формы подтверждения, если перед проверкой подлинности требуется отображение формы подтверждения.

Процедура

1. В качестве администратора арендатора выберите **Администрирование > Управление каталогами > Соединители**
2. На странице «Соединители» выберите ссылку «Рабочий процесс» для настраиваемого соединителя.
3. Нажмите **Адаптеры проверки подлинности**, а затем нажмите **CertificateAuthAdapter**.
Вы будете перенаправлены на страницу входа диспетчера удостоверений.
4. В строке CertificateAuthAdapter нажмите **Изменить**.
5. Настройте страницу адаптера проверки подлинности с помощью сертификатов.

Примечание Звездочка обозначает обязательное поле. Все остальные поля являются необязательными.

Параметр	Описание
* Имя	Имя должно быть задано. По умолчанию используется имя CertificateAuthAdapter. Его можно изменить.
Включить адаптер сертификатов	Установите флажок, чтобы включить проверку подлинности с помощью сертификата.
* Корневые и промежуточные сертификаты ЦС	Выберите файлы сертификатов для загрузки. Вы можете выбрать несколько корневых и промежуточных сертификатов центра сертификации, зашифрованных в формате DER или PEM.
Загруженные сертификаты ЦС	<p>Загруженные файлы сертификатов перечислены в разделе «Загруженные сертификаты ЦС» формы.</p> <p>Чтобы новые сертификаты стали доступны, необходимо перезапустить службу.</p> <p>Нажмите Перезапуск веб-службы, чтобы перезапустить службу и добавить сертификаты в доверенную службу.</p> <p>Примечание При перезапуске службы проверка подлинности с помощью сертификата не включается. После перезапуска службы необходимо продолжить настройку на данной странице. При нажатии кнопки Сохранить внизу страницы будет включена проверка подлинности с помощью сертификата в службе.</p>
Использовать электронную почту при отсутствии UPN в сертификате	Если в сертификате отсутствует основное имя пользователя (UPN), то установите этот флажок, чтобы использовать атрибут EmailAddress в качестве расширения альтернативного имени субъекта для проверки учетных записей пользователей.

Параметр	Описание
Принимаемые политики сертификатов	Создайте список идентификаторов объектов, которые принимаются в расширениях политик сертификата. Введите числа идентификаторов объекта (OID) для политики выпуска сертификата. Нажмите Добавить еще одно значение , чтобы добавить дополнительные идентификаторы.
Включить отзыв сертификатов	Установите флажок, чтобы включить проверку отзыва сертификата. В этом случае пользователи, у которых отозваны сертификаты, не смогут пройти проверку подлинности.
Использовать CRL из сертификатов	Установите флажок, чтобы использовать список отзыва сертификатов (CRL), опубликованный центром сертификации, выдавшим сертификаты, для подтверждения статуса сертификата (отозван он или нет).
Расположение CRL	Введите путь к файловому серверу или локальный путь к файлу, из которого нужно извлечь CRL.
Включить отзыв OCSP	Установите флажок, чтобы использовать протокол проверки состояния сертификатов (OCSP) и получить статус отзыва сертификата.
Использовать CRL в случае отказа OCSP	Если настроить и CRL, и OCSP, то при установке этого флажка будет осуществлен возврат к использованию CRL, если проверка по OCSP недоступна.
Отправить специальный параметр OCSP	Установите флажок, чтобы отправлять в ответе уникальный идентификатор запроса OCSP.
URL-адрес OCSP	Если включен отзыв по OCSP, введите адрес сервера OCSP для проверки отзыва.
Сертификат подписи ответчика OCSP	Введите путь к сертификату OCSP для ответчика, <i>/path/to/file.cer</i> .
Включить форму подтверждения перед проверкой подлинности	Установите этот флажок, чтобы включить отображение пользователям страницы подтверждения перед входом на портал «Мои приложения» для проверки подлинности с использованием сертификата.
Содержимое формы подтверждения	Введите в этом поле текст, который будет отображаться в форме подтверждения.

6. Нажмите кнопку **Сохранить**.

Следующие шаги

- Добавьте метод проверки подлинности сертификата в политику доступа по умолчанию. Выберите **Администрирование > Управление каталогами > Политики** и щелкните **Изменить политику по умолчанию**, чтобы отредактировать правила политики по умолчанию, добавить сертификат и сделать его первым методом проверки подлинности для политики по умолчанию. Сертификат должен быть первым в списке методов проверки подлинности в правиле политики, в противном случае проверка подлинности сертификата завершится сбоем.
- При настроенной проверке подлинности с помощью сертификата и установленной за подсистемой балансировки нагрузки устройством службы убедитесь, что компонент Directories Management соединитель настроен на сквозное подключение SSL через подсистему балансировки нагрузки и SSL не замыкается на эту подсистему. Эта конфигурация гарантирует, что между соединителем и клиентом будет установлена связь по протоколу SSL для передачи сертификата соединителю.

Настройка экземпляра стороннего поставщика удостоверений для проверки подлинности пользователей

Стороннего поставщика удостоверений можно настроить таким образом, чтобы использовать его для проверки подлинности пользователей в службе Directories Management.

Перед использованием консоли администрирования для добавления экземпляра стороннего поставщика удостоверений выполните следующее.

- Убедитесь, что сторонние экземпляры совместимы с SAML 2.0 и что служба может подключиться к стороннему экземпляру.
- Получите соответствующие сведения о метаданных сторонних производителей, которые следует добавить при настройке поставщика удостоверений на консоли администрирования. Сведениями о метаданных, которые вы получаете из стороннего экземпляра, является URL-адрес метаданных или сами метаданные.

Настройка подключения стороннего поставщика удостоверений

vRealize Automation поставляется с экземпляром подключения поставщика удостоверений по умолчанию. Пользователям может потребоваться создать дополнительные подключения поставщиков удостоверений для выполнения моментальной регистрации пользователей или настройки других пользовательских параметров.

vRealize Automation поставляется с поставщиком удостоверений по умолчанию. В большинстве случаев для удовлетворения потребностей заказчика достаточно иметь поставщика удостоверений по умолчанию. Однако при использовании существующего корпоративного решения по управлению учетными данными можно настроить специального поставщика удостоверений для перенаправления пользователей в существующее решение.

Если используется пользовательский поставщик удостоверений, то функция управления каталогами будет использовать метаданные SAML, предоставленные поставщиком, чтобы установить с ним отношения доверия. После установления отношений доверия функция управления каталогами сопоставляет пользователей из утверждения SAML со списком внутренних пользователей vRealize Automation по идентификаторам имен субъектов.

Необходимые условия

- Настройте сетевые диапазоны, которые требуется направлять в этот экземпляр поставщика удостоверений для проверки подлинности. См. раздел [Добавление или изменение сетевого диапазона](#).
- Получите доступ к документу с метаданными стороннего поставщика. Это может быть URL-адрес метаданных или фактические метаданные.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

На этой странице отображаются все настроенные поставщики удостоверений.

2. Щелкните **Добавить поставщика удостоверений**.

Откроется меню с параметрами поставщика удостоверений.

3. Выберите Создать стороннего поставщика удостоверений.**4. Введите соответствующие сведения для настройки поставщика удостоверений.**

Параметр	Описание
Имя поставщика удостоверений	Введите имя этого экземпляра поставщика удостоверений.
Метаданные SAML	<p>Добавьте XML-документ с метаданными сторонних поставщиков удостоверений для установления отношения доверия с поставщиком удостоверений.</p> <ol style="list-style-type: none"> Введите в текстовое поле URL-адрес метаданных SAML или xml-содержимое. Щелкните Обработать метаданные пост. удост. Форматы идентификаторов имен, поддерживаемые поставщиком удостоверений, извлекаются из метаданных и добавляются в таблицу «Форматы идентификаторов имен». В столбце значений идентификаторов имен выберите атрибут пользователя в службе для сопоставления с отображаемыми форматами идентификаторов. Можно добавлять настраиваемые форматы идентификаторов имен сторонних производителей и сопоставлять их со значениями атрибутов пользователей в службе. (Необязательно) Выберите формат строки идентификатора ответа NameIDPolicy.
Пользователи	Выберите каталоги пользователей Directories Management, которые могут проходить проверку подлинности с помощью этого поставщика удостоверений.
Моментальная регистрация пользователей	<p>Выберите соответствующие параметры для выполнения моментальной регистрации пользователей с использованием соответствующего стороннего поставщика удостоверений.</p> <p>Введите Имя каталога для моментальной регистрации.</p> <p>Введите один или несколько доменов, существующих в системе внешнего поставщика удостоверений, который будет использоваться для моментальной регистрации.</p>
Сеть	<p>Перечисляются существующие сетевые диапазоны, настроенные в службе.</p> <p>Выберите сетевые диапазоны для пользователей на основе их IP-адресов, которые вы хотите направлять в этот экземпляр поставщика удостоверений для проверки подлинности.</p>
Способы проверки подлинности	Добавьте способы проверки подлинности, поддерживаемые сторонним поставщиком удостоверений. Выберите класс контекста проверки подлинности SAML, который поддерживает соответствующий способ проверки подлинности.
Сертификат подписи SAML	Щелкните Метаданные поставщика услуг (SP) , чтобы увидеть URL-адрес для метаданных поставщика услуг SAML Directories Management. Скопируйте и сохраните URL-адрес. Этот URL-адрес указывается при редактировании оператора контроля SAML в стороннем поставщике удостоверений для сопоставления с пользователями Directories Management.
Hostname	Если отображается поле Hostname , введите имя узла, куда перенаправляется поставщик удостоверений для проверки подлинности. Если используется нестандартный порт, отличный от 443, его можно указать как Hostname:Port. Например, myco.example.com:8443.

5. Нажмите кнопку Добавить.**Следующие шаги**

- Скопируйте и сохраните метаданные поставщика услуг Directories Management, которые требуются для настройки экземпляра стороннего поставщика удостоверений. Это метаданные доступны в разделе «Сертификат подписи SAML» на странице «Поставщик удостоверений».
- Добавьте метод проверки подлинности поставщика удостоверений в политику служб по умолчанию.

Сведения о добавлении и настройке ресурсов, добавляемых в каталог, см. в руководстве *Настройка ресурсов в Directories Management*.

Управление способами проверки подлинности, применяемыми для пользователей

Служба Directories Management пытается проверить подлинность пользователей, используя настроенные способы проверки подлинности, политики доступа по умолчанию, сетевые диапазоны и экземпляры поставщика удостоверений.

При попытке пользователя войти в систему служба оценивает правила политики доступа по умолчанию, чтобы выбрать, какие правила в политике необходимо применить. Способы проверки подлинности применяются в порядке их перечисления в правиле. Выбирается первый экземпляр поставщика удостоверений, который соответствует требованиям выбранного правила по способу проверки подлинности и сетевому диапазону, запрос проверки подлинности пользователя перенаправляется в экземпляр поставщика удостоверений. Если проверка подлинности не удастся, то применяется следующий настроенный в правиле способ проверки подлинности.

Можно добавлять правила, которые указывают способы проверки подлинности, используемые в зависимости от типа устройства без каких-либо дополнительных условий или в зависимости от типа устройства и конкретного диапазона сети. Например, можно настроить правило, которое требует, чтобы для пользователей, выполняющих вход с устройств iOS из определенной сети, выполнялась проверка подлинности с помощью RSA SecurID, и другое правило, в котором указано, что для всех типов устройств, на которых выполняется вход с IP-адреса внутренней сети, следует выполнять проверку подлинности с помощью пароля.

Добавление или изменение сетевого диапазона

Сетевыми диапазонами можно управлять, чтобы определить IP-адреса, с которых пользователи могут выполнять вход по ссылке Active Directory. Создаваемые сетевые диапазоны добавляются в конкретные экземпляры поставщика удостоверений и правила политики доступа.

Определите сетевые диапазоны для развертывания Directories Management на основе топологии вашей сети.

В качестве сетевого диапазона по умолчанию создается один диапазон с именем «ВСЕ ДИАПАЗОНЫ». Этот сетевой диапазон включает все IP-адреса, доступные в Интернете (0.0.0.0–255.255.255.255). Даже в том случае, если ваше развертывание имеет один экземпляр поставщика удостоверений, диапазон IP-адресов можно изменять и добавлять другие диапазоны, чтобы исключить или включить конкретные IP-адреса в сетевой диапазон по умолчанию. Можно создать другие сетевые диапазоны с конкретными IP-адресами, которые можно применять для специальных целей.

Примечание Сетевой диапазон по умолчанию (ВСЕ ДИАПАЗОНЫ) и его описание (сеть для всех диапазонов) можно редактировать. Вы можете изменять имя и описание, в том числе вводить текст на другом языке, щелкая имя сетевого диапазона на странице «Сетевые диапазоны».

Необходимые условия

- Вы настроили арендаторов для развертывания vRealize Automation и создали соответствующий канал связи с Active Directory для поддержки обычной проверки подлинности по идентификатору пользователя Active Directory и паролю.

- Служба Active Directory установлена и настроена для использования в вашей сети.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Сетевые диапазоны**.
2. Измените существующий сетевой диапазон или добавьте новый.

Параметр	Описание
Изменить существующий диапазон	Щелкните имя сетевого диапазона, чтобы его изменить.
Добавить диапазон	Щелкните Добавить сетевой диапазон , чтобы добавить новый диапазон.

3. Заполните форму.

Элемент формы	Описание
Имя	Введите имя сетевого диапазона.
Описание	Введите описание сетевого диапазона.
Сегменты View	Параметр «Сегменты View» появляется только в том случае, если модуль View включен. Узел URL-адреса доступа клиента. Введите правильный URL-адрес доступа клиента Horizon для сетевого диапазона. Порт доступа клиента. Введите правильный номер порта доступа клиента Horizon для сетевого диапазона.
Диапазоны IP-адресов	Измените или добавьте диапазоны IP-адресов, пока не будут включены все требуемые IP-адреса и не останется нежелательных адресов.

Следующие шаги

- Свяжите каждый сетевой диапазон с экземпляром поставщика удостоверений.
- Свяжите сетевые диапазоны с соответствующим правилом политики доступа. См. [Настройка параметров политики доступа](#).

Выбор атрибутов для синхронизации с каталогом

При настройке каталога Directories Management для синхронизации с Active Directory указываются атрибуты пользователя, которые должны синхронизироваться с каталогом. Перед настройкой каталога на странице «Атрибуты пользователя» можно указать, какие атрибуты требуются по умолчанию и, при желании, добавить дополнительные атрибуты, которые нужно сопоставить атрибутам Active Directory.

При настройке перед созданием каталога на странице «Атрибуты пользователя» можно изменить обязательные атрибуты по умолчанию на необязательные, отметить атрибуты как обязательные и добавить пользовательские атрибуты.

Для получения списка сопоставленных атрибутов по умолчанию см. [Управление атрибутами пользователя, синхронизируемыми из Active Directory](#).

После создания каталога можно изменить обязательный атрибут на необязательный и удалить пользовательские атрибуты. Нельзя изменить атрибут, чтобы он стал быть обязательным атрибутом.

При добавлении других атрибуты для синхронизации каталога после его создания перейдите на страницу каталога «Сопоставленные атрибуты» для сопоставления этих атрибутов атрибутам Active Directory.

Процедура

1. Войдите в службу vRealize Automation от имени системного администратора или администратора арендатора.
2. Откройте вкладку «Администрирование».
3. Выберите **Управление каталогами > Атрибуты пользователя**
4. В разделе «Атрибуты по умолчанию» нужно проверить список обязательных атрибутов и внести соответствующие изменения, чтобы указать, какие атрибуты должны быть обязательными.
5. В разделе «Атрибуты» в список необходимо добавить имя атрибута каталога Directories Management.
6. Нажмите кнопку **Сохранить**.

Состояние атрибута по умолчанию обновится, и новые атрибуты будут добавлены в список сопоставленных атрибутов каталога.
7. После создания каталога перейдите на страницу «Хранилища удостоверений» и выберите каталог.
8. Нажмите **Настройки синхронизации > Сопоставленные атрибуты**.
9. В раскрывающемся меню для добавленных атрибутов выберите атрибут Active Directory для сопоставления.
10. Нажмите кнопку **Сохранить**.

Результаты

Каталог обновится в следующий раз при синхронизации с Active Directory.

Применение политики доступа по умолчанию

Служба Directories Management включает политику доступа по умолчанию, которая контролирует доступ пользователей к порталам приложений. При необходимости правила политики можно изменять.

Если вы включаете методы проверки подлинности, отличные от проверки подлинности по паролю, необходимо отредактировать политику по умолчанию и добавить в правила политики включенный метод проверки подлинности.

Для каждого правила в политике доступа по умолчанию требуется соответствие набору критериев, чтобы пользователи могли получать доступ к portalу приложений. Вы применяете сетевой диапазон, указываете тип пользователя, который может получать доступ к содержимому, и выбираете методы проверки подлинности, которые необходимо использовать. См. [Управление политиками доступа](#).

Количество попыток входа пользователя в службу с помощью заданного метода проверки подлинности может быть разным. Служба предпринимает только одну попытку проверки подлинности для Kerberos или проверку подлинности сертификата. Если попытка входа пользователя завершается сбоем, выполняется попытка входа с помощью следующего метода проверки подлинности. Максимальное количество неудачных попыток входа в систему для пароля Active Directory и проверки подлинности

RSA SecurID по умолчанию равно 5. Если пользователь совершает пять неудачных попыток входа в систему, служба пытается выполнить вход для пользователя, используя следующий метод проверки подлинности в списке. После применения всех методов проверки подлинности служба выдает сообщение об ошибке.

Применение способов проверки подлинности к правилам политики

В правилах политики по умолчанию настраивается только способ проверки подлинности с помощью пароля. Чтобы выбрать другие настроенные способы проверки подлинности и установить последовательность их применения, нужно изменить правила политики.

Необходимые условия

Способы проверки подлинности, поддерживаемые организацией, должны быть активированы и настроены.

См. [Интеграция альтернативных продуктов для проверки подлинности пользователей с управлением каталогами](#).

Процедура

1. Выберите **Администрирование > Управление каталогами > Политики**.
2. Выберите политику доступа по умолчанию, которую необходимо отредактировать.
3. Чтобы изменить правило политики, в столбце «Способ проверки подлинности» выберите способ проверки подлинности для изменения в правилах политики.

Для добавления нового правила политики щелкните значок **+**.

4. Нажмите кнопку **Сохранить** и еще раз щелкните **Сохранить** на странице «Политика».

Изменить правило политики

Если сетевой диапазон для пользователя составляет...

и пользователь пытается получить доступ к содержимому из...

в этом случае пользователю необходимо выполнить проверку подлинности, используя следующий метод.

и

Если не удалось выполнить проверку подлинности с помощью предыдущего метода:

только

[+ методы возврата в основную среду](#)

Выполнить повторную проверку подлинности ч. через:

5. Нажмите кнопку **Сохранить** и еще раз щелкните **Сохранить** на странице «Политика».

Настройка Kerberos для Directories Management

Проверка подлинности с помощью Kerberos позволяет пользователям, которые успешно вошли в свой домен Active Directory, получать доступ к portalу приложений без дополнительных запросов учетных данных. Во время проверки подлинности Windows обеспечивается применение протокола Kerberos для защиты передачи данных между браузерами пользователей и службой Directories Management. Чтобы реализовать функцию Kerberos для своего развертывания, саму службу Active Directory настраивать не нужно.

В настоящее время проверка подлинности с помощью Kerberos при передаче данных между браузером пользователя и службой выполняется только в операционных системах Windows. Для доступа к службе из других операционных систем проверка подлинности с помощью Kerberos не применяется.

■ **Настройка проверки подлинности с помощью Kerberos**

Чтобы настроить службу Directories Management для обеспечения проверки подлинности с помощью Kerberos, необходимо присоединиться к домену и включить проверку подлинности с помощью Kerberos на соединителе Directories Management.

■ **Настройка Internet Explorer для доступа к веб-интерфейсу**

Необходимо настроить браузер Internet Explorer, если Kerberos настроен для вашего развертывания и если вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью Internet Explorer.

■ **Настройка Firefox для доступа к веб-интерфейсу**

Необходимо настроить браузер Firefox, если для вашего развертывания настроен протокол Kerberos и вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью браузера Firefox.

■ **Настройка браузера Chrome для доступа к веб-интерфейсу**

Необходимо настроить браузер Chrome, если для вашего развертывания настроен протокол Kerberos и вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью браузера Chrome.

Настройка проверки подлинности с помощью Kerberos

Чтобы настроить службу Directories Management для обеспечения проверки подлинности с помощью Kerberos, необходимо присоединиться к домену и включить проверку подлинности с помощью Kerberos на соединителе Directories Management.

Необходимые условия

- Разверните NSX Edge в vCenter и настройте подсистему балансировки нагрузки NSX.
Дополнительные сведения о настройке подсистемы балансировки нагрузки см. в разделе *Балансировка нагрузки в vRealize Automation*.
- Присоедините домен к главному арендатору. Это необходимо сделать до создания подключений к каталогу в отдельных арендаторах.
 - а) Войдите в арендатор по умолчанию под именем administrator@vsphere.local.
 - б) Создайте локального пользователя TestUser и укажите его в качестве администратора арендатора.
 - в) Выберите **Администрирование > Управление каталогами > Соединители**.
 - г) Выберите «Присоединиться к домену» на каждом соединителе устройства.
 - д) В разделе «Присоединиться к домену» выберите «Другой домен» и укажите домен, к которому должен подключиться арендатор. Также укажите учетные данные и организационное подразделение, к которому следует подключиться.

- Настройте подключения к каталогу для арендаторов по умолчанию и арендаторов, не используемых по умолчанию. Проверка подлинности Kerberos работает как со встроенной проверкой подлинности Windows, так и с Active Directory через LDAP. См. [Настройка ссылки Active Directory по LDAP/IWA](#) и [Настройка подключения к каталогу OpenLDAP](#).
- Убедитесь, что имя узла vRealize Automation совпадает с доменом Active Directory, к которому он присоединяется. Например, если vRealize Automation присоединяется к области Active Directory с именем COMPANY.COM, имя узла должно иметь вид node.company.com.
- Настройте поставщик удостоверений рабочей области. Убедитесь, что все узлы в развертывании зарегистрированы в поставщике удостоверений рабочей области и задано имя подсистемы балансировки нагрузки.
 - а) Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.
 - б) Выберите соответствующую ссылку поставщика удостоверений.
Например, WorkspaceIDP_1.
 - в) Щелкните ссылку поставщика удостоверений и найдите настроенное имя узла поставщика удостоверений. Запишите имя узла, так как оно понадобится при настройке веб-браузеров.
 - г) Зарегистрируйте все необходимые узлы в поставщике удостоверений рабочей области и укажите в качестве имени узла полное доменное имя подсистемы балансировки нагрузки.
 - д) Нажмите кнопку **Сохранить**.
- Настройте каталог для арендатора по умолчанию. См. раздел «Настройка доступа к арендатору по умолчанию» в документе *Установка vRealize Automation*

Процедура

1. В качестве администратора арендатора выберите **Администрирование > Управление каталогами > Соединители**
2. На странице «Соединители» для соединителя, настраиваемого для проверки подлинности с помощью Kerberos, нажмите **Присоединить к домену**.
3. На странице «Присоединение к домену» введите информацию для домена Active Directory.

Параметр	Описание
Домен	Введите полное доменное имя Active Directory. Введенное доменное имя должно быть в том же домене Windows, что и сервер соединителя.
Пользователь домена	Введите имя пользователя учетной записи в Active Directory, который имеет разрешение на присоединение к этому домену Active Directory.
Доменный пароль	Введите пароль пользователя Active Directory. Этот пароль не сохраняется в Directories Management .

Нажмите кнопку **Сохранить**.

Страница «Присоединение к домену» обновится, и будет выведено сообщение, что в данный момент вы присоединены к домену.

4. В столбце «Рабочий процесс» для соединителя нажмите **Адаптеры проверки подлинности**.

5. Нажмите **KerberosIdpAdapter**

Вы будете перенаправлены на страницу входа диспетчера удостоверений.

6. Нажмите **Изменить** в строке KerberosIdpAdapter и настройте страницу проверки подлинности Kerberos.

Параметр	Описание
Имя	Имя должно быть задано. По умолчанию используется имя KerberosIdpAdapter. Его можно изменить.
Атрибут UID каталога	Введите атрибут учетной записи, который содержит имя пользователя.
Включить проверку подлинности Windows.	Выберите этот параметр, чтобы расширить взаимодействие по проверке подлинности между браузерами пользователей и Directories Management.
Включить NTLM	Выберите этот параметр, чтобы включить функцию проверки подлинности только на основе протокола NT LAN Manager (NTLM), если инфраструктура Active Directory использует проверку подлинности NTLM.
Включить перенаправление	Выберите этот параметр, если карусельный DNS и подсистема балансировки нагрузки не поддерживают Kerberos. Запросы на проверку подлинности перенаправляются на узел, указанный в поле «Имя узла для перенаправления». Если этот флажок установлен, введите имя узла для перенаправления в текстовом поле Имя узла для перенаправления . Это, как правило, имя узла, на котором запущена служба.

7. Нажмите кнопку **Сохранить**.

8. Настройте проверку подлинности Kerberos на всех необходимых узлах.

а) Выберите **Администрирование > Управление каталогами > Соединители**.

На этой странице отображаются настроенные в настоящее время соединители. По умолчанию настроена только проверка подлинности с помощью пароля.

б) Щелкните гиперссылку рабочего процесса, связанную с первым Устройство vRealize Automation.

в) Щелкните ссылку KerberosIdpAdapter, чтобы открыть страницу проверки подлинности.

Возможно, потребуется ввести пароль и заново открыть ссылку KerberosIdpAdapter.

г) Укажите атрибут UID каталога и введите значение по умолчанию sAMAccountName.

д) Установите флажки **Включить проверку подлинности Windows** и **Включить перенаправление**.

е) Флажок **NTLM** должен быть снят, так как он необходим только для контроллеров домена старых версий.

ж) Введите имя устройства VA1 в качестве имени узла перенаправления.

з) Нажмите кнопку **Сохранить**.

9. Настройте политику доступа по умолчанию Для конфигурации Kerberos требуются три политики доступа: Kerberos, пароль, локальный пароль.

- а) Выберите **Администрирование > Управление каталогами > Политики**.
- б) Выберите default_access_policy_set.
- в) Щелкните связанное с гиперссылкой значение «Пароль» под заголовком «Методы проверки подлинности» в адресной строке веб-браузера.
- г) Щелкните зеленые значки «+», чтобы создать новые методы проверки подлинности для Kerberos, пароля и Пароля (локальный каталог).
- д) Для каждого метода проверки подлинности выберите **ВСЕ ДИАПАЗОНЫ** в качестве сетевого диапазона пользователей, а в качестве средства доступа к содержимому пользователя укажите веб-браузер.
- е) Измените первый метод проверки подлинности на Kerberos, а в качестве метода возврата в основную среду укажите пароль.
- ж) Щелкните **Сохранить**, а затем — **ОК**.

Настройка Internet Explorer для доступа к веб-интерфейсу

Необходимо настроить браузер Internet Explorer, если Kerberos настроен для вашего развертывания и если вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью Internet Explorer.

Проверка подлинности с помощью Kerberos работает вместе с Directories Management в операционных системах Windows.

Примечание Не выполняйте эти операции, связанные с Kerberos, в других операционных системах.

Необходимые условия

Настройте браузер Internet Explorer для каждого пользователя или предоставьте пользователям необходимые инструкции после настройки Kerberos.

Процедура

- 1.** Убедитесь, что вы вошли в систему Windows как пользователь в домене.
- 2.** В Internet Explorer включите автоматический вход.
 - а) Выберите **Сервис > Свойства браузера > Безопасность**.
 - б) Щелкните **Настраиваемый уровень**.
 - в) Выберите **Автоматический вход только в зоне интрасети**.
 - г) Нажмите кнопку **ОК**.

3. Убедитесь, что этот экземпляр виртуального устройства соединителя является частью зоны местной интрасети.
 - а) Используйте Internet Explorer для доступа к URL-адресу входа в Directories Management на веб-сайте *https://myconnectorhost.domain/authenticate/*.
 - б) Найдите зону в правом нижнем углу в строке состояния окна браузера.
Если зона — «Местная интрасеть», настройка Internet Explorer завершена.
4. Если зона — не «Местная интрасеть», добавьте URL-адрес входа в Directories Management в зону интрасети.
 - а) Выберите **Сервис > Свойства браузера > Безопасность > Местная интрасеть > Сайты**.
 - б) Установите флажок **Автоматически определять принадлежность к интрасети**.
Если этот флажок еще не установлен, установите его, чтобы добавить в зону интрасети.
 - в) (Необязательно) Если вы установили флажок **Автоматически определять принадлежность к интрасети**, нажимайте кнопку **ОК**, пока не будут закрыты все диалоговые окна.
 - г) В диалоговом окне «Местная интрасеть» щелкните **Дополнительно**.
Появляется второе диалоговое окно с именем «Местная интрасеть».
 - д) Введите URL-адрес Directories Management в текстовом поле **Добавить этот веб-сайт в зону**.
https://myconnectorhost.domain/authenticate/
 - е) Нажмите **Добавить > Закрыть > ОК**.
5. Убедитесь, что для Internet Explorer разрешено выполнение проверки подлинности Windows на надежном узле.
 - а) В диалоговом окне «Свойства браузера» перейдите на вкладку **Дополнительно**.
 - б) Установите флажок **Разрешить встроенную проверку подлинности Windows**.
Этот параметр вступит в силу только после перезапуска Internet Explorer.
 - в) Нажмите кнопку **ОК**.
6. Войдите в веб-интерфейс для проверки доступа.
Если проверка подлинности с помощью Kerberos завершается успешно, тестовый URL-адрес подключается к веб-интерфейсу.

Результаты

Протокол Kerberos защищает весь обмен данными между этим экземпляром браузера Internet Explorer и Directories Management. Теперь пользователи могут использовать единый вход для доступа к portalу «Мои приложения».

Настройка Firefox для доступа к веб-интерфейсу

Необходимо настроить браузер Firefox, если для вашего развертывания настроен протокол Kerberos и вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью браузера Firefox.

Проверка подлинности с помощью Kerberos работает вместе с Directories Management в операционных системах Windows.

Необходимые условия

Настройте браузер Firefox для каждого пользователя или предоставьте пользователям необходимые инструкции после настройки Kerberos.

Процедура

1. В текстовом поле «URL-адрес» браузера Firefox введите **about:config** для доступа к расширенным параметрам.
2. Щелкните **I'll be careful, I promise!**.
3. Дважды щелкните **network.negotiate-auth.trusted-uris** в столбце «Имя предпочтения».
4. Введите в текстовом поле URL-адрес Directories Management.
https://myconnectorhost.domain.com
5. Нажмите кнопку **OK**.
6. Дважды щелкните **network.negotiate-auth.delegation-uris** в столбце «Имя предпочтения».
7. Введите в текстовом поле URL-адрес Directories Management.
https://myconnectorhost.domain.com/authenticate/
8. Нажмите кнопку **OK**.
9. Протестируйте функции Kerberos с помощью браузера Firefox для входа по URL-адресу входа. Например, *https://myconnectorhost.domain.com/authenticate/*.

Если проверка подлинности с помощью Kerberos завершается успешно, тестовый URL-адрес подключается к веб-интерфейсу.

Результаты

Протокол Kerberos защищает весь обмен данными между этим экземпляром браузера Firefox и Directories Management. Теперь пользователи могут использовать единый вход для доступа к portalу «Мои приложения».

Настройка браузера Chrome для доступа к веб-интерфейсу

Необходимо настроить браузер Chrome, если для вашего развертывания настроен протокол Kerberos и вы хотите предоставлять пользователям доступ к веб-интерфейсу с помощью браузера Chrome.

Проверка подлинности с помощью Kerberos работает вместе с Directories Management в операционных системах Windows.

Примечание Не выполняйте эти операции, связанные с Kerberos, в других операционных системах.

Необходимые условия

- Настройте Kerberos.

- Так как Chrome использует конфигурацию Internet Explorer для обеспечения проверки подлинности с помощью Kerberos, настройте Internet Explorer, чтобы Chrome мог использовать конфигурацию Internet Explorer. Сведения о настройке Chrome для проверки подлинности Kerberos см. в документации Google.

Процедура

1. Протестируйте функции Kerberos с помощью браузера Chrome.
2. Выполните вход в Directories Management на веб-сайте <https://myconnectorhost.domain.com/authenticate/>.

Если проверка подлинности с помощью Kerberos завершается успешно, тестовый URL-адрес подключается к веб-интерфейсу.

Результаты

Если проверка подлинности с помощью Kerberos настроена правильно, соответствующий протокол (Kerberos) защищает весь обмен данными между этим экземпляром браузера Chrome и Directories Management. Пользователи могут использовать единый вход для доступа к portalу «Мои приложения».

Обновление внешних соединителей для управления каталогами

Если в конфигурации управления каталогами vRealize Automation используется внешний соединитель, возможно, понадобится время от времени обновлять этот соединитель.

Может потребоваться обновить внешний соединитель при обновлении версии развертывания vRealize Automation или если в новой сборке соединителя предлагается необходимая вам функция.

Этот документ предназначен только для тех пользователей, которые развертывали дополнительные отдельные устройства внешнего соединителя. В vRealize Automation, например, устройства внешнего соединителя используются с проверкой подлинности смарт-карты.

По умолчанию соединитель использует веб-сайт VMware для процедуры обновления, что требует подключения к Интернету для этого устройства соединителя. Необходимо также настроить параметры прокси-сервера для устройства соединителя, если это возможно.

Если у экземпляра соединителя нет подключения к Интернету, можно выполнить обновление в автономном режиме. Чтобы выполнить обновление в автономном режиме, необходимо загрузить пакет обновления и настроить локальный веб-сервер для размещения файла обновления.

Целевая аудитория

Эта информация предназначена для пользователей, которые устанавливают, обновляют и настраивают управление каталогами. Эта информация предназначена для опытных системных администраторов сред Windows и Linux, знакомых с технологией виртуальных машин.

Подготовка к обновлению внешнего соединителя

Для подготовки к обновлению соединителя необходимо выполнить проверку на наличие обновлений и настроить параметры прокси-сервера для устройства (при необходимости).

■ Проверка наличия новой версии для внешнего соединителя через Интернет

Если устройство соединителя подключено к Интернету, можно проверять наличие новых версий через Интернет непосредственно с этого устройства.

■ Настройка параметров прокси-сервера для внешнего устройства соединителя

Устройство соединителя получает доступ к серверам обновления VMware через Интернет. Если конфигурация сети обеспечивает доступ к Интернету через прокси-сервер HTTP, необходимо настроить параметры прокси-сервера для устройства.

Проверка наличия новой версии для внешнего соединителя через Интернет

Если устройство соединителя подключено к Интернету, можно проверять наличие новых версий через Интернет непосредственно с этого устройства.

Процедура

1. Выполните вход на устройство в качестве пользователя root.
2. Выполните следующую команду.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

3. Выполните следующую команду, чтобы проверить наличие обновления в сети.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

Настройка параметров прокси-сервера для внешнего устройства соединителя

Устройство соединителя получает доступ к серверам обновления VMware через Интернет. Если конфигурация сети обеспечивает доступ к Интернету через прокси-сервер HTTP, необходимо настроить параметры прокси-сервера для устройства.

Настройте прокси-сервер для обработки только интернет-трафика. Чтобы убедиться, что прокси-сервер настроен должным образом, установите для параметра внутреннего трафика значение no-proxy в пределах домена.

Примечание Прокси-серверы, требующие проверки подлинности, не поддерживаются.

Необходимые условия

- Убедитесь, что у вас имеется пароль пользователя root для устройства соединителя.
- Убедитесь, что у вас имеются сведения о прокси-сервере.

Процедура

1. Выполните вход на устройство в качестве пользователя root.
2. В командной строке введите YaST, чтобы запустить служебную программу YaST.
3. На панели слева выберите **Сетевые службы**, а затем — **Прокси-сервер**.

4. Введите URL-адреса прокси-серверов в полях **URL-адрес HTTP-прокси** и **URL-адрес HTTPS-прокси**.
5. Нажмите кнопку **Готово** и выйдите из служебной программы YaST.
6. Перезапустите сервер Tomcat на виртуальном устройстве соединителя, чтобы использовать новые параметры прокси-сервера.

```
service horizon-workspace restart
```

Результаты

Для устройства соединителя сейчас доступны серверы обновления VMware.

Онлайн-обновление внешнего соединителя

Можно выполнить онлайн-обновление внешнего соединителя управления каталогами, если у вас установлено подходящее подключение к сети.

Необходимые условия

- Убедитесь, что устройство соединителя может разрешить и получить доступ к `vapp-updates.vmware.com` через порт 80 по HTTP.
- Проверьте наличие обновления соединителя. Выполните соответствующую команду, чтобы проверить наличие обновлений. См. раздел «Проверка доступности обновления соединителя Directories Management в сети».
- Убедитесь, что доступно как минимум 2 ГБ дискового пространства на основном корневом разделе устройства.
- Убедитесь, что соединитель настроен правильно.
- Сделайте моментальный снимок устройства соединителя, чтобы создать его резервную копию. Для получения дополнительной информации о том, как делать моментальные снимки, см. документацию vSphere.
- Если для исходящего доступа по HTTP требуется прокси-сервер HTTP, настройте параметры прокси-сервера для устройства соединителя. См. раздел «Настройка параметров прокси-сервера для устройства соединителя Directories Management».

Процедура

1. Выполните вход на устройство в качестве пользователя `root`.
2. Выполните следующую команду.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

3. Выполните следующую команду, чтобы проверить наличие обновления в сети.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

4. Выполните следующую команду, чтобы обновить устройство.

```
/usr/local/horizon/update/updatesmgr.hznupdate
```

Сообщения, получаемые в процессе обновления, сохраняются в файл `update.log` по адресу `/opt/vmware/var/log/update.log`.

5. Запустите команду `updatesmgr.hzn check` еще раз, чтобы убедиться, что более свежего обновления не существует.

```
/usr/local/horizon/update/updatesmgr.hzncheck
```

6. Проверьте версию обновленного устройства.

```
vami-cli version --appliance
```

Отобразится новая версия.

7. Перезапустите устройство соединителя.

```
reboot
```

Автономное обновление внешнего соединителя

Если существующее устройство соединителя управления каталогами vRealize Automation не может подключиться к Интернету для обновления, можно выполнить автономное обновление. Необходимо задать репозиторий обновления на локальном веб-сервере и настроить для устройства соединителя использование локального веб-сервера для обновления.

Необходимые условия

- Проверьте наличие обновления соединителя. Проверьте наличие обновлений на сайте загрузок My VMware по адресу my.vmware.com.
- Убедитесь, что доступно как минимум 2 ГБ дискового пространства на основном корневом разделе устройства.
- Убедитесь, что соединитель настроен правильно.
- Сделайте моментальный снимок устройства соединителя, чтобы создать его резервную копию. Для получения дополнительной информации о том, как делать моментальные снимки, см. документацию vSphere.

- Настройте для устройства соединителя использование локального веб-сервера для размещения файла обновления. См. раздел «Подготовка локального веб-сервера к автономному обновлению».

Процедура

1. Подготовка локального веб-сервера к обновлению в автономном режиме

Прежде чем начать обновление соединителя в автономном режиме, подготовьте локальный веб-сервер, создав структуру каталога, которая включает подкаталог для устройства соединителя.

2. Настройка соединителя и выполнение обновления в автономном режиме

Для выполнения обновления в автономном режиме настройте устройство соединителя таким образом, чтобы оно указывало на локальный веб-сервер. Затем обновите устройство.

Подготовка локального веб-сервера к обновлению в автономном режиме

Прежде чем начать обновление соединителя в автономном режиме, подготовьте локальный веб-сервер, создав структуру каталога, которая включает подкаталог для устройства соединителя.

Необходимые условия

- Загрузите файл `identity-manager-connector-versionNumber-buildNumber-updaterepo.zip` из раздела «My VMware». Зайдите на веб-сайт my.vmware.com, перейдите на страницу «Загрузка VMware Identity Manager» и загрузите файл, находящийся в разделе **Пакет обновления соединителя VMware Identity Manager в автономном режиме**.
- Если вы используете веб-сервер IIS, настройте веб-сервер для разрешения специальных символов в именах файлов. Эти настройки выполняются в разделе **Фильтрация запросов** путем выбора параметра **Разрешить двойное преобразование**.

Процедура

1. Создайте каталог на веб-сервере по адресу `http://веб-сервер/BM/` и скопируйте в него загруженный ZIP-файл.
2. Убедитесь, что веб-сервер включает типы MIME для `.sig (text/plain)` и `.sha256 (text/plain)`.

Без этих типов MIME веб-серверу не удастся проверить наличие обновлений.

3. Распакуйте файл.

Содержимое распакованного ZIP-файла выполняется здесь: `http://веб-сервер/BM/`.

Распакованное содержимое файла содержит следующие подкаталоги: `/manifest` и `/package-pool`.

4. Выполните следующую команду `updateLocal.hzn`, чтобы убедиться, что этот URL-адрес содержит допустимое содержимое обновления.

```
/usr/local/horizon/update/updatesLocal.hzn checkurl http://веб-сервер/BM
```

Настройка соединителя и выполнение обновления в автономном режиме

Для выполнения обновления в автономном режиме настройте устройство соединителя таким образом, чтобы оно указывало на локальный веб-сервер. Затем обновите устройство.

Необходимые условия

Подготовьте локальный веб-сервер для обновления в автономном режиме.

Процедура

1. Выполните вход на устройство в качестве пользователя root.
2. Выполните следующую команду, чтобы настроить репозиторий обновления, для которого используется локальный веб-сервер.

```
/usr/local/horizon/update/updatelocal.hzn seturl http://веб-сервер/ВМ/
```

Примечание Чтобы отменить конфигурацию и восстановить возможность обновления по сети, можно выполнить следующую команду.

```
/usr/local/horizon/update/updatelocal.hzn setdefault
```

3. Выполните обновление.

- а) Выполните следующую команду.

```
/usr/local/horizon/update/updatemgr.hznupdateinstaller
```

- б) Выполните следующую команду, чтобы проверить версию доступного обновления.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- в) Выполните следующую команду, чтобы обновить соединитель.

```
/usr/local/horizon/update/updatemgr.hznupdate
```

Сообщения, получаемые в процессе обновления, сохраняются в файл `update.log` по адресу `/opt/vmware/var/log/update.log`.

- г) Выполните команду `updatemgr.hzn check` еще раз.

```
/usr/local/horizon/update/updatemgr.hzncheck
```

- д) Проверьте версию обновленного устройства.

```
vamicli version --appliance
```

Эта команда должна отобразить новую версию.

- е) Перезапустите устройство соединителя.

Например, в командной строке выполните следующую команду.

```
reboot
```

Результаты

Обновление соединителя завершено.

Настройка параметров после обновления внешнего соединителя

После обновления до соединителя 2016.3.1.0 или более новой версии может понадобиться настроить некоторые параметры.

Повторное присоединение к домену с помощью проверки подлинности Kerberos

Если используются каталоги проверки подлинности Kerberos или Active Directory (встроенная проверка подлинности Windows), необходимо отсоединиться от домена, а затем снова присоединиться к нему. Это обязательное действие для всех виртуальных устройств соединителя в развертывании.

1. Выберите **Администрирование > Управление каталогами > Соединители**.
2. На странице «Соединители» для каждого соединителя, который используется для проверки подлинности Kerberos или Active Directory (встроенная проверка подлинности Windows), нажмите кнопку **Покинуть домен**.
3. Чтобы присоединиться к домену, нужны учетные данные Active Directory с правами на присоединение к домену. Дополнительные сведения см. в разделе [Присоединение компьютера соединителя к домену](#).
4. Если используется проверка подлинности Kerberos, включите адаптер проверки подлинности Kerberos еще раз. Чтобы получить доступ к странице «Адаптеры проверки подлинности», нажмите соответствующую ссылку в столбце **Работник** на странице соединителей и выберите вкладку **Адаптеры проверки подлинности**.
5. Убедитесь, что другие используемые адаптеры проверки подлинности включены.

Страница обновления доменов

Если Active Directory (встроенная проверка подлинности Windows) или Active Directory по LDAP используется с включенным параметром **Этот каталог поддерживает расположение службы DNS**, сохраните страницу «Домены» каталога.

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Выберите применимый каталог, чтобы изменить его.
3. Введите пароль пользователя с различающимся именем домена и нажмите **Сохранить**.
4. Нажмите кнопку **Синхронизировать параметры** в левой части страницы и выберите вкладку **Домены**.
5. Нажмите кнопку **Сохранить**.

Расположение службы DNS и контроллеры домена

Примечание В соединителе 2016.3.1.0 или более новой версии файл `domain_krb.properties` автоматически создается и заполняется контроллерами домена при создании каталога с включенным расположением службы DNS. Если страница «Домены» сохраняется после обновления и в исходном развертывании был файл `domain_krb.properties`, в него вносятся домены, которые могли быть добавлены впоследствии и которых не было в файле. Если в исходном развертывании не было файла `domain_krb.properties`, файл создается и автоматически заполняется контроллерами домена. Дополнительные сведения о файле `domain_krb.properties` см. в разделе [Выбор контроллеров домена](#).

Устранение ошибок обновления внешнего соединителя

Чтобы устранить неполадки обновления внешнего соединителя управления каталогами vRA, просмотрите журналы ошибок. Если соединитель не запускается, можно восстановить предыдущий экземпляр, выполнив откат до моментального снимка.

■ Проверка журналов ошибок обновления

Чтобы устранить ошибки, которые произошли во время обновления, проверьте журналы ошибок. Файлы журналов обновлений находятся в каталоге `/opt/vmware/var/log`.

■ Выполнение отката к моментальному снимку соединителя

Если соединитель не запускается надлежащим образом после обновления и невозможно устранить эту проблему, проверив журналы ошибок обновления и запустив команду обновления еще раз, можно выполнить откат к предыдущему экземпляру соединителя.

■ Сбор пакета файлов журнала

Для отправки в службу поддержки VMware можно собрать пакет файлов журнала. Этот пакет можно получить на странице настройки соединителя.

Проверка журналов ошибок обновления

Чтобы устранить ошибки, которые произошли во время обновления, проверьте журналы ошибок. Файлы журналов обновлений находятся в каталоге `/opt/vmware/var/log`.

Если возникли какие-либо ошибки, после обновления соединитель может не запускаться.

Процедура

1. Выполните вход на устройство соединителя.
2. Перейдите в каталог `/opt/vmware/var/log`.
3. Откройте файл `update.log` и просмотрите сообщения об ошибках.
4. Устраните ошибки и повторно запустите команду обновления. Команда обновления возобновляет работу с той точки, на которой она остановилась.

Примечание Кроме того, можно выполнить восстановление из моментального снимка и запустить обновление еще раз.

Выполнение отката к моментальному снимку соединителя

Если соединитель не запускается надлежащим образом после обновления и невозможно устранить эту проблему, проверив журналы ошибок обновления и запустив команду обновления еще раз, можно выполнить откат к предыдущему экземпляру соединителя.

Процедура

- ◆ Восстановите соединитель из одного из моментальных снимков, выполненных в качестве резервной копии оригинального экземпляра соединителя. Для получения дополнительной информации см. документацию vSphere.

Сбор пакета файлов журнала

Для отправки в службу поддержки VMware можно собрать пакет файлов журнала. Этот пакет можно получить на странице настройки соединителя.

В пакет включаются перечисленные ниже файлы журнала.

Таблица 2-9. Файлы журнала

Компонент	Расположение файла журнала	Описание
Журналы Apache Tomcat (catalina.log)	/opt/vmware/horizon/workspace/logs/catalina.log	Apache Tomcat записывает сообщения, не записанные в другие файлы журнала.
Журналы конфигулятора (configurator.log)	/opt/vmware/horizon/workspace/logs/configurator.log	Запросы, поступающие в конфигулятор от клиента REST и веб-интерфейса пользователя.
Журналы соединителя (connector.log)	/opt/vmware/horizon/workspace/logs/connector.log	Запись каждого запроса, полученного из веб-интерфейса. Каждая запись журнала включает также URL-адрес, временную метку и исключения запроса. Действия по синхронизации не вносятся в журнал.

Процедура

1. Войдите на страницу настройки соединителя по адресу `https://connectorURL:8443/cfg/logs`.
2. Нажмите кнопку **Подготовить пакет журналов**.
3. Загрузите пакет и отправьте его в службу поддержки VMware.

Сценарий: настройка ссылки Active Directory для обеспечения высокой доступности vRealize Automation

Администратору арендатора необходимо настроить Active Directory через подключение каталога LDAP для поддержки проверки подлинности пользователя и обеспечения развертывания высокой доступности vRealize Automation.

Каждое устройство vRealize Automation содержит соединитель, который поддерживает проверку подлинности пользователей, хотя для обеспечения синхронизации каталога обычно настроен только один соединитель. В качестве соединителя синхронизации можно выбрать любой соединитель. Для поддержки высокой доступности службы управления каталогами необходимо настроить второй соединитель,

соответствующий второму устройству vRealize Automation, который подключается к поставщику удостоверений и указывает на ту же самую службу Active Directory. При использовании такой конфигурации, если одно устройство выходит из строя, второе принимает на себя управление процессом проверки подлинности пользователей.

В среде с высокой доступностью все узлы должны обслуживать один и тот же набор каталогов Active Directory, пользователей, методов проверки подлинности и т. д. Наиболее простым способом реализации такой конфигурации является применение поставщика удостоверений в кластере путем настройки узла подсистемы балансировки нагрузки в качестве узла поставщика удостоверений. Благодаря такой конфигурации все запросы на проверку подлинности направляются в подсистему балансировки нагрузки, которая затем отправляет их на один из соединителей.

Необходимые условия

- Установите распределенное развертывание vRealize Automation с соответствующей подсистемой балансировки нагрузки. См. *Установка vRealize Automation*.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Щелкните **Добавить каталог**.
3. Укажите специальные настройки учетной записи Active Directory и примите параметры по умолчанию.

Параметр	Пример вводимых данных
Имя каталога	Добавьте IP-адрес имени домена Active Directory
Соединитель синхронизации	Каждое устройство vRealize Automation содержит соединитель. Используйте любой доступный соединитель.
Базовое имя домена	Введите различающееся имя начальной точки для поиска сервера каталогов. Например, cn=users,dc=corp,dc=local .
Имя домена привязки	Введите полное различающееся имя, включая обычное имя, учетной записи пользователя Active Directory с разрешениями на поиск пользователей. Например, cn=config_admin infra,cn=users,dc=corp,dc=local .
Пароль имени домена привязки	Введите пароль Active Directory для учетной записи, с помощью которой можно искать пользователей.

4. Щелкните **Проверить подключение**, чтобы проверить подключение к настроенному каталогу.

При сбое подключения проверьте значения во всех полях и при необходимости обратитесь к системному администратору.

5. Нажмите **Сохранить и Далее**.

Откроется страница «Выбор доменов» со списком доменов.

6. Выберите домен по умолчанию и нажмите кнопку **Далее**.

7. Убедитесь, что имена атрибутов сопоставлены с соответствующими атрибутами Active Directory. В противном случае в раскрывающемся меню выберите правильный атрибут Active Directory. Нажмите кнопку **Далее**.

8. Выберите группы и пользователей для синхронизации.

- а) Щелкните значок **Добавить** (+).
- б) Введите домен пользователя и щелкните элемент **Поиск групп**.
Например, **cn=users,dc=corp,dc=local**.
- в) Установите флажок **Выбрать все**.
- г) Нажмите **Выбрать**.
- д) Нажмите кнопку **Далее**.
- е) Щелкните +, чтобы добавить дополнительных пользователей. Например, введите **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Чтобы удалить пользователей, щелкните +. Таким образом, создается фильтр, позволяющий исключить некоторые типы пользователей. Вы выбираете атрибут пользователя для фильтрации, правило запроса и значение.

- ж) Нажмите кнопку **Далее**.

9. Посмотрите на странице, сколько пользователей и групп синхронизируются с каталогом, и щелкните команду **Синхронизировать каталог**.

Процесс синхронизации каталогов занимает некоторое время, но проходит в фоновом режиме, и вы можете продолжать работать.

10. Настройте второй соединитель для поддержки высокой доступности.

- а) Войдите в подсистему балансировки нагрузки для развертывания vRealize Automation в качестве администратора арендатора.

URL-адрес подсистемы балансировки нагрузки — *<адрес подсистемы балансировки нагрузки>/vcac/org/tenant_name*.

- б) Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.

- в) Щелкните поставщика удостоверений, который в настоящее время используется для вашей системы.

Появляются существующий каталог и соединитель, которые обеспечивают базовое управление учетными данными для вашей системы.

- г) Щелкните раскрывающийся список **Добавить соединитель** и выберите соединитель, который соответствует дополнительному устройству vRealize Automation.

- д) Введите соответствующий пароль в текстовом поле **Пароль имени домена привязки**, которое появляется при выборе соединителя.

- е) Щелкните **Добавить соединитель**.
- ж) Измените имя узла для указания на подсистему балансировки нагрузки.

Результаты

Корпоративный каталог Active Directory подключен к vRealize Automation. Управление каталогами настроено для обеспечения высокой доступности.

Следующие шаги

Для обеспечения усиленной безопасности можно настроить двунаправленную доверенную связь между поставщиком удостоверений и Active Directory. См. раздел [Настройка двунаправленных отношений доверия между vRealize Automation и Active Directory](#).

Настройка внешних соединителей для проверки подлинности с помощью смарт-карты и сторонних поставщиков удостоверений в vRealize Automation

Системному администратору необходимо настроить внешний соединитель для развертывания vRealize Automation с помощью консоли управления каталогами, если используются сторонние поставщики удостоверений с проверкой подлинности с помощью сертификата или смарт-карты. Кроме того, описываемая здесь процедура применяется ко всем типам проверки подлинности на основе сертификата.

Управление каталогами поддерживает несколько поставщиков удостоверений и кластеров соединителей для каждого настроенного экземпляра Active Directory. Чтобы использовать проверку подлинности с помощью смарт-карты или стороннего поставщика удостоверений, можно настроить один внешний соединитель или кластер соединителей с соответствующим поставщиком удостоверений вне подсистемы балансировки нагрузки, в которой настроено сквозное подключение SSL. Дополнительные сведения см. в разделе [Управление соединителями и кластерами соединителей](#).

Дополнительные сведения об обновлении внешнего соединителя см. в разделе [Обновление внешних соединителей для управления каталогами](#).

Проверка подлинности с помощью смарт-карты поддерживает различные варианты конфигурации сертификата. См. раздел [Настройка сертификата или адаптера смарт-карты для использования со службой управления каталогами](#).

Необходимые условия

- Настройте соответствующее подключение Active Directory для развертывания vRealize Automation.
- Загрузите файл в формате OVA, необходимый для настройки соединителя, используя ссылку [Средства и комплект SDK VMware vRealize Automation](#).

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

Процедура

1. Создание маркера активации соединителя

Прежде чем развернуть виртуальное устройство соединителя, которое будет использоваться для проверки подлинности с помощью смарт-карт, необходимо создать код активации для нового соединителя в консоли vRealize Automation. Код активации позволяет создать связь между управлением каталогами и соединителем.

2. Развертывание файла OVA соединителя

После загрузки файла OVA соединителя его можно развернуть с помощью клиента VMware vSphere Client или vSphere Web Client.

3. Настройка параметров соединителя

После развертывания файла OVA соединителя необходимо запустить мастер настройки, чтобы активировать устройство и задать пароли администратора.

4. Использование центра открытых сертификатов

При установке службы управления каталогами создается сертификат SSL по умолчанию. В целях тестирования можно использовать сертификат по умолчанию, но для производственной среды нужно создать и установить коммерческие сертификаты SSL.

5. Создание поставщика удостоверений рабочей области

Необходимо создать поставщика удостоверений рабочей области, который будет использовать внешний соединитель.

6. Настройка проверки подлинности на основе сертификата и правил политики доступа по умолчанию

Для Active Directory и домена vRealize Automation необходимо настроить внешний соединитель.

Создание маркера активации соединителя

Прежде чем развернуть виртуальное устройство соединителя, которое будет использоваться для проверки подлинности с помощью смарт-карт, необходимо создать код активации для нового соединителя в консоли vRealize Automation. Код активации позволяет создать связь между управлением каталогами и соединителем.

Можно настроить один соединитель или кластер соединителей. Если нужно использовать кластер соединителей, выполните описанную процедуру снова для каждого необходимого соединителя.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Управление каталогами > Соединители**.
2. Щелкните **Добавить соединитель**.
3. Введите имя нового соединителя в текстовом поле **Идентификатор соединителя**.

4. Нажмите **Создать код активации**.

Код активации для соединителя отобразится в текстовом поле **Код активации соединителя**.

5. Скопируйте код активации, чтобы использовать его при настройке соединителя с помощью файла OVA.

6. Нажмите кнопку **ОК**.

Развертывание файла OVA соединителя

После загрузки файла OVA соединителя его можно развернуть с помощью клиента VMware vSphere Client или vSphere Web Client.

Разверните файл OVA с помощью клиента vSphere Client или vSphere Web Client.

Необходимые условия

- Идентифицируйте DNS-записи и имя узла для развертывания файла OVA соединитель.
- С vSphere Web Client следует использовать браузер Firefox или Chrome. Не используйте Internet Explorer для развертывания файла OVA.
- Загрузите файл в формате OVA, необходимый для настройки соединителя, используя ссылку [Средства и комплект SDK VMware vRealize Automation](#).

Процедура

1. В клиенте vSphere Client или vSphere Web Client выберите **Файл > Развернуть шаблон OVF**.
2. На страницах развертывания шаблона OVF введите данные для развертывания соединитель.

Страница	Описание
Источник	Перейдите к расположению пакета OVA или введите допустимый URL-адрес.
Сведения о шаблоне OVA	Убедитесь, что выбрана правильная версия.
Лицензия	Ознакомьтесь с условиями лицензионного соглашения и нажмите кнопку Принимаю .
Имя и расположение	Введите имя виртуального устройства. Имя должно быть уникальным в пределах папки иерархии и содержать не более 80 символов. Имена следует вводить с учетом регистра. Выберите расположение для виртуального устройства.
Узел или кластер	Выберите узел или кластер, чтобы запустить развернутый шаблон.
Пул ресурсов	Выберите пул ресурсов.
Хранилище	Выберите расположение, в котором будут храниться файлы виртуальной машины.
Формат диска	Выберите формат диска для файлов. Для производственных сред следует использовать формат «толстой» подготовки . Для оценки и тестирования используйте формат «тонкой» подготовки .
Сопоставление сетей	Сопоставьте сети в вашей производственной среде с сетями в шаблоне OVF.

Страница	Описание
Свойства	<p>а) В поле Часовой пояс выберите правильный часовой пояс.</p> <p>б) Флажок «Программа улучшения качества программного обеспечения» установлен по умолчанию. В рамках этой программы VMware собирает анонимные данные о развертывании, чтобы лучше удовлетворять требованиям пользователей. Снимите флажок, чтобы данные не собирались.</p> <p>в) Введите имя узла в текстовом поле «Имя узла». Если оставить это поле пустым, для поиска имени узла будет использоваться обратный поиск DNS.</p> <p>г) Чтобы настроить статический IP-адрес соединитель, введите адрес шлюза по умолчанию, DNS-сервера, маски сети, а также IP-адрес.</p> <hr/> <p>Важно! Если оставить хотя бы одно поле пустым, включая поле «Имя узла», будет использоваться протокол DHCP.</p> <hr/> <p>Чтобы настроить протокол DHCP, оставьте адресные поля пустыми.</p>
Готово к завершению	Проверьте выбранные параметры и нажмите кнопку Готово .

Развертывание может занять несколько минут в зависимости от скорости сети. Ход выполнения можно просмотреть в соответствующем диалоговом окне.

- После завершения развертывания выберите устройство, щелкните его правой кнопкой мыши и выберите **Питание > Включить питание**.

Устройство будет инициализировано. Сведения можно просмотреть на вкладке **Консоль**. После завершения инициализации виртуального устройства на экране консоли отобразится версия и URL-адреса, с помощью которых можно войти в мастер настройки для завершения настройки.

Следующие шаги

Используя мастер настройки, необходимо добавить код активации и пароли администрирования.

Настройка параметров соединителя

После развертывания файла OVA соединителя необходимо запустить мастер настройки, чтобы активировать устройство и задать пароли администратора.

Необходимые условия

- Создан код активации для соединителя.
- Убедитесь, что соединитель включен, и известен его URL-адрес.
- Составьте список паролей для администратора соединителя, учетной записи привилегированного пользователя и учетной записи SSH-пользователя.

Процедура

- Чтобы запустить мастер настройки, введите URL-адрес соединитель, который отобразился на вкладке «Консоль» после развертывания файла OVA.
- На экране приветствия нажмите кнопку **Продолжить**.

- Создайте надежные пароли для учетных записей администратора виртуального устройства соединитель.

Надежные пароли должны состоять не менее чем из 8 символов, и содержать строчные и прописные буквы, а также по крайней мере одну цифру и специальный символ.

Параметр	Описание
Администратор устройства	Создайте пароль для администратора устройства. Имя пользователя — admin . Его нельзя менять. С помощью этой учетной записи и пароля можно входить в службы соединитель, чтобы управлять сертификатами, паролями устройства и конфигурацией системного журнала. Важно! Пароль пользователя admin должен состоять не менее чем из 6 символов.
Привилегированный пользователь	Пароль привилегированного пользователя VMware по умолчанию использовался для установки устройства соединитель. Создайте новый пароль привилегированного пользователя.
учетная запись SSH-пользователя	Создайте пароль для удаленного доступа к устройству соединителя.

- Нажмите кнопку **Продолжить**.
- На странице «Активировать соединитель» вставьте код активации и щелкните **Продолжить**.
- Если используется самозаверяющий сертификат на внутреннем соединителе vRealize Automation, можно получить соответствующий сертификат, выполнив следующую команду на устройстве vRealize Automation: `cat /etc/apache2/server-cert.pem`

Выберите вкладку **Сквозное подключение SSL на подсистеме балансировки нагрузки**, а затем выберите ссылку `/horizon_workspace_rootca.pem`.

После проверки кода активации и установления соединения между службой и экземпляром соединителя настройка соединителя завершена.

Следующие шаги

В службе необходимо настроить среду с учетом своих потребностей. Например, если вы добавили дополнительный соединитель, чтобы синхронизировать два встроенных каталога проверки подлинности Windows, необходимо создать каталог и связать его с новым соединителем.

Использование центра открытых сертификатов

При установке службы управления каталогами создается сертификат SSL по умолчанию. В целях тестирования можно использовать сертификат по умолчанию, но для производственной среды нужно создать и установить коммерческие сертификаты SSL.

Если служба управления каталогами указывает на подсистему балансировки нагрузки, сертификат SSL применяется к этой подсистеме.

При импорте сертификата необходимо поставить флажок **Пометить этот ключ как экспортируемый**.

При создании запроса подписи для пользовательского сертификата необходимо указать только имя сертификата (CN) или имя домена узла центра сертификации.

Необходимые условия

Создайте запрос подписи сертификата и получите действительный подписанный сертификат из центра сертификации. Если ваша организация предоставляет сертификаты SSL, подписанные в центре сертификации, их также можно использовать. У файлов сертификатов должен быть формат PEM.

Процедура

1. Войдите на страницу администрирования устройства соединителя, используя учетную запись администратора, по следующему адресу:
`https://myconnector.mycompany:8443/cfg`
2. В консоли администратора щелкните **Настройки устройства**.
По умолчанию выбрана конфигурация виртуального устройства.
3. Щелкните **Управлять настройками**.
4. Введите пароль пользователя-администратора для сервера VMware Identity Manager.
5. Выполните команду **Установить сертификат**.
6. В разделе «Сквозное подключение SSL» на вкладке **Устройство Identity Manager** выберите пункт **Пользовательский сертификат**.
7. В текстовом поле **Цепочка сертификатов SSL** вставьте имя узла, промежуточные и корневые сертификаты (в таком же порядке).

Сертификат SSL будет использоваться, только если указать всю цепочку сертификатов в правильном порядке. Для каждого сертификата скопируйте все содержимое между линиями и сами линии «-----BEGIN CERTIFICATE-----» и «-----END CERTIFICATE-----».

Убедитесь, что в сертификате содержится полное доменное имя узла.
8. Вставьте закрытый ключ в текстовом поле «Закрытый ключ». Скопируйте все содержимое между «-----BEGIN RSA PRIVATE KEY» и «-----END RSA PRIVATE KEY».
9. Нажмите кнопку **Сохранить**.

Пример. Примеры сертификатов

Пример цепочки сертификатов

```
-----BEGIN CERTIFICATE-----
jIQt9WdR9Vpg3WQT5+C3HU17bUOvwHP/rO+
...
...
W53+O05j5xsxZDJfWr1lqBIFF/OkIYCPcyK1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```

Пример цепочки сертификатов

```
WdR9Vpg3WQT5+C3HU17bUOwvhp/rjlQvt90+
```

```
...
```

```
...
```

```
...
```

```
O05j5xsxzDJfWr1lqBIFF/OkiYCPW53+cyK1
```

```
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
```

```
dR9Vpg3WQTjQvt9W5+C3HU17bUOwvhp/r0+
```

```
...
```

```
...
```

```
...
```

```
5j5xsxzDJfWr1lqW53+O0BIFF/OkiYCPcyK1
```

```
-----END CERTIFICATE-----
```

Пример цепочки закрытых ключей

```
-----BEGIN RSA PRIVATE KEY-----
```

```
jQvtg3WQT5+C3HU17bU9WdR9VpOwvhp/r0+
```

```
...
```

```
...
```

```
...
```

```
1lqBIFFW53+O05j5xsxzDJfWr/OkiYCPcyK1
```

```
-----END RSA PRIVATE KEY-----
```

Создание поставщика удостоверений рабочей области

Необходимо создать поставщика удостоверений рабочей области, который будет использовать внешний соединитель.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Управление каталогами > Поставщики удостоверений**.
2. Выберите **Добавить поставщика удостоверений**.
3. Выберите **Создать поставщика удостоверений рабочей области**.
4. Введите имя поставщика удостоверений в поле **Имя поставщика удостоверений**.
5. Выберите соответствующий каталог пользователей, которые будут использовать этого поставщика удостоверений.

Выбор каталога определяет, какие соединители будут доступны для данного поставщика удостоверений.

6. Выберите один или несколько внешних соединителей, настроенных для проверки подлинности с помощью смарт-карт.

Примечание Если для развертывания указано расположение вне подсистемы балансировки нагрузки, введите ее URL-адрес.

7. Выберите сеть для доступа к данному поставщику удостоверений.
8. Нажмите кнопку **Добавить**.

Настройка проверки подлинности на основе сертификата и правил политики доступа по умолчанию

Для Active Directory и домена vRealize Automation необходимо настроить внешний соединитель.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Управление каталогами > Соединители**.
2. Выберите необходимый соединитель в столбце **Рабочий процесс**.
Выбранный рабочий процесс будет отображаться в текстовом поле **Имя рабочего процесса** на вкладке соединителя **Подробные сведения**, а сведения о типе соединителя — в текстовом поле **Тип соединителя**.
3. Убедитесь, что соединитель связан с необходимым каталогом Active Directory. Для этого следует указать соответствующий каталог в текстовом поле **Связанный каталог**.
4. Введите соответствующее имя домена в текстовом поле **Связанные домены**.
5. Выберите вкладку **Адаптеры проверки подлинности** и включите элемент CertificateAuthAdapter.
6. Настройте проверку подлинности на основе сертификата согласно развертыванию.
См. раздел [Настройка проверки подлинности сертификата для управления каталогами](#).
7. Выберите **Администрирование > Управление каталогами > Политики**.
8. Щелкните **Изменить политику по умолчанию**.
9. Добавьте сертификат в правила политики и сделайте его первым в списке методов проверки подлинности.
Сертификат должен быть первым в списке методов проверки подлинности в правиле политики. В противном случае проверка подлинности на основе сертификата завершится сбоем.

Создание ссылки на Active Directory в нескольких доменах или лесах

Системному администратору необходимо настроить ссылку на Active Directory в нескольких доменах или лесах.

Процедура настройки ссылки на Active Directory в нескольких доменах или лесах по существу одинакова. Для ссылки на среду с несколькими лесами требуется двунаправленное доверие между всеми применимыми доменами.

Необходимые условия

- Установите распределенное развертывание vRealize Automation с соответствующей подсистемой балансировки нагрузки. См. *Установка vRealize Automation*.
- Войдите в vRealize Automation в качестве **администратора арендатора**.
- Настройте соответствующие домены и леса Active Directory для своего развертывания.

Процедура

1. Выберите **Администрирование > Управление каталогами > Каталоги**.
2. Щелкните **Добавить каталог**.
3. На странице «Добавить каталог» укажите имя для сервера Active Directory в текстовом поле **Имя каталога**.
4. Выберите **Active Directory (со встроенной проверкой подлинности Windows)** под заголовком **Имя каталога**.
5. Настройте соединитель, синхронизирующий пользователей Active Directory с каталогом VMware Directories Management в разделе «Синхронизация каталогов и проверка подлинности».

Параметр	Описание
Соединитель синхронизации	Выберите соответствующий соединитель для использования в системе. Каждое устройство vRealize Automation содержит соединитель по умолчанию. Если вам требуется помощь при выборе соединителя, обратитесь к системному администратору.
Проверка подлинности	Нажмите соответствующий переключатель, чтобы обозначить, выполняет ли выбранный соединитель проверку подлинности.
Атрибут поиска каталогов	Выберите соответствующий атрибут учетной записи, который содержит имя пользователя.

В зависимости от конфигурации развертывания для использования будут доступны один или несколько соединителей.

6. Введите соответствующие учетные данные домена присоединения в текстовых полях **Имя домена**, **Имя администратора домена** и **Пароль администратора домена**.

Например, можно ввести что-то подобное: **Имя домена**: `hs.trcint.com`, **Имя администратора домена**: `devadmin`, **Пароль администратора домена**: `xxxx`.

7. В разделе **Сведения о привязке пользователя** введите соответствующие учетные данные Active Directory (со встроенной проверкой подлинности Windows), чтобы упростить синхронизацию каталогов.

Параметр	Описание
Имя UPN пользователя привязки домена	Введите имя участника-пользователя для пользователя, который может выполнить проверку подлинности домена. Например, UserName@example.com.
Пароль имени домена привязки	Введите пароль пользователя привязки.

8. Нажмите **Сохранить и Далее**.

Появляется страница «Выбрать домены» со списком доменов.


9. Отметьте флажками соответствующие строчки, чтобы выбрать необходимые домены для развертывания системы.

10. Щелкните **Далее**.

11. Убедитесь, что имена атрибутов каталога Directories Management сопоставляются с нужными атрибутами Active Directory.

Если имена атрибутов каталога сопоставлены неправильно, выберите нужный атрибут Active Directory в раскрывающемся меню.

12. Нажмите кнопку **Далее**.

13. Щелкните , чтобы выбрать группы, которые должны синхронизироваться из Active Directory с каталогом.

Если при добавлении группы Active Directory ее участников нет в списке пользователей, они будут добавлены.

Примечание Система проверки подлинности пользователей Directories Management импортирует данные из Active Directory при добавлении групп и пользователей, при этом быстродействие системы ограничивается возможностями Active Directory. В результате операции импорта могут продолжаться очень долго в зависимости от количества добавляемых пользователей и групп. Для уменьшения вероятности появления задержек или проблем сократите количество групп и пользователей и выберите только те из них, которые требуются для работы системы vRealize Automation. При уменьшении производительности системы или возникновении ошибок закройте все ненужные приложения и убедитесь, что для службы Active Directory в системе выделен соответствующий объем памяти. Если проблема не исчезает, увеличьте соответствующим образом объем памяти, выделенной для Active Directory. Для систем с большим количеством пользователей и групп может понадобиться увеличить объем памяти, выделенной Active Directory, до 24 Гб.

14. Щелкните **Далее**.

15. Щелкните **+**, чтобы добавить дополнительных пользователей. Например, введите **CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com**.

Для исключения пользователей щелкните **+**, чтобы создать фильтр для исключения некоторых типов пользователей. Вы выбираете атрибут пользователя для фильтрации, правило запроса и значение.

16. Щелкните **Далее**.
17. Посмотрите на странице, сколько пользователей и групп синхронизируются с каталогом.
Если нужно изменить пользователей и группы, щелкните ссылки «Изменить».
18. Щелкните **Отправить в Workspace**, чтобы начать синхронизацию с каталогом.

Следующие шаги

Настройка групп и ролей пользователей

Администраторы арендатора создают бизнес-группы и настраиваемые группы, а также предоставляют пользователям права доступа к консоли vRealize Automation.

Назначение ролей пользователям или группам

Администраторы арендатора предоставляют пользователям права доступа, назначая роли пользователям или их группам.

Чтобы пользователи или группы пользователей могли изменять и запускать процесс, необходимо назначить им разрешения. Если пользователям или группам пользователей назначена роль «Диспетчер выпусков», они могут изменять и запускать процесс. Если пользователям или группам пользователей назначена роль «Инженер выпусков», они могут запускать процесс. Дополнительную информацию см. в руководстве *Использование vRealize Code Stream*.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Пользователи и группы > Пользователи и группы каталога**.
2. Введите имя пользователя или группы в поле **Поиск** и нажмите клавишу ВВОД.
Не используйте в имени знак @, обратную косую черту (\) или косую черту (/). Чтобы оптимизировать поиск, введите полностью имя пользователя или группы в формате «пользователь@домен».
3. Щелкните имя пользователя или группы, которым необходимо назначить роли.
4. Выберите одну или несколько ролей в списке «Добавление ролей для этого пользователя».
В списке «Полномочия, предоставленные выбранными ролями» перечислены предоставляемые полномочия.

5. (дополнительно) Нажмите кнопку **Далее**, чтобы просмотреть дополнительные сведения о пользователе или группе.
6. На вкладке **Общие** страницы **Сведения о пользователе** прокрутите список ролей, чтобы добавить пользователя.
 - а) Чтобы дать пользователю разрешения на изменение и запуск процесса установите флажок **Диспетчер выпусков**.
 - б) Чтобы дать пользователю разрешения на запуск процесса установите флажок **Инженер выпусков**.
7. Щелкните **Обновить**.

Результаты

Пользователи, вошедшие в службу vRealize Automation, должны выйти и войти обратно в vRealize Automation, прежде чем переходить на страницы, к которым они получили доступ.

Следующие шаги

При необходимости можно создавать собственные настраиваемые группы из пользователей и групп в подключениях Active Directory. См. раздел [Создание настраиваемой группы](#).

Создание настраиваемой группы

Администраторы арендатора могут создавать настраиваемые группы, объединяя другие настраиваемые группы, группы хранилища удостоверений и отдельных пользователей хранилища удостоверений. Настраиваемые группы обеспечивают более детальный контроль над доступом в vRealize Automation, чем бизнес-группы, которые соответствуют бизнес-подразделению, отделу или другому организационному подразделению.

Настраиваемые группы позволяют предоставлять права доступа для задач более избирательно, чем стандартные назначения групп vRealize Automation. Например, можно создать настраиваемую группу, чтобы разрешить администраторам арендаторов управлять разрешениями для конкретных пользователей в рамках арендатора.

Настраиваемым группам можно назначать роли, но это не всегда обязательно. Например, вы можете создать настраиваемую группу "Утверждающие спецификаций компьютеров", которая будет использоваться для предварительного подтверждения компьютеров. Также можно создавать настраиваемые группы для сопоставления бизнес-групп и централизованного управления всеми группами. В таких случаях роли назначать не нужно.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Пользователи и группы > Настраиваемые группы**.
2. Нажмите кнопку **Создать**.

3. В текстовом поле **Имя** введите имя группы.

Имена настраиваемых групп не должны содержать такие сочетания символов, как точка с запятой (;), за которой стоит знак равенства (=).

4. (дополнительно) В текстовом поле **Описание** введите описание.

5. Выберите одну или несколько ролей в списке «Добавление ролей для этой группы».

В списке «Полномочия, предоставленные выбранными ролями» перечислены предоставляемые полномочия.

6. Нажмите кнопку **Далее**.

7. Добавьте пользователей и группы, чтобы создать настраиваемую группу.

а) Введите имя пользователя или группы в поле **Поиск** и нажмите клавишу ВВОД.

Не используйте в имени знак @, обратную косую черту (\) или косую черту (/). Чтобы оптимизировать поиск, введите полностью имя пользователя или группы в формате «пользователь@домен».

б) Выберите пользователя или группу, которых нужно добавить в настраиваемую группу.

8. Щелкните элемент **Готово**.

Результаты

Пользователи, вошедшие в службу vRealize Automation, должны выйти и войти обратно в vRealize Automation, прежде чем переходить на страницы, к которым они получили доступ.

Динамическое добавление пользователей с настраиваемыми группами и правилами

В развернутую систему можно добавлять пользователей vRealize Automation без доступа к Active Directory, используя моментальную регистрацию пользователей. Для применения моментальной регистрации новых пользователей необходимо создать правила заполнения соответствующих настраиваемых групп.

При первоначальном входе в систему динамически добавляемые пользователи распределяются по группам на основе правил, которые создаются на странице мастера «Расширенные параметры участия в группе» (Advanced Group Membership). После первоначального входа в систему можно назначать членство в группе в обычном режиме. На этой странице, которая является второй страницей мастера, содержатся четыре поля выбора для создания правил, базирующихся на различных критериях, которые определяют динамически добавляемых пользователей.

Например, в первом поле выбора правил в качестве критерия можно выбрать «Домен» (Domain), а затем во втором поле выбрать «Соответствует» (Matches). После этого в третьем поле правил можно указать домен. Выбранные параметры формируют правило, которое описывает пользователей с динамическим участием, связанных с указанным доменом. Третье поле выбора — это поле для ввода произвольной информации, в котором можно указать любую информацию, логически связанную с информацией, указанной в первых двух полях.

Примечание При настройке динамически добавляемых пользователей в сопоставлении формата NameId указывается атрибут, который используется для однозначного определения пользователя. Этот атрибут, используемый в качестве параметра NameId, должен быть уникальным для данного пользователя, а сам атрибут должен предоставляться в составе утверждения SAML. Изменение атрибута NameId или значения NameId приведет к ошибке при попытке входа. Например, если сопоставить NameId с параметром SAMAccountName пользователя с использованием формата NameId `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`, необходимо также отдельно указать параметр SAMAccountName. Имя пользователя userName и значение SAMAccountName не должны изменяться.

vRealize Automation поддерживает сопоставление с использованием подстановочных знаков для настройки динамически добавляемых пользователей. Дополнительные сведения о подключении и использовании сопоставления с использованием подстановочных знаков см. в документации

[Сопоставления с использованием подстановочных знаков для динамически добавляемых пользователей](#).

Примечание Можно создать несколько правил для заполнения сведений о динамически добавляемых пользователях в соответствии с различными критериями. Если создается несколько правил, то с помощью поля выбора правил **Соответствие**, расположенного над основными полями правил, можно указать, должно ли средство vRealize Automation учитывать соответствие какому-либо из этих правил либо всем этим правилам при заполнении сведений о динамически добавляемых пользователях.

Процедура

1. Выберите **Администрирование > Пользователи и группы > Настраиваемые группы** и найдите существующую группу, например группу, которая подходит для динамически добавляемых пользователей.

Дополнительные сведения см. в разделе [Создание настраиваемой группы](#).

Щелкните строку группы, а не имя группы.

2. Выберите **Расширенные параметры участия**.

При необходимости на странице «Добавление пользователей в группу» (Add Users to Group) можно добавить в группу отдельных пользователей.

3. Нажмите кнопку **Далее** для просмотра страницы «Групповые правила» (Group Rules).

4. С помощью полей соответствия и выбора правил создайте одно или несколько правил, соответствующих вашей конфигурации пользователей.

В трех основных полях выбора правил, расположенных под полем **Соответствие**, нажмите стрелки вниз и введите информацию для активации раскрывающихся меню, с помощью которых можно создать нужное правило. Обратите внимание, что символы * и \ можно использовать так, как описано выше.

5. Нажмите кнопку **Далее**.
6. Чтобы исключить пользователей из группы, найдите и добавьте этих пользователей на страницу «Исключение пользователей из группы» (Exclude Users from Group).
7. Нажмите кнопку **Далее**.
8. Проверьте конфигурацию группы на странице «Проверка» (Review) и нажмите кнопку **Сохранить**, чтобы сохранить и применить правила и конфигурации.

Результаты

Динамически добавляемые пользователи будут добавляться в соответствии с созданными правилами.

Сопоставления с использованием подстановочных знаков для динамически добавляемых пользователей

В vRealize Automation можно использовать правила сопоставления на основе подстановочных знаков для настройки параметров динамически добавляемых пользователей.

Включение сопоставления на основе подстановочных знаков

Сопоставление на основе подстановочных знаков по умолчанию отключено. Чтобы включить сопоставление на основе подстановочных знаков, выполните соответствующую команду REST API, которая выглядит следующим образом.

```
PUT:- https://{VRA_HOSTNAME}/SAAS/t/VSPHERE.LOCAL/jersey/manager/api/system/config/
isDynamicGroupWildcardEnabled
Content-Type: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Accept: application/vnd.vmware.horizon.manager.systemconfigparameter+json
Authorization: HZN <token> (edited)
{
  "name": "isDynamicGroupWildcardEnabled",
  "values": {
    "values": [
      "true"
    ]
  }
}
```

Маркер HZN, предоставляемый API-интерфейсу, который обеспечивает настройку с использованием подстановочных знаков, должен быть назначен пользователю с правами администратора в арендаторе vsphere.local.

Сопоставление атрибутов в утверждении SAML с атрибутами пользователей vRealize Automation

Имя атрибута в утверждении SAML должно полностью соответствовать имени атрибута, определенному на странице «Атрибуты пользователя» в vRealize Automation. Атрибут SAML, содержащий имя пользователя, должен называться `firstName`, а атрибут фамилии должен называться `lastName` и т. д. Если поставщик удостоверений отправляет дополнительные атрибуты пользователей, не заданные на странице «Атрибуты пользователя», администратор должен добавить эти атрибуты на страницу. Например, если поставщик удостоверений отправляет сведения о членстве пользователей в группе в атрибуте SAML с именем `groups` или `memberof`, необходимо добавить на страницу «Атрибуты пользователя» в vRealize Automation атрибут `groups` или `memberof`. Капитализация названий атрибутов должна совпадать.

Примечание Чтобы однозначно определить строку, например `Group_Name`, в многозначном атрибуте, определяющем членство в группе пользователей, создайте следующее выражение с подстановочными знаками: `*Group_Name*`.

Для условий `Match` (Соответствует) и `Doesn't Match` (Не соответствует) можно использовать в качестве подстановочного знака символ звездочки (*), чтобы добавить в правило шаблон сопоставления символов. Например, при вводе `<userinput>*Smi*</userinput>` отображаются результаты `Smith`, `Smiley`, `Smirnoff` и другие похожие варианты, в том числе те, в которых сочетание `smi` стоит в середине слова. Чтобы найти все точные совпадения с шаблоном, добавьте обратную косую черту (\) перед звездочкой (*) при вводе шаблона. Например, при вводе `<userinput>*Adam*</userinput>` будут найдены все имена, полностью совпадающие с шаблоном `Adam*`. Можно использовать символ * в любой части фразы. Перед ним и после него можно добавить любой символ, в том числе `&`; *.

Создание бизнес-группы

Бизнес-группы применяются для связывания набора служб и ресурсов с группой пользователей. Часто эти группы соответствуют бизнес-подразделению, отделу или иным организационным единицам. Благодаря созданию бизнес-группы можно настроить резервирования и предоставлять пользователям право на подготовку элементов каталога служб для участников бизнес-группы.

К роли бизнес-группы можно добавить несколько отдельных пользователей поочередно или одновременно. Чтобы сделать последнее, нужно добавить к роли группу хранилища удостоверений или настраиваемую группу. Например, можно создать настраиваемую группу «Команда поддержки продаж» и добавить ее к роли поддержки. Использовать можно также существующие пользовательские группы хранилища удостоверений. Выбранные вами пользователи и группы должны быть допустимыми в хранилище удостоверений.

Для поддержки интеграции vCloud Director участники бизнес-группы vRealize Automation должны также быть членами организации vCloud Director.

После того как администратор арендатора создаст бизнес-группу, менеджер бизнес-группы получает разрешение на изменение своего адреса электронной почты и участников группы. Администратор арендатора может изменять значения всех параметров.

Эта процедура предполагает, что компонент Инфраструктура как услуга установлен и настроен.

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора арендатора**.
- Если необходимо добавить компьютеры, созданные членами бизнес-группы, к конкретной организационной единице Active Directory, настройте соответствующую политику Active Directory. См. раздел [Создание политики Active Directory](#). Эту политику можно настроить и применить при создании бизнес-группы. Кроме того, политику можно добавить позднее.
- Если для группы требуется предоставить префикс компьютера по умолчанию, который добавляется к началу имени подготовленного компьютера, запросите этот префикс у администратора структуры. См. раздел [Настройка префиксов компьютеров](#). Префиксы компьютеров не применяются к запросам Все как услуга.

Процедура

1. Выберите **Администрирование > Пользователи и группы > Бизнес-группы**.
2. Выберите значок **Создать (+)**.
3. Настройте сведения о бизнес-группе.

Параметр	Описание
Имя	Введите имя бизнес-группы.
Описание	Введите описание.
Адрес для отправки оповещений о ресурсах:	Введите один или несколько адресов электронной почты пользователей, которые будут получать оповещения о емкости. Псевдонимы электронной почты не поддерживаются, каждый эл. адрес должен принадлежать определенному пользователю. Отделяйте каждую запись запятой. Например, JoeAdmin@mycompany.com,WeiMgr@mycompany.com .
Политика Active Directory	Выберите для бизнес-группы политику Active Directory по умолчанию.

4. Добавьте настраиваемые свойства.
5. Нажмите кнопку **Далее** для перехода к странице участников.
6. Введите имя пользователя или имя настраиваемой группы пользователей и нажмите клавишу ВВОД.

В бизнес-группу можно добавить одного или несколько пользователей либо настраиваемых групп пользователей. Пользователей можно указать прямо сейчас либо создать пустые бизнес-группы и заполнить их позже.

Параметр	Описание
Роль диспетчера групп	Может создавать права и назначать политики подтверждения для группы.
Роль поддержки	Может запрашивать элементы каталога служб и управлять ими от имени других участников бизнес-группы.

Параметр	Описание
Роль пользователя с общим доступом	Может использовать ресурсы и выполнять действия с ресурсами, которые развернуты другими участниками бизнес-группы.
Роль пользователя	Может запрашивать элементы каталога служб, на которые пользователю предоставлены права.

7. Нажмите кнопку **Далее** для перехода к странице инфраструктуры.

8. Настройте параметры инфраструктуры по умолчанию.

Параметр	Описание
Префикс компьютера по умолчанию	<p>Выберите предварительно настроенный префикс компьютера для бизнес-группы. Этот префикс используется схемами элементов компьютера. Если схема элементов использует префикс по умолчанию и он здесь не указан, то префикс компьютера создается на основе имени бизнес-группы. Наилучшим решением будет выбор префикса по умолчанию. Вы можете по-прежнему настраивать схемы элементов с конкретными префиксами или позволять пользователям каталога служб переопределять их, когда они запрашивают схему элементов.</p> <p>В схемах элементов Все как услуга префиксы компьютера по умолчанию не используются. Если вы настраиваете здесь префикс и предоставляете право этой бизнес-группе на схему элементов Все как услуга, это не влияет на процесс подготовки компьютера Все как услуга.</p>
Контейнер Active Directory	<p>Введите контейнер Active Directory. Этот параметр применяется только для подготовки WIM.</p> <p>Для других способов подготовки требуется дополнительная настройка, чтобы добавить подготовленные компьютеры в контейнер AD.</p>

9. Щелкните элемент **Готово**.

Результаты

Администраторы структуры могут выделять ресурсы вашей бизнес-группе путем создания резервирования. Менеджеры бизнес-группы могут создавать права для участников бизнес-группы.

Следующие шаги

- Создайте резервирование для своей бизнес-группы с учетом того, где бизнес-группа выполняет подготовку компьютеров. См. раздел [Выбор сценария резервирования](#).
- Если элементы каталога опубликованы и службы существуют, вы можете создать право для участников бизнес-группы. См. раздел [Предоставление пользователям права на использование службы, элементов каталога и действий](#).

Устранение неполадок, связанных с низкой производительностью при отображении участников группы

Участники бизнес-группы или настраиваемой группы отображаются медленно при просмотре сведений о группе.

Проблема

При просмотре информации о пользователях в среде с большим количеством пользователей их имена медленно загружаются в интерфейсе пользователя.

Причина

В системах с большой средой Active Directory загрузка имен выполняется медленно.

Решение

- ◆ С целью уменьшения рабочей нагрузки в процессе поиска не добавляйте сотни отдельных участников по имени, а максимально часто используйте группы Active Directory или настраиваемые группы.

Устранение неполадок, связанных с неожиданными записями для фильтрации

В списке бизнес-групп, используемом для выбора параметров фильтра, отображаются неподвижные или повторяющиеся записи.

Проблема

Вы внесли изменения в бизнес-группы в разделе **Администрирование > Пользователи и группы > Бизнес-группы**. На странице «Развертывания» при попытке отфильтровать развертывания по бизнес-группе в списке бизнес-групп, доступных для фильтрации, не отражаются внесенные изменения или отображаются неподвижные результаты (например, повторяющиеся бизнес-группы).

Причина

Система производит опрос на предмет изменений каждые 30 минут.

Решение

Подождите полчаса и обновите страницу браузера, чтобы обновить список выбранных параметров фильтрации бизнес-групп.

Создание дополнительных арендаторов

Как системный администратор вы можете создать дополнительных арендаторов vRealize Automation, чтобы пользователи могли получать доступ к соответствующим приложениям и ресурсам, которые необходимы им для работы.

Арендатор — это группа пользователей со специальными привилегиями, которые работают в пределах экземпляра программного обеспечения. Как правило, арендатор vRealize Automation по умолчанию создается в процессе установки системы и ее начальной настройки. После этого администраторы могут создать дополнительных арендаторов, чтобы пользователи могли осуществлять вход в систему и выполнять свои рабочие задачи. Администраторы могут создать столько арендаторов, сколько требуется для работы системы. При создании арендаторов администраторы должны указать базовую конфигурацию, включая имя, URL-адрес входа в систему, локальных пользователей и администраторов. После ввода

основных сведений об арендаторе администратор арендатора должен войти в систему и настроить соответствующее подключение Active Directory с помощью функции управления каталогами на вкладке «Администрирование» консоли vRealize Automation. Кроме того, администраторы арендатора могут применять пользовательскую фирменную символику для арендаторов.

Необходимые условия

Войдите в консоль vRealize Automation в качестве **системного администратора**.

Процедура

1. (Необязательно) Указание информации об арендаторе

Первый шаг в настройке арендатора — присвоить имя новому арендатору, добавить его в vRealize Automation и создать URL-адрес доступа для конкретного арендатора.

2. (Необязательно) Настройка локальных пользователей

Администратор системы vRealize Automation должен настроить локальных пользователей для каждого применимого арендатора.

3. (Необязательно) Назначение администраторов

В хранилищах удостоверений, которые вы настроили для арендатора, можно назначить одного или нескольких администраторов арендатора и администраторов инфраструктуры как услуги.

Указание информации об арендаторе

Первый шаг в настройке арендатора — присвоить имя новому арендатору, добавить его в vRealize Automation и создать URL-адрес доступа для конкретного арендатора.

Необходимые условия

Войдите в консоль vRealize Automation в качестве **системного администратора**.

Процедура

1. Выберите **Администрирование > Арендаторы**.
2. Выберите значок **Создать (+)**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. Введите уникальный идентификатор для арендатора в текстовом поле **URL-имя**.

Этот URL-маркер используется для добавления идентификатора определенного арендатора в URL-адрес консоли vRealize Automation.

Например, введите **mytenant**, чтобы создать URL-адрес `https://vrealize-appliance-hostname.domain.name/vcac/org/mytenant`.

Примечание В vRealize Automation версии 7.0 и 7.1 URL-адрес арендатора может содержать только строчные символы.

6. (дополнительно) Введите адрес электронной почты в текстовом поле **Контактный адрес эл. почты**.
7. Щелкните элемент **Отправить и перейти далее**.

Настройка локальных пользователей

Администратор системы vRealize Automation должен настроить локальных пользователей для каждого применимого арендатора.

После того как администратор создаст общие сведения для арендатора, вкладка «Локальные пользователи» становится активной, и администратор может указать пользователей, которые могут получать доступ к арендатору. По окончании настройки арендатора локальные пользователи арендатора могут выполнять вход в своих арендаторов для выполнения рабочих заданий.

Примечание После добавления пользователя его конфигурацию нельзя изменить. Если необходимо изменить какой-либо элемент конфигурации пользователя, следует удалить пользователя и создать его заново.

Процедура

1. На вкладке «Локальные пользователи» нажмите кнопку **Добавить**.
2. Введите имена и фамилии пользователей в поля **Имя** и **Фамилия** в диалоговом окне «Сведения о пользователях».
3. Введите адрес электронной почты пользователя в поле **Электронная почта**.
4. Введите идентификатор и пароль для пользователя в полях **Имя пользователя** и **Пароль**.
5. Нажмите кнопку **Добавить**.
6. Повторите эту процедуру для всех локальных пользователей арендатора.

Результаты

Указанные локальные пользователи созданы для арендатора.

Назначение администраторов

В хранилищах удостоверений, которые вы настроили для арендатора, можно назначить одного или нескольких администраторов арендатора и администраторов инфраструктуры как услуги.

Администраторы арендатора отвечают за настройку специальной фирменной символики арендатора, а также за управление хранилищами удостоверений, пользователями, группами, правами и общими схемами элементов в контексте своего арендатора. Администраторы инфраструктуры как услуги отвечают за настройку конечных точек-источников инфраструктуры в IaaS, назначение администраторов структуры и мониторинг журналов инфраструктуры как услуги.

Необходимые условия

- Перед назначением администраторов инфраструктуры как услуги необходимо установить саму инфраструктуру IaaS. Дополнительные сведения об установке инфраструктуры как услуги см. в разделе *Установка vRealize Automation*.

Процедура

1. Введите имя пользователя или группы в поле поиска **Администраторы арендатора** и нажмите клавишу ВВОД.

Чтобы быстрее получить результаты, введите полное имя пользователя или группы, например myAdmins@mycompany.domain. Повторите этот шаг, чтобы назначить дополнительных администраторов арендатора.
2. Если установлена инфраструктура как услуга, введите имя пользователя или группы в поле поиска **Администраторы инфраструктуры как услуги (IaaS)** и нажмите клавишу ВВОД.

Чтобы быстрее получить результаты, введите полное имя пользователя или группы, например IaaSAdmins@mycompany.domain. Повторите этот шаг, чтобы назначить дополнительных администраторов инфраструктуры.
3. Нажмите кнопку **Добавить**.

Удаление арендатора

Системный администратор может удалить ненужные арендаторы из vRealize Automation.

При удалении арендатор будет немедленно удален из интерфейса vRealize Automation, но полное его удаление из развертывания может занять несколько часов. Если после удаления арендатора необходимо создать другой арендатор с тем же URL-адресом, подождите несколько часов до полного удаления, прежде чем создавать новый арендатор.

Необходимые условия

Войдите в консоль vRealize Automation в качестве **системного администратора**.

Процедура

1. Выберите **Администрирование > Арендаторы**.
2. Выберите арендатор, который необходимо удалить.

Не щелкайте действительное имя для выбора арендатора. В этом случае арендатор откроется для изменения.
3. Нажмите кнопку **Удалить**.

Результаты

Арендатор будет удален из развертывания vRealize Automation.

Настройка параметров безопасности в средах с несколькими арендаторами

В средах с несколькими арендаторами можно настраивать доступность объектов безопасности NSX для арендаторов.

При создании объекта безопасности NSX для него по умолчанию задается либо глобальная доступность (доступность во всех арендаторах, для которых создано резервирование связанной конечной точки), либо статус «Скрыт» (Hidden) (для всех пользователей, кроме администратора).

Доступность объектов безопасности в различных арендаторах зависит от того, имеется ли у связанной конечной точки резервирование или политика резервирования в арендаторе.

Средства, с помощью которых настраиваются доступность новых объектов безопасности в арендаторах и особенности функционирования существующих объектов безопасности в средах с несколькими арендаторами после обновления до этой версии vRealize Automation, рассмотрены в следующей теме [Управление доступом к объектам безопасности из арендаторов в vRealize Automation](#).

Настройка пользовательской фирменной символики

vRealize Automation позволяет применять пользовательскую фирменную символику для страниц входа и приложений арендатора.

Пользовательская фирменная символика позволяет настроить цвета текста и фона, логотипы и название компании, политики конфиденциальности, уведомления об авторских правах и другую актуальную информацию, которая должна отображаться на страницах входа или приложений арендатора.

Пользовательская фирменная символика для страницы входа арендатора

С помощью страницы «Фирменная символика на экране входа» можно применить пользовательскую фирменную символику к странице входа арендатора vRealize Automation.

На страницах входа арендаторов можно использовать фирменную символику vRealize Automation по умолчанию или настроить пользовательскую символику с помощью страницы «Фирменная символика на экране входа». Обратите внимание, что пользовательская фирменная символика применяется одинаково ко всем приложениям арендаторов.

Эта страница позволяет настроить фирменную символику на всех страницах входа арендатора.

На странице «Фирменная символика на экране входа» в области предварительного просмотра отображается фирменная символика, которая используется для входа в арендатор в данный момент.

Примечание После сохранения новой фирменной символики для страницы входа арендатора возможна задержка до пяти минут перед ее отображением на всех страницах входа.

Необходимые условия

Чтобы использовать собственную эмблему или другое изображение для фирменной символики, понадобится соответствующий файл.

Процедура

1. Войдите в службу vRealize Automation от имени системного администратора или администратора арендатора.
2. Откройте вкладку **Администрирование**.
3. Выберите **Фирменная символика > Фирменная символика на экране входа**

4. Чтобы добавить эмблему, нажмите кнопку **Передать** под полем «Эмблема», а затем перейдите в соответствующую папку и выберите файл изображения эмблемы.
5. Чтобы добавить еще одну эмблему, нажмите кнопку **Передать** под полем «Изображение» (необязательно), а затем перейдите в соответствующую папку и выберите дополнительный файл изображения.
6. Чтобы изменить цвета фона, введите соответствующие шестнадцатеричные коды в полях **Цвет фона**, **Цвет заголовка**, **Цвет фона кнопки входа** и **Цвет переднего плана кнопки входа**.
При необходимости найдите в Интернете список шестнадцатеричных кодов цвета.
7. Для применения своих параметров нажмите **Сохранить**.

Результаты

Пользователи арендатора будут видеть пользовательскую фирменную символику на страницах входа.

Пользовательская фирменная символика для приложений арендатора

Чтобы применить пользовательскую фирменную символику к приложениям арендатора vRealize Automation, воспользуйтесь страницей «Фирменная символика приложения».

В пользовательских приложениях можно использовать фирменную символику vRealize Automation по умолчанию или настроить пользовательскую символику с помощью страницы «Фирменная символика». Эта страница позволяет настроить фирменную символику в верхнем и нижнем колонтитулах страниц приложений. Обратите внимание, что пользовательская фирменная символика применяется одинаково ко всем пользовательским приложениям.

В нижней части страницы «Фирменная символика приложения» отображается фирменная символика, которая используется в колонтитулах в данный момент.

Необходимые условия

Чтобы использовать собственную эмблему в своей фирменной символике, понадобится файл изображения эмблемы.

Процедура

1. Войдите в службу vRealize Automation от имени системного администратора или администратора арендатора.
2. Откройте вкладку **Администрирование**.
3. Выберите **Фирменная символика > Фирменная символика приложения**
4. Перейдите на вкладку **Заголовок**, если она еще не активна.
5. Чтобы использовать фирменную символику vRealize Automation по умолчанию, установите флажок **Использовать значение по умолчанию**.

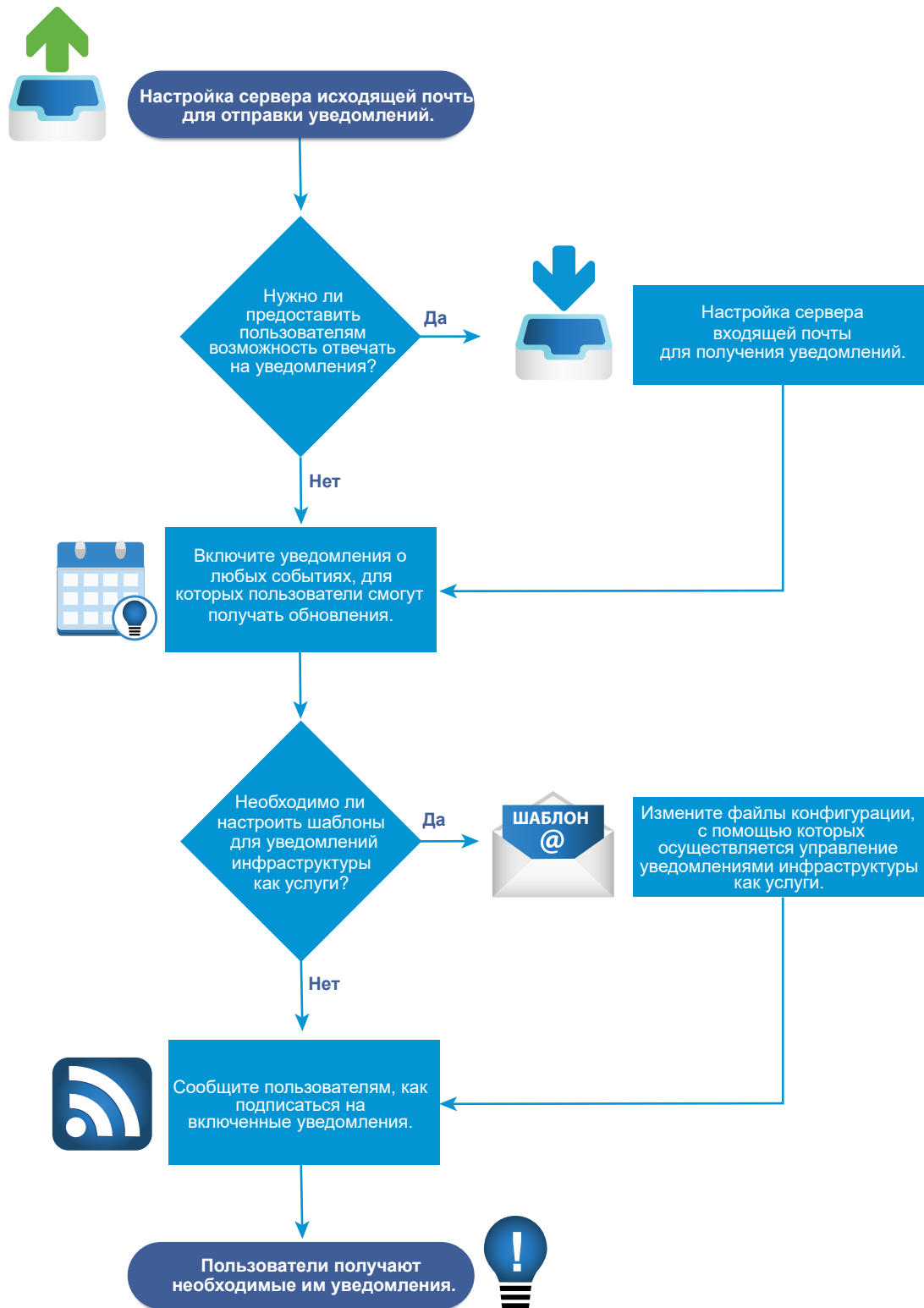
6. Чтобы применить пользовательскую фирменную символику, выберите соответствующие значения в полях на вкладках **Заголовок** и **Нижний колонтитул**.
 - а) Нажмите кнопку **Обзор** в поле **Эмблема в заголовке**, затем перейдите в соответствующую папку и выберите файл изображения эмблемы.
 - б) Введите соответствующее имя компании в поле **Название компании**.
Указанное имя отображается, когда пользователь наводит мышь на эмблему.
 - в) Введите соответствующее название в поле **Название продукта**.
Введенное здесь имя отображается в верхнем колонтитуле приложения рядом с эмблемой.
 - г) В поле **Шестнадцатеричное значение цвета фона** введите соответствующий шестнадцатеричный код цвета фона для периметра приложения.
При необходимости найдите в Интернете список шестнадцатеричных кодов цвета.
 - д) В поле **Шестнадцатеричное значение цвета текста** введите соответствующий шестнадцатеричный код цвета текста.
При необходимости найдите в Интернете список шестнадцатеричных кодов цвета текста.
 - е) Нажмите кнопку **Далее**, чтобы активировать вкладку «Нижний колонтитул».
 - ж) Введите нужное уведомление в поле **Уведомление об авторских правах**.
 - з) Введите ссылку на уведомление о политике конфиденциальности компании в поле **Ссылка на политику конфиденциальности**.
 - и) Введите необходимую контактную информацию компании в поле **Ссылка для связи**.
7. Щелкните **Обновить**, чтобы применить конфигурацию фирменной символики.

Результаты

Пользователи арендатора будут видеть пользовательскую фирменную символику на страницах своих приложений.

Контрольный список для настройки уведомлений

В vRealize Automation можно настроить отправку уведомлений пользователям при наступлении определенных событий. Пользователи могут выбрать, на какие уведомления подписаться, но только для тех событий, для которых включена отправка уведомлений.



Контрольный список для настройки уведомлений позволяет получить общее представление о последовательности шагов, которые необходимо выполнить, чтобы настроить уведомления. В нем также приведены ссылки на описание точек принятия решений и подробные инструкции для каждого шага.

Таблица 2-10. Контрольный список для настройки уведомлений

Задача	Требуемая роль	Сведения
<input type="checkbox"/> Настройка сервера исходящей почты для отправки уведомлений.	<ul style="list-style-type: none"> ■ Системные администраторы настраивают глобальные серверы по умолчанию. ■ Администраторы арендаторов настраивают серверы для своих арендаторов. 	<p>Сведения о том, как настроить сервер для арендатора в первый раз, см. в разделе Добавление сервера исходящей электронной почты для конкретного арендатора. Если необходимо переопределить глобальный сервер по умолчанию, см. раздел Переопределение сервера исходящей почты системы по умолчанию. Чтобы настроить глобальные серверы по умолчанию для всех арендаторов, см. раздел Создание глобального сервера исходящей электронной почты.</p>
<input type="checkbox"/> (Необязательно.) Настройка сервера входящей почты, чтобы пользователи могли завершать выполнение задачи, отвечая на уведомления.	<ul style="list-style-type: none"> ■ Системные администраторы настраивают глобальные серверы по умолчанию. ■ Администраторы арендаторов настраивают серверы для своих арендаторов. 	<p>Сведения о том, как настроить сервер для арендатора в первый раз, см. в разделе Добавление сервера входящей электронной почты для конкретного арендатора. Если необходимо переопределить глобальный сервер по умолчанию, см. раздел Переопределение сервера входящей почты системы по умолчанию.</p> <p>Сведения о том, как настроить глобальный сервер по умолчанию для всех арендаторов, см. в разделе Создание глобального сервера входящей электронной почты.</p>
<input type="checkbox"/> При необходимости можно указать дату отправки уведомления по электронной почте до даты окончания срока действия компьютера.	Системный администратор	См. раздел Настройка даты для уведомления электронной почты об истечении срока действия компьютера .
<input type="checkbox"/> Выбор событий vRealize Automation, при наступлении которых пользователям отправляются уведомления. Пользователи могут подписаться только на уведомления о событиях, для которых настроена отправка уведомлений.	Администратор арендатора	См. раздел Настройка уведомлений .

Таблица 2-10. Контрольный список для настройки уведомлений (продолжение)

Задача	Требуемая роль	Сведения
<input type="checkbox"/> (Необязательно.) Настройка шаблонов для уведомлений, отправляемых владельцам компьютеров в связи с событиями, которые касаются их компьютеров, например истечением срока аренды.	Любой пользователь с доступом к подкаталогу \Templates в каталоге установки сервера vRealize Automation (обычно это %SystemDrive%\Program Files x86\VMware\VCAC\Server) может задать шаблоны электронных уведомлений.	См. раздел Настройка шаблонов для автоматической отправки электронной почты в инфраструктуре как услуге .
<input type="checkbox"/> Пользователи будут автоматически подписаны на настроенные уведомления. При необходимости можно предоставить пользователям инструкции по оформлению подписки на включенные уведомления. Пользователи могут по своему усмотрению подписаться только на уведомления, касающиеся их роли.	Все пользователи	См. раздел Подписка на уведомления .

Настройка глобальных почтовых серверов уведомлений

В рамках настройки уведомлений для арендаторов администраторы арендаторов могут добавлять почтовые серверы. Системный администратор может настроить глобальные входящие и исходящие почтовые серверы, которые для арендаторов отображаются как заданные по умолчанию. Если администраторы арендаторов, прежде чем включить уведомления, не переопределяют эти параметры, решение vRealize Automation использует эти глобальные серверы.

Создание глобального сервера входящей электронной почты

Системные администраторы создают глобальный сервер входящей электронной почты для обработки входящих электронных уведомлений, таких как ответы на подтверждения. Можно создать только один сервер входящей электронной почты, который отображается как сервер по умолчанию для всех арендаторов. Если администраторы арендатора, прежде чем включить уведомления, не переопределяют эти параметры, решение vRealize Automation использует этот глобальный сервер.

Необходимые условия

Войдите в консоль vRealize Automation в качестве **системного администратора**.

Процедура

1. Выберите **Администрирование > Почтовые серверы**.
2. Щелкните значок **Добавить (+)**.
3. Выберите элемент **Электронная почта — Входящая**.

4. Нажмите кнопку **ОК**.
5. В текстовом поле **Имя** введите имя.
6. (дополнительно) В текстовом поле **Описание** введите описание.
7. (дополнительно) Установите флажок **SSL**, чтобы использовать SSL для обеспечения безопасности.
8. Выберите протокол сервера.
9. В текстовом поле **Имя сервера** введите имя сервера.
10. В текстовом окне **Порт сервера** введите номер порта сервера.
11. В текстовом окне **Имя папки** введите имя папки для электронных сообщений.
Этот параметр обязателен, только если выбран протокол сервера IMAP.
12. В текстовом поле **Имя пользователя** введите имя пользователя.
13. Введите пароль в текстовом поле **Пароль**.
14. В текстовом поле **Адрес электронной почты** введите адрес, на который смогут отправлять ответ пользователи vRealize Automation.
15. (дополнительно) Выберите элемент **Удалять с сервера**, чтобы удалить с сервера все обработанные электронные сообщения, полученные с помощью службы уведомлений.
16. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.
17. Щелкните элемент **Проверить подключение**.
18. Нажмите кнопку **Добавить**.

Создание глобального сервера исходящей электронной почты

Системные администраторы создают глобальный сервер исходящей электронной почты для обработки исходящих электронных уведомлений. Можно создать только один сервер исходящей электронной почты, который отображается как сервер по умолчанию для всех арендаторов. Если администраторы арендатора, прежде чем включить уведомления, не переопределяют эти параметры, решение vRealize Automation использует этот глобальный сервер.

Необходимые условия

Войдите в консоль vRealize Automation в качестве **системного администратора**.

Процедура

1. Выберите **Администрирование > Почтовые серверы**.
2. Щелкните значок **Добавить (+)**.
3. Выберите элемент **Электронная почта — Исходящая**.
4. Нажмите кнопку **ОК**.
5. В текстовом поле **Имя** введите имя.

6. (дополнительно) В текстовом поле **Описание** введите описание.
7. В текстовом поле **Имя сервера** введите имя сервера.
8. Выберите метод шифрования.
 - Щелкните **Использовать SSL**.
 - Щелкните **Использовать TLS**.
 - Чтобы отправить незашифрованные сообщения, выберите значение **Нет**.
9. В текстовом окне **Порт сервера** введите номер порта сервера.
10. (дополнительно) Если на сервере требуется проверка подлинности, установите флажок **Обязательно**.
 - а) В текстовом поле **Имя пользователя** введите имя пользователя.
 - б) В текстовом поле **Пароль** введите пароль.
11. В текстовом поле **Адрес отправителя** введите адрес, vRealize Automation с которого будут отправлять электронные сообщения.

Этот адрес электронной почты должен соответствовать указанному имени пользователя и паролю.
12. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.
13. Щелкните элемент **Проверить подключение**.
14. Нажмите кнопку **Добавить**.

Добавление сервера исходящей электронной почты для конкретного арендатора

Администраторы арендатора могут добавить сервер исходящей электронной почты, чтобы отправлять пользователям уведомления для завершения таких рабочих элементов, как подтверждения.

У каждого арендатора может быть только один сервер исходящей электронной почты. Если системный администратор уже настроил глобальный сервер исходящей электронной почты, см раздел [Переопределение сервера исходящей почты системы по умолчанию](#).

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора арендатора**.
- Если сервер электронной почты требует проверки подлинности, указанный пользователь должен быть настроен в хранилище удостоверений и принадлежать к бизнес-группе.

Процедура

1. Выберите **Администрирование > Уведомления > Почтовые серверы**.
2. Щелкните значок **Добавить (+)**.
3. Выберите элемент **Электронная почта — Исходящая**.
4. Нажмите кнопку **ОК**.

5. В текстовом поле **Имя** введите имя.
6. (дополнительно) В текстовом поле **Описание** введите описание.
7. В текстовом поле **Имя сервера** введите имя сервера.
8. Выберите метод шифрования.
 - Щелкните **Использовать SSL**.
 - Щелкните **Использовать TLS**.
 - Чтобы отправить незашифрованные сообщения, выберите значение **Нет**.
9. В текстовом окне **Порт сервера** введите номер порта сервера.
10. (дополнительно) Если на сервере требуется проверка подлинности, установите флажок **Обязательно**.
 - а) В текстовом поле **Имя пользователя** введите имя пользователя.
 - б) В текстовом поле **Пароль** введите пароль.
11. В текстовом поле **Адрес отправителя** введите адрес, vRealize Automation которого будут отправлять электронные сообщения.
 Этот адрес электронной почты должен соответствовать указанному имени пользователя и паролю.
12. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.
 Этот параметр доступен, только если включено шифрование.
 - Чтобы принимать самозаверяющие сертификаты, нажмите кнопку **Да**.
 - Чтобы отклонять самозаверяющие сертификаты, нажмите кнопку **Нет**.
13. Щелкните элемент **Проверить подключение**.
14. Нажмите кнопку **Добавить**.

Добавление сервера входящей электронной почты для конкретного арендатора

Администраторы арендатора могут добавить сервер входящей электронной почты, чтобы пользователи могли отвечать на уведомления для завершения таких рабочих элементов, как подтверждения.

У каждого арендатора может быть только один сервер входящей электронной почты. Если системный администратор уже настроил глобальный сервер входящей электронной почты, см раздел [Переопределение сервера входящей почты системы по умолчанию](#).

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора арендатора**.
- Убедитесь, что указанный пользователь есть в хранилище удостоверений и принадлежит к бизнес-группе.

Процедура

1. Выберите **Администрирование > Уведомления > Почтовые серверы**.

2. Щелкните значок **Добавить** (+).
3. Выберите **Электронная почта — Входящая** и нажмите кнопку **ОК**.
4. Настройте следующие параметры сервера входящей электронной почты.

Параметр	Действие
Имя	Введите имя сервера входящей электронной почты.
Описание	Введите описание сервера входящей электронной почты.
Безопасность	Установите флажок Использовать SSL .
Протокол	Выберите протокол сервера.
Имя сервера	Введите имя сервера.
Порт сервера	Введите номер порта сервера.

5. В текстовом окне **Имя папки** введите имя папки для электронных сообщений.
Этот параметр обязателен, только если выбран протокол сервера IMAP.
6. В текстовом поле **Имя пользователя** введите имя пользователя.
7. Введите пароль в текстовом поле **Пароль**.
8. В текстовом поле **Адрес электронной почты** введите адрес, на который смогут отправлять ответ пользователи vRealize Automation.
9. (дополнительно) Выберите элемент **Удалять с сервера**, чтобы удалить с сервера все обработанные электронные сообщения, полученные с помощью службы уведомлений.
10. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.
Этот параметр доступен, только если включено шифрование.
 - Чтобы принимать самозаверяющие сертификаты, нажмите кнопку **Да**.
 - Чтобы отклонять самозаверяющие сертификаты, нажмите кнопку **Нет**.
11. Щелкните элемент **Проверить подключение**.
12. Нажмите кнопку **Добавить**.

Переопределение сервера исходящей почты системы по умолчанию

Если системный администратор настроил сервер исходящей почты системы по умолчанию, администраторы арендатора могут переопределить этот глобальный параметр.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Уведомления > Почтовые серверы**.

2. Выберите сервер исходящей почты.
3. Щелкните элемент **Переопределить глобальные настройки**.
4. В текстовом поле **Имя** введите имя.
5. (дополнительно) В текстовом поле **Описание** введите описание.
6. В текстовом поле **Имя сервера** введите имя сервера.
7. Выберите метод шифрования.
 - Щелкните **Использовать SSL**.
 - Щелкните **Использовать TLS**.
 - Чтобы отправить незашифрованные сообщения, выберите значение **Нет**.
8. В текстовом окне **Порт сервера** введите номер порта сервера.
9. (дополнительно) Если на сервере требуется проверка подлинности, установите флажок **Обязательно**.
 - а) В текстовом поле **Имя пользователя** введите имя пользователя.
 - б) В текстовом поле **Пароль** введите пароль.
10. В текстовом поле **Адрес отправителя** введите адрес, vRealize Automation которого будут отправлять электронные сообщения.
 Этот адрес электронной почты должен соответствовать указанному имени пользователя и паролю.
11. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.
 Этот параметр доступен, только если включено шифрование.
 - Чтобы принимать самозаверяющие сертификаты, нажмите кнопку **Да**.
 - Чтобы отклонять самозаверяющие сертификаты, нажмите кнопку **Нет**.
12. Щелкните элемент **Проверить подключение**.
13. Нажмите кнопку **Добавить**.

Переопределение сервера входящей почты системы по умолчанию

Если системный администратор настроил сервер входящей почты системы по умолчанию, администраторы арендатора могут переопределить этот глобальный параметр.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Уведомления > Почтовые серверы**.
2. Выберите сервер входящей почты в таблице «Почтовые серверы».
3. Щелкните элемент **Переопределить глобальные настройки**.

4. Введите следующие параметры сервера входящей почты.

Параметр	Действие
Имя	Введите имя сервера входящей почты.
Описание	Введите описание сервера входящей электронной почты.
Безопасность	Установите флажок SSL , чтобы использовать SSL для обеспечения безопасности.
Протокол	Выберите протокол сервера.
Имя сервера	Введите имя сервера.
Порт сервера	Введите номер порта сервера.

5. В текстовом окне **Имя папки** введите имя папки для электронных сообщений.

Этот параметр обязателен, только если выбран протокол сервера IMAP.

6. В текстовом поле **Имя пользователя** введите имя пользователя.

7. Введите пароль в текстовом поле **Пароль**.

8. В текстовом поле **Адрес электронной почты** введите адрес, на который смогут отправлять ответ пользователи vRealize Automation.

9. (дополнительно) Выберите элемент **Удалять с сервера**, чтобы удалить с сервера все обработанные электронные сообщения, полученные с помощью службы уведомлений.

10. Выберите, может ли vRealize Automation принимать самозаверяющие сертификаты с почтового сервера.

Этот параметр доступен, только если включено шифрование.

- Чтобы принимать самозаверяющие сертификаты, нажмите кнопку **Да**.
- Чтобы отклонять самозаверяющие сертификаты, нажмите кнопку **Нет**.

11. Щелкните элемент **Проверить подключение**.

12. Нажмите кнопку **Добавить**.

Восстановление системных почтовых серверов по умолчанию

Администраторы арендатора, которые переопределяют системные серверы по умолчанию, могут восстанавливать глобальные параметры.

Необходимые условия

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

Процедура

1. Выберите **Администрирование > Уведомления > Почтовые серверы**.
2. Выберите почтовые серверы, которые необходимо восстановить.
3. Щелкните элемент **Вернуться к глобальным настройкам**.

4. Нажмите кнопку **Да**.

Настройка уведомлений

Пользователи сами указывают, хотят ли они получать уведомления, а администраторы арендаторов решают, какие события инициируют отправку уведомлений.

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора арендатора**.
- Убедитесь, что администратор арендатора или системный администратор настроили сервер исходящей почты. См. [Добавление сервера исходящей электронной почты для конкретного арендатора](#).

Процедура

1. Выберите **Администрирование > Уведомления > Сценарии**.
2. Выберите нужные уведомления.
3. Щелкните элемент **Активировать**.

Результаты

Пользователи, подписавшиеся на уведомления в разделе настроек, теперь получают их.

Настройка даты для уведомления электронной почты об истечении срока действия компьютера

Можно указать дату отправки уведомления по электронной почте до даты окончания срока действия компьютера.

Можно изменить значение параметра, определяющего количество дней до даты окончания срока действия компьютера, с учетом которой из vRealize Automation отправляется сообщение электронной почты о завершении срока действия. Сообщением электронной почты пользователи уведомляются о дате завершения срока действия компьютера. По умолчанию задана дата за 7 дней до завершения срока действия компьютера.

Процедура

1. Войдите в сервер vRealize Automation, используя учетные данные, обладающие правами администратора.
2. Перейдите к файлу `/etc/vcac/setenv-user` и откройте его.
3. Добавьте в файл следующую строку, чтобы задать количество дней до даты завершения срока действия компьютера. Значение 3 в данном примере означает, что уведомление будет отправлено за три дня до даты завершения срока действия компьютера.

```
VCAC_OPTS="$VCAC_OPTS -Dlease.enforcement.prearchive.notification.days=3"
```

4. Перезапустите службы vCAC на виртуальном устройстве, выполнив следующую команду:

```
service vcac-server restart
```

Следующие шаги

Если используется среда подсистемы балансировки нагрузки высокой доступности, повторите эту процедуру для всех виртуальных устройств в данной среде высокой доступности.

Настройка шаблонов для автоматической отправки электронной почты в инфраструктуре как услуге

Можно настроить отправку уведомлений по электронной почте владельцам компьютеров со сведениями о различных событиях vRealize Automation, которые относятся к их компьютерам.

К числу событий, которые инициируют отправку уведомлений, относятся истечение или скорое истечение срока действия архивации или аренды виртуальных машин.

Сведения о настройке и включении или выключении уведомлений vRealize Automation, отправляемых по электронной почте, см. в следующей статье блога и статьях базы знаний.

- [Настройка параметров электронной почты в vRealize Automation](#)
- [Настройка шаблонов сообщений электронной почты в vRealize Automation \(2088805\)](#)
- [Примеры настройки шаблонов сообщений электронной почты в vRealize Automation \(2102019\)](#)

Подписка на уведомления

Если администраторы настроили уведомления, вы будете автоматически подписаны. Уведомления о событиях могут включать в себя сообщения об успешном выполнении запроса каталога или о необходимости в подтверждении.

Если необходимо подписаться вручную, можно включить уведомления.

Необходимые условия

Войдите в vRealize Automation.

Процедура

1. Щелкните элемент **Параметры**.
2. В таблице «Уведомления» установите флажок **Включено** для почтового протокола.
3. Нажмите кнопку **Применить**.
4. Нажмите кнопку **Заккрыть**.

Создание настраиваемого RDP-файла для поддержки подключений RDP для подготовленных компьютеров

Системные администраторы создают настраиваемые файлы протокола удаленного рабочего стола. Эти файлы архитекторы инфраструктуры как услуги используют в схемах элементов для настройки параметров RDP. Можно создать RDP-файл и предоставить разработчикам архитектуры полный путь к нему, чтобы

его можно было включить в схемы элементов. Затем администратор каталога предоставляет пользователям право на использование действий с RDP.

Примечание Если в Internet Explorer включена конфигурация усиленной безопасности, с его помощью нельзя скачать RDP-файлы.

Необходимые условия

Войдите в службу диспетчера инфраструктуры как услуги в качестве администратора.

Процедура

1. Задайте для текущего каталога *<Каталог_установки_vRA>\Rdp*.
2. Скопируйте файл *Default.rdp* и переименуйте его на *Console.rdp* в том же каталоге.
3. Откройте файл *Console.rdp* в редакторе.
4. Добавьте в файл параметры RDP.
Например, **connect to console:i:1**.
5. При работе в распределенной среде войдите в качестве пользователя с правами администратора на узел инфраструктуры как услуги, где установлен компонент «Веб-сайт диспетчера модели».
6. Скопируйте файл *Console.rdp* в каталог *Каталог_установки_vRA\Server\Website\Rdp*.
7. Добавьте настраиваемое свойство *VirtualMachine.Rdp.File* в схему элементов.

Архитекторы инфраструктуры как услуги могут добавлять настраиваемые свойства RDP в схемы элементов компьютеров под управлением Windows, а затем администраторы каталога могут предоставлять пользователям право на использование действия «Подключиться с помощью RDP». См. раздел [Добавление поддержки подключения к удаленному рабочему столу \(RDP\) к схемам элементов компьютера Windows](#).

Сценарий: добавление данных о расположении центра обработки данных при развертываниях в нескольких регионах

Системному администратору нужно определить расположения центров обработки данных в Бостоне и Лондоне, чтобы администраторы структуры смогли применить их к вычислительным ресурсам в каждом центре обработки данных. При создании схем элементов разработчики архитектуры схем элементов могут включить параметр выбора расположения, чтобы при заполнении форм запросов на элементы каталога пользователи могли выбрать место подготовки компьютеров (Бостон или Лондон).

При наличии центра обработки данных в Лондоне и Бостоне нельзя, чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Лондона и наоборот. Чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Бостона, а пользователи Лондона — в инфраструктуре Лондона, необходимо разрешить пользователям выбирать соответствующее расположение для подготовки при запросе компьютеров.



Нельзя отфильтровать расположения центров обработки данных в XML-файле по арендатору или бизнес-группе. В среде с несколькими арендаторами для фильтрации по арендатору или бизнес-группе можно использовать определения свойств. Сведения об использовании определений свойств см. в записи блога [How to use dynamic property definitions](#) (Использование динамических определений свойств).

Процедура

1. Войдите на узел веб-сервера инфраструктуры как услуги, используя учетные данные администратора. Это компьютер, на котором установлен компонент «Веб-сайт» инфраструктуры как услуги.
2. Измените файл `WebSite\XmlData\DataCenterLocations.xml` в каталоге установки сервера Windows (обычно это `%SystemDrive%\Program Files x86\VMware\vCAC\Server`).
3. Измените раздел `CustomDataType` файла, чтобы создать записи `Data Name` для каждого расположения.

```
<CustomDataType>
  <Data Name="London" Description="London datacenter" />
  <Data Name="Boston" Description="Boston datacenter" />
</CustomDataType>
```

4. Сохраните файл и закройте его.
5. Перезапустите службу диспетчера.
6. Если есть несколько узлов веб-сервера инфраструктуры как услуги, повторите эту процедуру для каждого избыточного экземпляра.

Результаты

Администратор структуры может применить соответствующие расположения к вычислительным ресурсам, расположенным в каждом центре обработки данных. См. раздел [Сценарий: применение размещения к вычислительному ресурсу при развертываниях в нескольких регионах](#).

Следующие шаги

Можно добавить свойство `Vrm.DataCenter.Location` к схеме элементов или включить в схеме элементов параметр **Отобразить расположение по запросу**, чтобы требовать от пользователя указывать расположение центра обработки данных при запросе подготовки компьютера.

Настройка vRealize Orchestrator

vRealize Orchestrator — это механизм автоматизации и управления, который позволяет расширить vRealize Automation для поддержки Все как услуга и других функций. Можно настроить и использовать сервер vRealize Orchestrator, предварительно настроенный на устройстве vRealize Automation, или можно развернуть vRealize Orchestrator как внешний экземпляр сервера и настроить для него связь с vRealize Automation.

vRealize Orchestrator помогает администраторам и разработчикам архитектуры разрабатывать сложные задачи автоматизации с помощью конструктора рабочих процессов, а затем получать доступ и выполнять рабочие процессы из vRealize Automation.

vRealize Orchestrator может получать доступ и управлять внешними технологическими комплексами, а также приложениями с помощью подключаемых модулей vRealize Orchestrator.

После настройки vRealize Automation для использования vRealize Orchestrator можно публиковать рабочие процессы vRealize Orchestrator в каталоге служб vRealize Orchestrator в рамках управления схемой элементов Все как услуга.

Чтобы запустить рабочие процессы для расширенного управления компьютерами Инфраструктура как услуга, необходимо настроить vRealize Orchestrator как конечную точку.

Привилегии по настройке

Системные администраторы и администраторы арендатора могут настроить решение vRealize Automation, чтобы оно использовало внешний или встроенный сервер vRealize Orchestrator.

Кроме того, системные администраторы могут определять папки рабочих процессов, которые доступны каждому арендатору.

Администраторы арендатора могут настраивать подключаемые модули vRealize Orchestrator в качестве конечных точек.

Роль	Привилегии по настройке, связанные с vRealize Orchestrator
Системные администраторы	<ul style="list-style-type: none"> ■ Настраивают сервер vRealize Orchestrator для всех арендаторов. ■ Определяют папки рабочих процессов vRealize Orchestrator по умолчанию для каждого арендатора.
Администраторы арендатора	<ul style="list-style-type: none"> ■ Настраивают сервер vRealize Orchestrator для своего собственного арендатора. ■ Добавляют подключаемые модули vRealize Orchestrator в качестве конечных точек.

Настройка встроенного сервера vRealize Orchestrator

Устройство vRealize Automation включает в себя предварительно сконфигурированный экземпляр vRealize Orchestrator.

Необходимые условия

Развертывание устройства vRealize Automation. Подробные сведения см. в разделе *Развертывание устройства vRealize Automation* в *Установка vRealize Automation*.

Процедура

1. Войдите в консоль vRealize Automation в качестве **системного администратора** или **администратора арендатора**.
2. Выберите **Администрирование > Конфигурация VRO > Конфигурация сервера**.
3. Выберите **Использовать сервер Orchestrator по умолчанию**.

Результаты

Подключения к встроенному серверу vRealize Orchestrator теперь настроены. Папка рабочих процессов **VCAC** и связанные действия служебной программы импортируются автоматически. Папка рабочих процессов **VCAC > ASD** содержит рабочие процессы для настройки конечных точек и создания сопоставлений ресурсов.

Выполнение входа в центр управления vRealize Orchestrator

Чтобы изменить конфигурацию экземпляра vRealize Orchestrator по умолчанию, встроенного в vRealize Automation, необходимо войти в центр управления vRealize Orchestrator.

Служба конфигурации встроенного экземпляра vRealize Orchestrator запускается автоматически.

Примечание Чтобы убедиться, что конфигурация запускается автоматически, выполните команду `chkconfig vco-configurator` в консоли командной строки vRealize Orchestrator Appliance. Если служба сообщает о состоянии off, выполните команду `chkconfig vco-configurator on` и перезагрузите устройство.

Процедура

1. Подключитесь к URL-адресу vRealize Automation в веб-браузере.
2. Щелкните **Центр управления vRealize Orchestrator**.

Произойдет перенаправление на страницу `https://vra-va-hostname.domain.name_or_load_balancer_address:8283/vco-controlcenter`.

3. Введите учетные данные пользователя root среды vRealize Automation.

Выполнение входа в клиент vRealize Orchestrator

Для выполнения общих задач администрирования или изменения и создания рабочих процессов в экземпляре vRealize Orchestrator по умолчанию следует войти в клиент vRealize Orchestrator.

Клиентский интерфейс vRealize Orchestrator предназначен для разработчиков с правами администратора, которые хотят разрабатывать рабочие процессы, действия и другие пользовательские элементы.

Процедура

1. Подключитесь к URL-адресу vRealize Automation в веб-браузере.

2. Для входа в клиент vRealize Orchestrator на основе HTML5.

- а) Щелкните **Клиент vRealize Orchestrator**.
- б) Введите имя пользователя и пароль для клиента vRealize Orchestrator и нажмите **Вход**.

В качестве учетных данных используются имя пользователя и пароль администратора арендатора по умолчанию.

3. Для входа в устаревший клиент vRealize Orchestrator.

- а) Щелкните **Устаревший клиент vRealize Orchestrator**.
Будет загружен файл с клиентом.
- б) Нажмите «Скачать» и следуйте подсказкам.
- в) В окне **Предупреждение системы безопасности** выберите действие для предупреждения о сертификате.

Клиент vRealize Orchestrator обменивается данными с сервером vRealize Orchestrator, используя сертификат SSL. Доверенный центр сертификации не подписывает сертификат во время установки. Предупреждение системы безопасности появляется при каждом подключении к серверу vRealize Orchestrator.

Параметр	Описание
Продолжить	Продолжить использовать текущий сертификат SSL. Предупреждение появится снова при восстановлении подключения к тому же серверу vRealize Orchestrator или при попытке синхронизировать рабочий процесс с удаленным сервером vRealize Orchestrator.
Отмена	Закрыть окно и остановить процесс входа.

- г) Щелкните **Запустить**.
- д) На странице входа в vRealize Orchestrator в текстовом поле **Имя узла** введите IP-адрес или доменное имя устройства vRealize Automation и номер порта по умолчанию — **443**.
Например, введите `vrealize_automation_appliance_ip:443`.
- е) Введите имя пользователя и пароль для клиента vRealize Orchestrator и нажмите кнопку **Вход**.
В качестве учетных данных используются имя пользователя и пароль администратора арендатора по умолчанию.

Следующие шаги

Используйте клиент vRealize Orchestrator для разработки и запуска рабочих процессов, а также для экспорта содержимого в другие среды vRealize Orchestrator с помощью пакетов. См. разделы *Использование клиента VMware vRealize Orchestrator* и *Разработка с использованием VMware vRealize Orchestrator*.

Настройка внешнего сервера vRealize Orchestrator

vRealize Automation можно настроить для использования внешнего сервера vRealize Orchestrator.

Системные администраторы могут настраивать сервер vRealize Orchestrator по умолчанию глобально для всех арендаторов. Администраторы арендатора могут настраивать сервер vRealize Orchestrator только для своих арендаторов.

Для подключения к экземплярам внешнего сервера vRealize Orchestrator учетная запись пользователя должна иметь в vRealize Orchestrator разрешения на просмотр и выполнение.

- Проверка подлинности для единого входа. Информация о пользователе передается в vRealize Orchestrator с помощью запроса Все как услуга, и пользователю предоставляются разрешения на просмотр и выполнение для запрашиваемого рабочего процесса.
- Базовая проверка подлинности. Предоставленная учетная запись пользователя должна быть записью участника группы vRealize Orchestrator с разрешениями на просмотр и выполнение или участником группы vcoadmins.

Необходимые условия

- Установите и настройте внешнее устройство vRealize Orchestrator. См. раздел *Установка и настройка vRealize Orchestrator* в [документации по продукту vRealize Orchestrator](#).
- Войдите в консоль vRealize Automation в качестве **системного администратора** или **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конфигурация сервера**.
2. Щелкните **Использовать внешний сервер Orchestrator**.
3. Введите имя и, при необходимости, описание.
4. В текстовом поле **Узел** введите IP-адрес или имя DNS компьютера, на котором выполняется сервер vRealize Orchestrator.

Примечание Если внешний сервер vRealize Orchestrator настроен для работы в режиме кластера, введите IP-адрес или имя узла для виртуального сервера с подсистемой балансировки нагрузки, который распределяет запросы клиентов по всем серверам vRealize Orchestrator в кластере.

5. В текстовом поле **Порт** введите номер порта для взаимодействия с внешним сервером vRealize Orchestrator.

По умолчанию для vRealize Orchestrator используется порт 8281.

6. Выберите тип проверки подлинности.

Параметр	Описание
Single Sign-On	Обеспечивает подключение к серверу vRealize Orchestrator с помощью vCenter Single Sign-On. Этот вариант можно применять только в том случае, если вы настроили vRealize Orchestrator и vRealize Automation для использования общего экземпляра службы vCenter Single Sign-On.
Обычная	Обеспечивает подключение к серверу vRealize Orchestrator с помощью имени пользователя и пароля, которые следует ввести в текстовых полях Имя пользователя и Пароль . Вводимая учетная запись должна быть записью участника группы vcoadmins в vRealize Orchestrator или участника группы с разрешениями на просмотр и выполнение.

7. Щелкните элемент **Проверить подключение**.

8. Нажмите кнопку **ОК**.

9. Импортируйте пакет `xaas.package`.

- Войдите в устройство vRealize Automation как пользователь **root**.
- В папке `/usr/lib/vcac/content/o11n/` выберите пакет `xaas.package`.
- Импортируйте пакет `xaas.package` во внешний клиент.

Результаты

Вы настроили подключение к внешнему серверу vRealize Orchestrator и импортировали папку рабочих процессов **VCAC** и связанные действия служебной программы. Папка рабочих процессов **VCAC > ASD** содержит рабочие процессы для настройки конечных точек и создания сопоставлений ресурсов.

Следующие шаги

[Выполнение входа в клиент vRealize Orchestrator.](#)

Настройка ресурсов

Для таких ресурсов, как конечные точки, резервирования и профили сети можно настроить поддержку определения схемы элементов vRealize Automation и подготовки компьютеров.

Контрольный список для настройки ресурсов инфраструктуры как услуги

Администраторы инфраструктуры как услуги и администраторы структуры настраивают ресурсы инфраструктуры как услуги, чтобы интегрировать существующую инфраструктуру с vRealize Automation и выделить ресурсы инфраструктуры для бизнес-групп vRealize Automation.

Чтобы получить общее представление о последовательности шагов, которые необходимо выполнить для настройки ресурсов инфраструктуры как услуги, воспользуйтесь контрольным списком настройки ресурсов инфраструктуры как услуги.

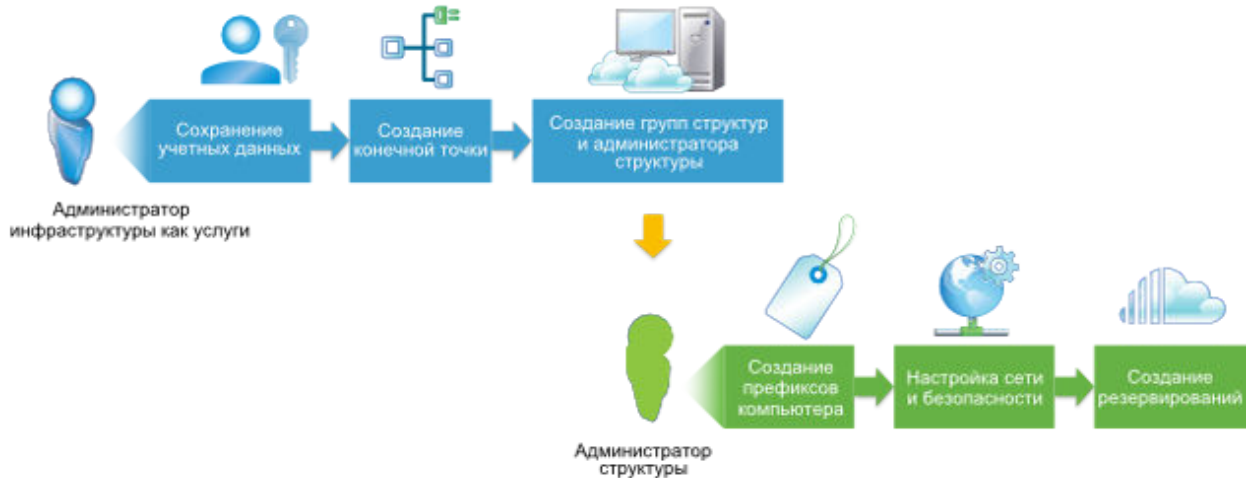


Таблица 2-11. Контрольный список для настройки ресурсов инфраструктуры как услуги

Задача	Роль vRealize Automation	Сведения
<input type="checkbox"/> Создание конечных точек инфраструктуры, позволяющих управлять ресурсами с помощью vRealize Automation.	администратор инфраструктуры как услуги	Выбор сценария конечной точки.
<input type="checkbox"/> Создание группы структур для объединения ресурсов инфраструктуры в группы и назначения одного или нескольких администраторов для управления этими ресурсами в качестве администраторов структуры vRealize Automation.	администратор инфраструктуры как услуги	Создание групп структур.
<input type="checkbox"/> Настройка префиксов компьютеров, используемых для создания имен компьютеров, подготовленных с помощью vRealize Automation.	Администратор структуры	Настройка префиксов компьютеров.
<input type="checkbox"/> (Необязательно.) Создание профилей сети для настройки параметров сети подготовленных компьютеров.	Администратор структуры	Создание профиля сети в vRealize Automation.
<input type="checkbox"/> Выделение ресурсов инфраструктуры для бизнес-групп (создание резервирований и, при необходимости, профилей резервирования и резервирования хранилищ).	<ul style="list-style-type: none"> ■ Администратор инфраструктуры как услуги, если он также настроен в качестве администратора структуры ■ Администратор структуры 	Настройка резервирований и их политик.

Настройка конечных точек

Для обмена данными между vRealize Automation и инфраструктурой необходимо создать и настроить конечные точки.

Определения конечных точек подразделяются на категории по типу:

- **Облака**

Категория облака содержит типы конечных точек vCloud Air, vCloud Director, Amazon EC2 и OpenStack.

- **управление IP-адресами**

Эта категория доступна, только если в рабочем процессе vRealize Orchestrator был зарегистрирован тип сторонней конечной точки управления IP-адресами (например, Infoblox).

- **Управление**

Эта категория содержит только тип конечной точки vRealize Operations Manager.

- **Сеть и безопасность**

Эта категория содержит прокси-сервер и типы конечных точек NSX.

Конечная точка прокси-сервера может быть связана с конечной точкой Amazon, vCloud Air или vCloud Director.

Конечная точка NSX может быть связана с конечной точкой vSphere.

- **Оркестрация**

Эта категория содержит только тип конечной точки vRealize Orchestrator.

- **Хранилище**

Эта категория содержит конечную точку NetApp ONTAP.

- **Виртуальные**

Эта категория содержит типы конечных точек vSphere, Hyper-V (SCVMM) и KVM (RHEV).

В vRealize Orchestrator можно настроить дополнительные типы конечных точек и использовать их с поддерживаемыми типами конечных точек в vRealize Automation. Выполнять импорт и экспорт конечных точек также можно программным способом.

Сведения о работе с конечными точками после обновления или переноса см. в разделе [Факторы, которые необходимо учитывать при работе с обновленными или перенесенными конечными точками](#).

Выбор сценария конечной точки

Выберите сценарий конечной точки на основании типа конечной точки назначения.

Сведения о доступных параметрах конечной точки см. в разделе [Справочник по параметрам конечных точек](#).

Таблица 2-12. Выбор сценария конечной точки

Конечная точка	Дополнительные сведения
vSphere	См. раздел Создание конечной точки vSphere в vRealize Automation и ее связывание с NSX.
NSX	См. раздел Создание конечной точки NSX for vSphere и настройка связи с конечной точкой vSphere в vRealize Automation или Создание конечной точки NSX-T и настройка связи с конечной точкой vSphere в vRealize Automation .
vCloud Air (по подписке или по требованию)	См. раздел Создание конечной точки vCloud Air .
vCloud Director	См. раздел Создание конечной точки vCloud Director .
vRealize Orchestrator	См. раздел Создание конечной точки vRealize Orchestrator .
vRealize Operations	См. раздел Создание конечной точки vRealize Operations Manager .
Сторонние поставщики служб управления IP-адресами	См. раздел Создание конечной точки стороннего поставщика управления IP-адресами .
Microsoft Azure	См. раздел Создание конечной точки Microsoft Azure .
Puppet	См. раздел Создание конечной точки Puppet .
Amazon	См. Создание конечной точки Amazon и Добавление типа экземпляра Amazon .
OpenStack	См. раздел Создание конечной точки OpenStack .
Прокси-сервер	Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы
Hyper-V (SCVMM)	См. раздел Создание конечной точки Hyper-V (SCVMM) .
KVM (RHEV)	См. раздел Справочник по параметрам конечных точек .
NetApp ONTAP	См. Компактное хранилище для виртуальной подготовки и Справочник по параметрам конечных точек .
Hyper-V (автономное решение), XenServer или образец пула Xen	См. раздел Создание конечной точки Hyper-V, XenServer или пула Xen .
Импорт конечных точек	См. раздел Программный импорт и экспорт конечных точек .

Справочник по параметрам конечных точек

С помощью параметров конечных точек задаются расположение и учетные данные для сбора данных и развертывания каталога служб.

Вкладка «Общие»

Для большинства конечных точек vRealize Automation используются следующие параметры. Отдельно отмечены специфические параметры определенных типов конечных точек.

Таблица 2-13. Настройки вкладки **Общие**

Параметр	Описание
Имя	Введите имя конечной точки.
Описание	Введите описание конечной точки.
Адрес	<p>Введите адрес конечной точки, используя специальный формат адреса.</p> <ul style="list-style-type: none"> ■ Для конечной точки KVM (RHEV) или NetApp ONTAP адрес должен быть задан в одном из следующих форматов: <ul style="list-style-type: none"> ■ <code>https://полное_доменное_имя</code> ■ <code>https://IP-адрес</code> <p>Например: <code>https://mycompany-kvmrhev1.mycompany.local</code> или <code>netapp-1.mycompany.local</code>.</p> ■ Для конечной точки OpenStack адрес должен быть задан в формате <code>https:// FQDN/powervc/openstack/ service</code>. Например: <code>https://openstack.mycompany.com/powervc/openstack/admin</code>. ■ Для конечной точки OpenStack адрес должен быть задан в одном из следующих форматов: <ul style="list-style-type: none"> ■ <code>https://полное_доменное_имя:500</code> ■ <code>https://IP-адрес:500</code> ■ Для конечной точки vSphere адрес должен быть задан в формате <code>https://host/sdk</code>. ■ Для конечной точки NSX адрес должен быть задан в формате <code>https://host</code>. ■ Для конечной точки vRealize Orchestrator адрес должен использовать протокол <code>https</code> и содержать полное доменное имя или IP-адрес сервера vRealize Orchestrator, а также номер порта vRealize Orchestrator. Например, <code>https://vrealize-automation-appliance-hostname:443/vco</code>. ■ Для конечной точки vRealize Operations адрес должен быть задан в формате <code>https://host/suite-api</code>.
Интегрированные учетные данные	<p>Если используются интегрированные учетные данные vSphere, вводить имя пользователя и пароль не нужно.</p> <p>Этот параметр применим только к конечным точкам vSphere.</p>
Имя пользователя	Введите имя пользователя с привилегиями администратора, которое вы сохранили для конечной точки, в необходимом для конечной точки формате, как показано в пользовательском интерфейсе.
Пароль	Введите пароль администратора, сохраненный для этой конечной точки.
Проект OpenStack	<p>Введите имя арендатора OpenStack.</p> <p>Этот параметр применим только к конечным точкам OpenStack.</p>
Организация	<p>Если вы являетесь администратором организации, здесь можно ввести название организации vCloud Director.</p> <p>Этот параметр применим только для решения vCloud Director.</p>
Идентификатор ключа доступа	<p>Введите идентификатор ключа Amazon AWS.</p> <p>Этот параметр применим только к конечным точкам Amazon.</p>
Секретный ключ доступа	<p>Введите секретный ключ доступа Amazon AWS.</p> <p>Этот параметр применим только к конечным точкам Amazon.</p>

Таблица 2-13. Настройки вкладки **Общие** (продолжение)

Параметр	Описание
Порт	Введите номер порта для подключения в адресе конечной точки прокси-сервера. Этот параметр применим только к конечным точкам прокси-серверов.
Приоритет	Введите значение приоритета. Это должно быть целое число, большее или равное 1. Чем меньше данное значение, тем выше приоритет. Значение приоритета связано со встроенным настраиваемым свойством VMware.VCenterOrchestrator.Priority . Этот параметр применим только к конечным точкам vRealize Orchestrator.

Вкладка «Свойства»

Вкладка свойств используется всеми типами конечных точек для сохранения настраиваемых свойств или групп и параметров свойств. Примеры настраиваемых свойств для конкретных типов конечных точек см. в разделе *Справочник по настраиваемым свойствам*.

Вкладка «Связь»

В зависимости от связываемой конечной точки можно создать связь с конечной точкой NSX или конечной точкой прокси-сервера. Можно связать конечную точку vSphere с конечной точкой NSX, чтобы назначить параметры NSX конечной точке vSphere. Можно также связать конечную точку vCloud Air, vCloud Director или Amazon с конечной точкой прокси-сервера, чтобы назначить параметры прокси-сервера соответствующей конечной точке vCloud Air, vCloud Director или Amazon.

Проверить подключение

Функцию проверки подключения можно использовать для проверки учетных данных, адреса конечной точки узла, а также сертификата для конечной точки vSphere, NSX или vRealize Operations Manager. См. раздел [Факторы, которые следует учитывать при проверке подключения](#).

Создание конечной точки vSphere в vRealize Automation и ее связывание с NSX

В vRealize Automation можно создать конечные точки vSphere, которые взаимодействуют с vCenter для обнаружения вычислительных ресурсов, сбора данных и подготовки компьютеров. Кроме того, можно связать параметры NSX с конечной точкой vSphere, связав их с конечной точкой NSX for vSphere, одной или несколькими конечными точками NSX-T или обоими типами конечных точек NSX.

Связывание конечной точки vSphere с конечными точками NSX for vSphere и NSX-T позволяет настроить NSX for vSphere и NSX-T для разных кластеров в одном vCenter:

- Администратор инфраструктуры как услуги может связать конечную точку vSphere с конечной точкой NSX for vSphere и конечной точкой NSX-T.
- Администратор структуры может создать резервирование NSX for vSphere или NSX-T в зависимости от вычислительного ресурса.
- Разработчик схемы элементов может создавать схемы элементов, которые относятся либо к NSX for vSphere, либо к NSX-T. В одной и той же среде vCenter можно развертывать оба типа схем элементов.

Можно создать связь между конечными точками vSphere и NSX. Связи могут быть следующими:

- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere.

- Одна конечная точка vSphere связана с несколькими конечными точками NSX-T.
- Одна конечная точка NSX-T связана с несколькими конечными точками vSphere.
- Одна конечная точка NSX for vSphere связана с одной конечной точкой vSphere.
- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere и с одной конечной точкой NSX-T.

Если конечная точка vSphere связана как с конечной точкой NSX for vSphere, так и с конечной точкой NSX-T, то кластером управляет NSX for vSphere или NSX-T. Диспетчер NSX определяется vRealize Automation, когда с конечных точек собираются данные и устанавливается взаимосвязь.

Чтобы узнать тип платформы NSX, управляющей определенным кластером, нужно посмотреть столбец **Тип NSX** на странице **Вычислительные ресурсы**.

Дополнительные сведения о создании конечных точек NSX, связанных с конечной точкой vSphere, см. в разделе [Создание конечной точки NSX for vSphere и настройка связи с конечной точкой vSphere в vRealize Automation](#) или [Создание конечной точки NSX-T и настройка связи с конечной точкой vSphere в vRealize Automation](#).

Информацию о проверке подключения конечной точки и доверии для сертификатов см. в разделе [Факторы, которые следует учитывать при проверке подключения](#).

После обновления или переноса конечной точки vSphere, использующей диспетчер NSX, создается новая конечная точка NSX, в которой содержится связь между исходной конечной точкой vSphere и новой конечной точкой NSX.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Чтобы управлять конечной точкой vSphere, необходимо установить прокси-агент vSphere. Имя агента должно совпадать с именем конечной точки. Информацию об установке агента см. в разделе *Установка vRealize Automation*.
- Если планируется использовать конечную точку vSphere для развертывания виртуальных машин из шаблонов OVF, убедитесь, что в vCenter Server учетные данные содержат привилегию VApp.Import для vSphere, связанную с конечной точкой.

Привилегия VApp.Import позволяет выполнить развертывание компьютера vSphere с помощью параметров, импортированных из файла OVF. Сведения о привилегии vSphere можно найти в [документации по комплекту vSphere SDK](#).

Если файл OVF размещен на веб-сайте, см. раздел [Создание конечной точки прокси-сервера для веб-сайта узла OVF](#).

- Чтобы задать дополнительные параметры сети и безопасности NSX для конечной точки vSphere, создайте конечную точку NSX for vSphere или NSX-T. Создав или отредактировав конечную точку vSphere, можно связать ее с конечной точкой NSX.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.

2. Выберите Создать > Виртуальный > vSphere.

3. В текстовом поле Имя введите имя.

Имя должно соответствовать имени конечной точки, указанной для прокси-агента vSphere во время установки. Если эти имена не совпадают, сбор данных завершится с ошибкой.

4. (дополнительно) В текстовом поле Описание введите описание.

5. В текстовом поле Адрес укажите URL-адрес экземпляра vCenter Server.

Тип URL-адреса должен быть такой: **https://*имя_узла*/sdk** или **https://*IP-адрес*/sdk**.

Например, **https://vsphereA/sdk**.

6. Введите имя пользователя с правами администратора vSphere и пароль или используйте интегрированные учетные данные vSphere.

Укажите учетные данные, для которых предоставлено разрешение на изменение пользовательских атрибутов.

Формат имени пользователя: *domain\username*.

Чтобы использовать учетную запись службы прокси-агента vSphere для подключения к vCenter Server, выберите **Использовать интегрированные учетные данные**.

Если используются интегрированные учетные данные vSphere, вводить имя пользователя и пароль не нужно.

7. (дополнительно) Выберите элемент Свойства и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.

8. (дополнительно) Чтобы настроить параметры сети и безопасности NSX для конечной точки, выберите элемент Связи и создайте связь с существующей конечной точкой NSX for vSphere или конечной точкой NSX-T.

Для создания связи необходима хотя бы одна конечная точка NSX.

9. (дополнительно) Выберите элемент Проверить подключение, чтобы проверить учетные данные, адрес конечной точки узла и доверие к сертификату. Одновременно проверяется рабочее состояние службы диспетчера и агента, а также возможность получения данных из конечной точки. При нажатии кнопки ОК проверяются те же условия.

Команда **Проверить подключение** возвращает следующие возможные результаты проверки.

■ **Ошибка сертификата**

Если сертификат не найден, признан ненадежным или срок его действия истек, отобразится запрос на принятие отпечатка сертификата. Если отпечаток не будет принят, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

■ **Ошибка агента**

Связанный агент vSphere не найден. Для успешной проверки требуется запущенный агент.

■ **Ошибка узла**

Указанный адрес конечной точки недоступен, или не запущена связанная служба диспетчера. Для успешной проверки требуется запущенная служба диспетчера.

- Ошибка в учетных данных

Обнаружено недопустимое сочетание имени пользователя и пароля для конечной точки с указанным адресом.

- Timeout

Проверка не завершилась в течение отведенного времени (2 минуты).

Если действие **Проверка подключения** не выполнено, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

Если возникла проблема с доверенным сертификатом (например, истек срок его действия), отобразится запрос на принятие отпечатка сертификата.

10. Чтобы сохранить конечную точку, нажмите кнопку **ОК**.

При нажатии кнопки **ОК** проверяются те же условия, что и при действии **Проверка подключения**.

Если выполняется любое из указанных выше условий, выводится сообщение. Если сохранение все же будет выполнено, на экране для пользователя останется сообщение об ошибке.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Примечание Не изменяйте имена центров обработки данных vSphere после первоначального сбора данных. Это может привести к сбою подготовки.

Дополнительные сведения см. в разделе [Просмотр вычислительных ресурсов и запуск сбора данных](#).

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки NSX for vSphere и настройка связи с конечной точкой vSphere в vRealize Automation

В vRealize Automation можно создать конечную точку NSX for vSphere и связать ее с существующей конечной точкой vSphere.

Конечную точку NSX for vSphere можно связать с конечной точкой vSphere.

Можно создать связь между конечными точками vSphere и NSX. Связи могут быть следующими:

- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere.
- Одна конечная точка vSphere связана с несколькими конечными точками NSX-T.
- Одна конечная точка NSX-T связана с несколькими конечными точками vSphere.
- Одна конечная точка NSX for vSphere связана с одной конечной точкой vSphere.

- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere и с одной конечной точкой NSX-T.

Если конечная точка vSphere связана как с конечной точкой NSX for vSphere, так и с конечной точкой NSX-T, то кластером управляет NSX for vSphere или NSX-T. Диспетчер NSX определяется vRealize Automation, когда с конечных точек собираются данные и устанавливается взаимосвязь.

Чтобы узнать тип платформы NSX, управляющей определенным кластером, нужно посмотреть столбец **Тип NSX** на странице **Вычислительные ресурсы**.

Информацию о проверке подключения конечной точки и доверии для сертификатов см. в разделе [Факторы, которые следует учитывать при проверке подключения](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Следует установить прокси-агент vSphere для управления конечной точкой vSphere, также следует использовать одинаковое имя для конечной точки и агента. Информацию об установке агента см. в разделе *Установка vRealize Automation*.
- Настройте параметры сети NSX for vSphere. См. раздел [Настройка параметров компонентов сети и безопасности в vRealize Automation](#).
- [Создание конечной точки vSphere в vRealize Automation и ее связывание с NSX](#).

В процессе подготовки к использованию возможностей сети, безопасности и балансировки нагрузки NSX в vRealize Automation при использовании учетных данных диспетчера NSX необходимо использовать учетную запись администратора диспетчера NSX.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Сеть и безопасность > NSX**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. В текстовом поле **Адрес** укажите URL-адрес экземпляра NSX for vSphere.
Тип URL-адреса должен быть таким: **https://имя_узла** или **https://IP-адрес**.
Например, **https://abx.nsx-manager.local/**.
6. Введите имя пользователя с правами администратора и пароль NSX, сохраненные для конечной точки NSX for vSphere.
7. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
8. Чтобы связать параметры сети и безопасности NSX for vSphere с существующей конечной точкой vSphere, нажмите кнопку **Связи** и выберите существующую конечную точку vSphere.

Перед созданием связи необходимо создать конечную точку vSphere.

Конечную точку vSphere можно связать только с одним типом платформы сети и безопасности — NSX for vSphere или NSX-T.

Конечную точку NSX for vSphere можно связать только с одной конечной точкой vSphere. Следствием этого ограничения является невозможность подготовить универсальную сеть по требованию и подключить ее к компьютерам vSphere, подготовленным на разных экземплярах vCenter.

По окончании создания связи в столбце «Описание» (Description) на странице указывается тип связи для NSX for vSphere.

9. (дополнительно) Выберите элемент **Проверить подключение**, чтобы проверить учетные данные, адрес конечной точки узла и доверие к сертификату. Одновременно проверяется рабочее состояние службы диспетчера и агента, а также возможность получения данных из конечной точки. При нажатии кнопки **ОК** проверяются те же условия.

Команда **Проверить подключение** возвращает следующие возможные результаты проверки.

- Ошибка сертификата

Если сертификат не найден, признан ненадежным или срок его действия истек, отобразится запрос на принятие отпечатка сертификата. Если отпечаток не будет принят, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

- Ошибка агента

Связанный агент vSphere не найден. Для успешной проверки требуется запущенный агент.

- Ошибка узла

Указанный адрес конечной точки недоступен, или не запущена связанная служба диспетчера. Для успешной проверки требуется запущенная служба диспетчера.

- Ошибка в учетных данных

Обнаружено недопустимое сочетание имени пользователя и пароля для конечной точки с указанным адресом.

- Timeout

Проверка не завершилась в течение отведенного времени (2 минуты).

Если действие **Проверка подключения** не выполнено, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

Если возникла проблема с доверенным сертификатом (например, истек срок его действия), отобразится запрос на принятие отпечатка сертификата.

10. Чтобы сохранить конечную точку, нажмите кнопку **ОК**.

При нажатии кнопки **ОК** проверяются те же условия, что и при действии **Проверка подключения**. Если выполняется любое из указанных выше условий, выводится сообщение. Если сохранение все же будет выполнено, на экране для пользователя останется сообщение об ошибке.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Дополнительные сведения о запуске сбора данных для существующих конечных точек после первоначального сбора данных см. в разделе [Просмотр вычислительных ресурсов и запуск сбора данных](#).

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки NSX-T и настройка связи с конечной точкой vSphere в vRealize Automation

В vRealize Automation можно создать конечную точку NSX-T и связать ее с существующей конечной точкой vSphere.

В vRealize Automation для подключения к конечной точке NSX-T используется базовая проверка подлинности.

Чтобы обеспечить отказоустойчивость и высокую доступность в развертываниях, каждая конечная точка центра обработки данных NSX-T представляет собой кластер из трех диспетчеров NSX.

- vRealize Automation может указывать на один из диспетчеров NSX. В этом случае один диспетчер NSX получает вызовы API-интерфейса из vRealize Automation.
- vRealize Automation может указывать на виртуальный IP-адрес кластера. В этом случае одному диспетчеру NSX передается управление виртуальным IP-адресом. Диспетчер получает вызовы API-интерфейса из vRealize Automation. В случае сбоя другой узел в кластере принимает на себя управление виртуальным IP-адресом и получает вызовы API-интерфейса из vRealize Automation.

Дополнительные сведения по настройке виртуального IP-адреса см. в разделе *Настройка виртуального IP-адреса (VIP) для кластера в руководстве по установке NSX-T Data Center* в [документации VMware по NSX-T Data Center](#).

- vRealize Automation может указывать на виртуальный IP-адрес подсистемы балансировки нагрузки для распределения вызовов по трем диспетчерам NSX. В этом случае все три диспетчера NSX получают вызовы API-интерфейса из vRealize Automation.

Виртуальный IP-адрес можно настроить в сторонней подсистеме балансировки нагрузки или в подсистеме балансировки нагрузки NSX-T.

Данный вариант рекомендуется использовать для крупных сред, чтобы распределять вызовы API-интерфейса vRealize Automation между тремя диспетчерами NSX.

Используйте эту информацию при указании конечной точки NSX-T на шаге 5.

Конечную точку NSX-T можно связать с одной или несколькими конечными точками vSphere.

Можно создать связь между конечными точками vSphere и NSX. Связи могут быть следующими:

- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere.
- Одна конечная точка vSphere связана с несколькими конечными точками NSX-T.

- Одна конечная точка NSX-T связана с несколькими конечными точками vSphere.
- Одна конечная точка NSX for vSphere связана с одной конечной точкой vSphere.
- Одна конечная точка vSphere связана с одной конечной точкой NSX for vSphere и с одной конечной точкой NSX-T.

Если конечная точка vSphere связана как с конечной точкой NSX for vSphere, так и с конечной точкой NSX-T, то кластером управляет NSX for vSphere или NSX-T. Диспетчер NSX определяется vRealize Automation, когда с конечных точек собираются данные и устанавливается взаимосвязь.

Чтобы узнать тип платформы NSX, управляющей определенным кластером, нужно посмотреть столбец **Тип NSX** на странице **Вычислительные ресурсы**.

При развертывании схемы элементов, которая содержит конечную точку NSX-T, развертывание назначает тег компонентам NSX-T в развертывании. Имя тега совпадает с именем развертывания.

Информацию о проверке подключения конечной точки и доверии для сертификатов см. в разделе [Факторы, которые следует учитывать при проверке подключения](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Следует установить прокси-агент vSphere для управления конечной точкой vSphere, также следует использовать одинаковое имя для конечной точки и агента. Информацию об установке агента см. в разделе *Установка vRealize Automation*.
- Настройте параметры сети NSX-T. См. раздел [Настройка параметров компонентов сети и безопасности в vRealize Automation](#).
- [Создание конечной точки vSphere в vRealize Automation и ее связывание с NSX](#).

В процессе подготовки к использованию возможностей сети, безопасности и балансировки нагрузки NSX в vRealize Automation при использовании учетных данных диспетчера NSX необходимо использовать учетную запись администратора диспетчера NSX.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Сеть и безопасность > NSX-T**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. Введите URL-адрес для экземпляра диспетчера конечных точек NSX-T или виртуального IP-адреса (см. выше) в текстовом поле **Адрес**.

Тип URL-адреса должен быть таким: **https://имя_узла** или **https://IP-адрес**.

Например: **https://abx-nsxt3-manager.local**

6. Введите имя пользователя с правами администратора и пароль NSX, сохраненные для конечной точки NSX-T.

7. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
8. Чтобы связать параметры сети и безопасности NSX-T с существующей конечной точкой vSphere, нажмите кнопку **Связи** и выберите существующую конечную точку vSphere.

Перед созданием связи необходимо создать конечную точку vSphere.

Конечную точку vSphere можно связать только с одним типом платформы сети и безопасности — NSX for vSphere или NSX-T.

Конечную точку NSX-T можно связать с несколькими конечными точками vSphere. Один экземпляр NSX-T может управлять несколькими кластерами ESX на разных экземплярах vCenter.

По окончании создания связи в столбце «Описание» (Description) на странице указывается тип связи для NSX-T.

9. (дополнительно) Выберите элемент **Проверить подключение**, чтобы проверить учетные данные, адрес конечной точки узла и доверие к сертификату. Одновременно проверяется рабочее состояние службы диспетчера и агента, а также возможность получения данных из конечной точки. При нажатии кнопки **ОК** проверяются те же условия.

Команда **Проверить подключение** возвращает следующие возможные результаты проверки.

- **Ошибка сертификата**

Если сертификат не найден, признан ненадежным или срок его действия истек, отобразится запрос на принятие отпечатка сертификата. Если отпечаток не будет принят, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

- **Ошибка агента**

Связанный агент vSphere не найден. Для успешной проверки требуется запущенный агент.

- **Ошибка узла**

Указанный адрес конечной точки недоступен, или не запущена связанная служба диспетчера. Для успешной проверки требуется запущенная служба диспетчера.

- **Ошибка в учетных данных**

Обнаружено недопустимое сочетание имени пользователя и пароля для конечной точки с указанным адресом.

- **Timeout**

Проверка не завершилась в течение отведенного времени (2 минуты).

Если действие **Проверка подключения** не выполнено, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

Если возникла проблема с доверенным сертификатом (например, истек срок его действия), отобразится запрос на принятие отпечатка сертификата.

10. Чтобы сохранить конечную точку, нажмите кнопку **ОК**.

При нажатии кнопки **ОК** проверяются те же условия, что и при действии **Проверка подключения**. Если выполняется любое из указанных выше условий, выводится сообщение. Если сохранение все же будет выполнено, на экране для пользователя останется сообщение об ошибке.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Дополнительные сведения о запуске сбора данных для существующих конечных точек после первоначального сбора данных см. в разделе [Просмотр вычислительных ресурсов и запуск сбора данных](#).

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки vCloud Air

Конечную точку vCloud Air можно создать для службы, предоставляемой по требованию или по подписке. При необходимости можно привязать параметры прокси-сервера к конечной точке vCloud Director, выполнив привязку к конечной точке прокси-сервера.

Сведения о консоли управления vCloud Air см. в документации по vCloud Air.

Примечание Резервирования, определенные для конечных точек vCloud Air и конечных точек vCloud Director, не поддерживают использование профилей сети для подготавливаемых компьютеров.

Для конечных точек vCloud Air название организации и имя VDC должны быть идентичными для экземпляра подписки vCloud Air.

Дополнительные сведения о привязке параметров прокси-сервера к конечной точке см. в разделе [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Убедитесь, что у вас есть права **администратора виртуальной инфраструктуры** для учетной записи службы подписки vCloud Air или учетной записи OnDemand.
- Если необходимо настроить дополнительные параметры безопасности и подключение через прокси-сервер, создайте конечную точку прокси-сервера. Выполнить привязку к конечной точке прокси-сервера можно при создании конечной точки vCloud Director. См. раздел [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Облако > vCloud Air**.
3. Введите имя и, при необходимости, описание.

4. Примите используемый по умолчанию адрес конечной точки vCloud Air, указанный в текстовом поле **Адрес**, или введите новый.

Используемый по умолчанию адрес конечной точки vCloud Air — <https://vca.vmware.com> (как указано в глобальном свойстве Default URL for vCloud Air endpoint).

5. Введите имя и пароль администратора.

Следует использовать учетные данные службы подписки vCloud Air или администратора учетной записи OnDemand.

Формат имени пользователя: *domain\username*.

Укажите учетные данные администратора организации с правами на подключение с помощью VMware Remote Console.

6. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
7. (дополнительно) Чтобы настроить дополнительные безопасные и обязательные подключения через прокси-сервер, выберите элемент **Связи** и создайте связь с существующей конечной точкой прокси-сервера.

Для создания связи необходима хотя бы одна конечная точка прокси-сервера.

8. Нажмите кнопку **ОК**.

Следующие шаги

[Создание групп структур.](#)

Создание конечной точки vCloud Director

Вы можете создать конечную точку vCloud Director для управления всеми виртуальными центрами данных vCloud Director в вашей среде или создать отдельные конечные точки для управления каждой организацией vCloud Director. При необходимости можно привязать параметры прокси-сервера к конечной точке vCloud Director, выполнив привязку к конечной точке прокси-сервера.

Сведения о виртуальных центрах данных см. в документации по vCloud Director.

Не создавайте автономную конечную точку и конечные точки организации для одного и того же экземпляра vCloud Director.

vRealize Automation использует прокси-агент для управления ресурсами vSphere.

Примечание Резервирования, определенные для конечных точек vCloud Air и конечных точек vCloud Director, не поддерживают использование профилей сети для подготавливаемых компьютеров.

Сведения об аренде для компьютеров vCloud Director должны быть указаны в vRealize Automation, а не в vCloud Director. Если сведения об аренде указываются в vCloud Director, они не будут распознаны и использованы в vRealize Automation. Введите сведения об аренде для компьютеров vCloud Director в своей схеме элементов vRealize Automation, а не в vCloud Director.

Дополнительные сведения о привязке параметров прокси-сервера к конечной точке см. в разделе [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Если необходимо настроить дополнительные параметры безопасности и подключение через прокси-сервер, создайте конечную точку прокси-сервера. Выполнить привязку к конечной точке прокси-сервера можно при создании конечной точки vCloud Director. См. раздел [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Облако > vCloud Director**.
3. Введите имя и, при необходимости, описание.
4. В текстовом поле **Адрес** укажите URL-адрес сервера vCloud Director.
URL-адрес должен относиться к типу *Полное доменное имя* или *IP-адрес*.
Например, <https://mycompany.com>.
5. Введите имя и пароль администратора.
 - Чтобы подключиться к серверу vCloud Director и указать организацию, в которой у пользователя есть роль администратора, используйте учетные данные администратора организации. Используя эти учетные данные, конечная точка может получить доступ только к связанным виртуальным центрам данных организации. Вы можете добавить конечные точки для каждой дополнительной организации в экземпляре vCloud Director, чтобы выполнить интеграцию с решением vRealize Automation.
 - Чтобы предоставить доступ всем виртуальным центрам данных организации в экземпляре vCloud Director, воспользуйтесь учетными данными системного администратора для vCloud Director и не заполняйте текстовое поле **Организация**.
6. Если вы являетесь администратором организации, вы можете ввести имя организации vCloud Director в текстовом поле **Организация**.

Параметр	Описание
Обнаружение всех виртуальных центров данных организации	Если вы реализовали vCloud Director в частном облаке, можно не заполнять текстовое поле Организация , чтобы разрешить приложению обнаруживать все доступные виртуальные центры данных организации.
Отдельные конечные точки для каждого виртуального центра данных организации	В текстовом поле Организация введите имя организации vCloud Director.

Имя в текстовом поле **Организация** совпадает с именем вашей организации vCloud Director, которая может быть также именем вашего виртуального центра данных. Если вы используете Virtual Private Cloud, это имя является уникальным идентификатором в формате M123456789–12345. В выделенном облаке это имя целевого виртуального центра данных.

Для подключения непосредственно к vCloud Director на уровне системы, например без заполнения поля «Организация», требуются учетные данные системного администратора. Если в конечной точке вы указываете организацию, потребуется пользователь с учетными данными администратора данной организации.

Укажите учетные данные с правами на подключение с помощью VMware Remote Console.

- Чтобы управлять всеми организациями с использованием одной конечной точки, укажите учетные данные системного администратора.
- Чтобы управлять виртуальным центром обработки данных каждой организации с использованием отдельных конечных точек, создайте отдельные учетные данные администратора организации для каждого виртуального центра обработки данных.

Не создавайте автономную системную конечную точку и конечные точки организации для одного и того же экземпляра vCloud Director.

7. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
8. (дополнительно) Чтобы настроить дополнительные безопасные и обязательные подключения через прокси-сервер, выберите элемент **Связи** и создайте связь с существующей конечной точкой прокси-сервера.

Для создания связи необходима хотя бы одна конечная точка прокси-сервера.

9. Нажмите кнопку **ОК**.

Следующие шаги

[Создание групп структур.](#)

Создание конечной точки Amazon

Вы можете создать конечную точку, чтобы подключиться к экземпляру Amazon. При необходимости можно связать настройки прокси-сервера с конечной точкой Amazon, выполнив связывание с конечной точкой прокси-сервера.

vRealize Automation позволяет использовать несколько типов экземпляров Amazon при создании схем элементов. Сведения о том, как импортировать собственные типы экземпляров, см. в разделе [Добавление типа экземпляра Amazon](#).

Дополнительные сведения о привязке параметров прокси-сервера к конечной точке см. в разделе [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Если необходимо настроить дополнительные параметры безопасности и подключение через прокси-сервер, создайте конечную точку прокси-сервера. При создании конечной точки Amazon можно настроить связь с конечной точкой прокси-сервера. См. раздел [Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы](#).

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.

2. Выберите **Создать > Облако > Amazon EC2**.

3. Введите имя и, при необходимости, описание.

Обычно это имя указывает на учетную запись Amazon, которая соответствует этой конечной точке.

4. Укажите идентификатор ключа доступа административного уровня для конечной точки Amazon.

С идентификатором ключа доступа Amazon должна быть связана только одна конечная точка.

Получить ключ доступа, необходимый для создания конечной точки Amazon, можно двумя способами. Во-первых, можно запросить ключ у пользователя с учетными данными администратора AWS с полным доступом. Во-вторых, можно дополнительно настроить права привилегированного пользователя с помощью политики для администратора AWS с полным доступом. Дополнительную информацию см. в документации Amazon.

5. Укажите секретный ключ доступа для конечной точки Amazon.

6. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.

7. (дополнительно) Чтобы настроить дополнительные безопасные и обязательные подключения через прокси-сервер, выберите элемент **Связи** и создайте связь с существующей конечной точкой прокси-сервера.

Для создания связи необходима хотя бы одна конечная точка прокси-сервера.

8. Нажмите кнопку **ОК**.

Результаты

После создания конечной точки vRealize Automation начнет сбор данных из областей Amazon Web Services.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Добавление типа экземпляра Amazon

Вместе с vRealize Automation поставляется несколько типов экземпляров, которые предназначены для использования со схемами элементов Amazon. Администратор может добавлять и удалять типы экземпляров.

Типы экземпляров компьютеров, которыми управляют администраторы инфраструктуры как услуги, доступны разработчикам архитектуры схем элементов, когда они создают или изменяют схемы элементов Amazon. Образы компьютеров Amazon и типы экземпляров Amazon делаются доступными с помощью продукта Amazon Web Services.

Необходимые условия

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

Процедура

1. Откройте **Инфраструктура > Администрирование > Типы экземпляров**.
2. Нажмите кнопку **Создать**.
3. Добавьте новый тип экземпляра, указав следующие параметры.

Сведения о доступных типах экземпляров Amazon и значениях, которые можно указать для их параметров, см. в документации по Amazon Web Services в разделе *Типы экземпляров EC2 — Amazon Web Services (AWS)* на сайте aws.amazon.com/ec2 и *Типы экземпляров* на сайте docs.aws.amazon.com.

- Имя
- Имя API
- Имя типа
- Название производительности ввода-вывода
- ЦП
- Память (ГБ)
- Хранилище (ГБ)
- Вычислительные модули

4. Щелкните значок **Сохранить** (✓).

Результаты

Когда разработчики архитектуры инфраструктуры как услуги создают схемы элементов Amazon Web Services, они могут использовать ваши настраиваемые типы экземпляров.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки прокси-сервера и связывание с конечной точкой облачной службы

Можно создать конечную точку прокси-сервера и связать ее параметры прокси-сервера с конечной точкой vCloud Air, vCloud Director или Amazon.

После обновления или переноса конечной точки vCloud Air, vCloud Director или конечной точки Amazon, использующей диспетчер прокси-сервера, создается новая конечная точка vCloud Air, vCloud Director или Amazon, в которой содержится связь между конечной точкой vCloud Air, vCloud Director или Amazon и новой конечной точкой прокси-сервера.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Создайте конечную точку одного из следующих типов:
 - [Создание конечной точки vCloud Air](#)
 - [Создание конечной точки Amazon](#)

■ Создание конечной точки vCloud Director

Для связывания конечной точки прокси-сервера необходимо иметь хотя бы одну конечную точку vCloud Air, vCloud Director или Amazon.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Сеть и безопасность > Прокси-сервер**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. В текстовом поле **Адрес** укажите URL-адрес установленного прокси-агента.
6. Укажите номер порта, который нужно указывать для подключения к прокси-серверу в текстовом поле **Порт**.
7. Введите имя и пароль администратора.
8. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
9. Чтобы связать параметры прокси-сервера с конечной точкой vCloud Air, vCloud Director или Amazon, нажмите кнопку **Связи** и выберите конечные точки.

Для создания связи необходима хотя бы одна конечная точка vCloud Air, vCloud Director или Amazon.

Конечную точку прокси-сервера можно связать с несколькими конечными точками.

10. Нажмите кнопку **ОК**.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки прокси-сервера для веб-сайта узла OVF

Можно создать конечную точку прокси-сервера для использования при импорте файла OVF в компонент компьютера vSphere в схеме элементов или в качестве набора значений для профиля компонента «Образ» при размещении файла OVF на веб-сайте.

Дополнительные сведения по настройке для развертывания OVF см. в разделе [Создание конечной точки vSphere в vRealize Automation](#) и ее связывание с NSX и [Настройка схемы элементов для подготовки из файла OVF](#).

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Сеть и безопасность > Прокси-сервер**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. В текстовом поле **Адрес** введите URL-адрес для веб-сайт, на котором размещается файл OVF.
6. В текстовом поле **Порт** укажите номер порта, который нужно использовать для подключения к прокси-серверу.
7. Введите имя и пароль администратора.
8. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
9. Нажмите кнопку **ОК**.

Результаты

Теперь можно использовать конечную точку для определения веб-сайта, на котором необходимо получить OVF. Дополнительные сведения см. в разделе [Определение параметров схемы элементов для компонента vSphere с помощью файла OVF](#) и [Определение набора значений образа для профиля компонента с помощью файла OVF](#).

Создание конечной точки vRealize Orchestrator

Можно создать конечную точку vRealize Orchestrator для подключения к серверу vRealize Orchestrator.

Вы можете настроить несколько конечных точек, чтобы подключиться к разным серверам vRealize Orchestrator, однако для каждой конечной точки нужно задать приоритет.

При выполнении рабочих процессов vRealize Orchestrator vRealize Automation сначала использует конечную точку vRealize Orchestrator с наивысшим приоритетом. Если к ней невозможно подключиться, то устройство переходит к следующей конечной точке с наивысшим приоритетом, пока сервер vRealize Orchestrator не сможет выполнить рабочий процесс.

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Оркестрация > vRealize Orchestrator**.
3. Введите имя и, при необходимости, описание.

4. Введите URL-адрес с полным квалифицированным именем или IP-адрес сервера vRealize Orchestrator и номер порта vRealize Orchestrator.

Следует использовать транспортный протокол HTTPS. Если порт не указан, используется порт по умолчанию 443.

Чтобы использовать экземпляр vRealize Orchestrator по умолчанию, который содержится в устройстве vRealize Automation, введите

`https://vrealize-automation-appliance-hostname:443/vco`.

5. Укажите свои учетные данные vRealize Orchestrator в текстовых полях **Имя пользователя** и **Пароль**, чтобы подключиться к конечной точке vRealize Orchestrator.

Используемые учетные данные должны иметь разрешения на выполнение любых рабочих процессов vRealize Orchestrator, которые можно вызвать из Инфраструктура как услуга

Чтобы использовать экземпляр vRealize Orchestrator по умолчанию, содержащийся в устройстве vRealize Automation, используйте имя пользователя **administrator@vsphere.local** и пароль администратора, указанный при настройке службы единого входа.

6. В текстовом поле **Свойство** введите целое число не меньше 1.

Чем меньше значение, тем выше приоритет.

7. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.

8. Нажмите кнопку **ОК**.

Настройка конечных точек vRealize Orchestrator для сети

Если вы используете рабочие процессы vRealize Automation для вызова рабочих процессов vRealize Orchestrator, нужно настроить экземпляр или сервер vRealize Orchestrator в качестве конечной точки.

Сведения о добавлении конечной точки vRealize Orchestrator см. здесь [Создание конечной точки vRealize Orchestrator](#).

Конечную точку vRealize Orchestrator можно связать со схемой элементов нескольких компьютеров, чтобы убедиться, что для запуска всех рабочих процессов vRealize Orchestrator компьютеров, подготовленных с использованием этой схемы элементов, применена эта конечная точка.

vRealize Automation содержит встроенный экземпляр vRealize Orchestrator по умолчанию.

Рекомендуется использовать встроенный экземпляр в качестве конечной точки vRealize Orchestrator для выполнения рабочих процессов vRealize Automation в производственной или тестовой среде или создания пилотной версии.

Также рекомендуется использовать эту конечную точку vRealize Orchestrator для запуска рабочих процессов vRealize Automation в производственной среде.

Подключаемый модуль vRealize Orchestrator автоматически устанавливается с vRealize Orchestrator 7.1 или более поздних версий. Отдельно устанавливаемые подключаемые модули vRealize Orchestrator отсутствуют.

Создание конечной точки vRealize Operations Manager

Можно создать конечную точку vRealize Operations Manager для подключения к API пакета узла vRealize Operations Manager.

Дополнительные сведения о проверке подключения vRealize Operations Manager и доверии для сертификатов см. в разделе [Факторы, которые следует учитывать при проверке подключения](#).

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Управление > vRealize Operations Manager**.
3. Введите имя и, при необходимости, описание.
4. В текстовом поле **Адрес** укажите URL-адрес сервера vRealize Operations Manager.
Формат URL-адреса: **https://hostname/suite-api**.
5. Введите свои имя пользователя и пароль vRealize Operations Manager.
6. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
7. (дополнительно) Выберите элемент **Проверить подключение**, чтобы проверить учетные данные, адрес конечной точки узла и доверие к сертификату. Одновременно проверяется рабочее состояние службы диспетчера и агента, а также возможность получения данных из конечной точки. При нажатии кнопки **ОК** проверяются те же условия.

Команда **Проверить подключение** возвращает следующие возможные результаты проверки.

- **Ошибка сертификата**
Если сертификат не найден, признан ненадежным или срок его действия истек, отобразится запрос на принятие отпечатка сертификата. Если отпечаток не будет принят, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.
- **Ошибка агента**
Связанный агент vSphere не найден. Для успешной проверки требуется запущенный агент.
- **Ошибка узла**
Указанный адрес конечной точки недоступен, или не запущена связанная служба диспетчера. Для успешной проверки требуется запущенная служба диспетчера.
- **Ошибка в учетных данных**
Обнаружено недопустимое сочетание имени пользователя и пароля для конечной точки с указанным адресом.
- **Timeout**

Проверка не завершилась в течение отведенного времени (2 минуты).

Если действие **Проверка подключения** не выполнено, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

Если возникла проблема с доверенным сертификатом (например, истек срок его действия), отобразится запрос на принятие отпечатка сертификата.

8. Нажмите кнопку **ОК**.

Создание конечной точки стороннего поставщика управления IP-адресами

Если в vRealize Orchestrator зарегистрирован и настроен тип сторонней конечной точки управления IP-адресами, то в vRealize Automation можно создать конечную точку для этого поставщика управления IP-адресами.

Если вы импортировали пакет vRealize Orchestrator для внешнего решения по управлению IP-адресами и зарегистрировали тип конечной точки управления IP-адресами в vRealize Orchestrator, вы можете выбрать этот тип конечной точки управления IP-адресами при создании конечной точки vRealize Automation.

Примечание В основе этого примера лежит использование подключаемого модуля управления IP-адресами Infoblox, который можно скачать на портале VMware Solution Exchange. Эту процедуру также можно использовать, если создан собственный пакет поставщика управления IP-адресами с помощью комплекта SDK для управления IP-адресами от VMware. Процедура импорта и настройки собственного пакета для управления IP-адресами от стороннего поставщика такая же, как описано в предварительных требованиях.

Первая конечная точка управления IP-адресами для vRealize Automation создается при регистрации типа конечной точки для подключаемого модуля поставщика решений управления IP-адресами в vRealize Orchestrator.

Необходимые условия

- [Получение и импорт пакета стороннего поставщика управления IP-адресами в vRealize Orchestrator.](#)
- [Запустите рабочий процесс для регистрации типа сторонней конечной точки управления IP-адресами в vRealize Orchestrator.](#)
- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.

Для этого примера создайте конечную точку управления IP-адресами Infoblox, используя тип конечной точки, который был зарегистрирован в vRealize Orchestrator для подключаемого модуля или пакета стороннего поставщика управления IP-адресами.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.

2. Выберите Создать > Управление IP-адресами > Тип конечной точки управления IP-адресами.

Выберите тип конечных точек внешнего зарегистрированного поставщика управления IP-адресами, например Infoblox. Конечные точки внешнего поставщика управления IP-адресами доступны, только если импортирован сторонний пакет vRealize Orchestrator и выполнены его рабочие процессы для регистрации типа конечных точек.

Для управления IP-адресами Infoblox в списке отображаются только основные типы конечных точек. Типы дополнительных конечных точек управления IP-адресами можно задать с помощью настраиваемых свойств.

Например, выберите тип конечных точек внешнего зарегистрированного поставщика управления IP-адресами **Infoblox NIOS**.

3. Введите имя и, при необходимости, описание.

4. В текстовом поле Адрес введите расположение зарегистрированной конечной точки управления IP-адресами, используя формат URL-адреса для данного поставщика, например `https://host_name/name`.

Например, создано несколько конечных точек управления IP-адресами, таких как `https://nsx62-scale-infoblox` и `https://nsx62-scale-infoblox2`, при регистрации типа конечных точек управления IP-адресами в vRealize Orchestrator. Введите основной зарегистрированный тип конечной точки. Чтобы указать одну или несколько дополнительных конечных точек управления IP-адресами, можно использовать настраиваемые свойства для моделирования расширяемых атрибутов, относящихся к данному поставщику решений управления IP-адресами.

5. Чтобы получить доступ к учетной записи поставщика решения для управления IP-адресами, необходимо ввести имя пользователя и пароль.

Учетные данные учетной записи поставщика решений управления IP-адресами необходимы для создания, настройки и редактирования конечной точки при работе в vRealize Automation. vRealize Automation использует учетные данные конечных точек управления IP-адресами для обмена данными с заданным типом конечной точки, например Infoblox, чтобы выделять IP-адреса и выполнять другие операции. Это поведение аналогично использованию учетных данных конечных точек vSphere в vRealize Automation.

6. (дополнительно) Выберите элемент Свойства и добавьте свойства конечных точек, которые имеют значение для данного поставщика решений управления IP-адресами.

Для каждого поставщика решений управления IP-адресами, например Infoblox и Bluecat, используются уникальные расширяемые атрибуты, которые можно моделировать с помощью настраиваемых свойств vRealize Automation. Например, Infoblox использует расширяемые атрибуты, чтобы различать основные и дополнительные конечные точки.

7. Нажмите кнопку ОК.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки Microsoft Azure

Можно создать конечную точку Microsoft Azure, чтобы упростить подключение с использованием учетных данных между vRealize Automation и развертыванием Azure.

Конечная точка обеспечивает подключение к ресурсу, в данном случае — экземпляру Azure, который можно использовать для создания схем элементов виртуальной машины. У вас должна быть конечная точка Azure, которая будет использоваться как основа схемы элементов для подготовки виртуальных машин Azure. Если используется несколько подписок Azure, необходимы конечные точки для каждого идентификатора подписки.

Либо можно создать подключение Azure непосредственно из vRealize Orchestrator, используя команду «Добавить подключение Azure» в разделе **Библиотека > Azure > Конфигурация** в дереве рабочих процессов vRealize Orchestrator. Для большинства сценариев рекомендуется использовать подключение через конечную точку (как описано здесь).

Конечные точки Azure поддерживаются vRealize Orchestrator и элементами «Все как услуга». Конечную точку Azure можно создать, удалить и изменить. Если изменить существующую конечную точку и не выполнять никакие обновления на портале Azure через новое подключение в течение нескольких часов, могут возникнуть проблемы. Необходимо перезапустить службу vRealize Orchestrator с помощью команды `service vco-service restart`. Если этого не сделать, могут возникнуть ошибки.

Необходимые условия

- Настройте экземпляр Microsoft Azure и получите действующую подписку Microsoft Azure, позволяющую использовать идентификатор подписки. Подробнее о настройке Azure и получении идентификатора подписки см. в разделе [Настройка конечной точки Microsoft Azure](#).
- Убедитесь, что в развертывании vRealize Automation есть по крайней мере один арендатор и одна бизнес-группа.
- Создайте приложение Active Directory, как описано в разделе <https://azure.microsoft.com/ru-ru/documentation/articles/resource-group-create-service-principal-portal>.
- Запишите указанную далее информацию, связанную с Azure, так как она понадобится во время настройки конечной точки и схемы элементов.
 - идентификатор подписки
 - идентификатор арендатора
 - имя учетной записи хранилища
 - имя группы ресурса
 - расположение
 - имя виртуальной сети
 - идентификатор клиентского приложения
 - секретный ключ клиентского приложения
 - URN образа виртуальной машины

- Развертывание vRealize Automation Azure поддерживается в некоторых регионах распространения Microsoft Azure. См. раздел [Регионы с поддержкой Azure](#).
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.
3. На вкладке «Подключаемый модуль» в раскрывающемся меню **Подключаемый модуль** выберите вариант **Azure**.
4. Нажмите кнопку **Далее**.
5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Заполните текстовые поля на вкладке «Сведения» в соответствии с параметрами конечной точки.

Параметр	Описание
Параметры подключения	
Имя подключения	Уникальное имя для подключения к новой конечной точке. Это имя появится в интерфейсе vRealize Orchestrator, чтобы помочь определить конкретное подключение.
Идентификатор подписки Azure	Идентификатор подписки Azure. Идентификатор определяет учетные записи хранения, виртуальные машины и другие ресурсы Azure, к которым вы имеете доступ.
Среда Azure	Географический регион для развернутого ресурса Azure. vRealize Automation поддерживает все текущие регионы Azure, в зависимости от идентификатора подписки.
Параметры диспетчера ресурсов	
URI-адрес службы Azure	URI-адрес, который обеспечивает доступ к вашему экземпляру Azure. Значение по умолчанию <code>https://management.azure.com/</code> подходит для многих типичных реализаций. Это поле автоматически заполняется при выборе среды.
Идентификатор арендатора	Идентификатор арендатора Azure, который должен использоваться конечной точкой.
Идентификатор клиента	Идентификатор клиента Azure, который должен использоваться конечной точкой. Он назначается при создании приложения Active Directory.
Секретный ключ клиента	Ключ, который используется с идентификатором клиента Azure. Этот ключ назначается при создании приложения Active Directory.
URI-адрес хранилища Azure	URI-адрес, по которому вы получаете доступ к экземпляру хранилища Azure. Это поле автоматически заполняется при выборе среды.

Параметр	Описание
Параметры прокси	
Прокси-узел	Если в компании используется веб-сервер прокси, введите имя узла этого сервера.
Прокси-порт	Если в компании используется веб-сервер прокси, введите номер порта этого сервера.

8. (дополнительно) Выберите элемент «Свойства» и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения настраиваемых свойств.

9. Щелкните элемент **Готово**.

Следующие шаги

Создайте соответствующие группы ресурсов, учетные записи хранения и группы безопасности сети в Azure. Нужно также создать подсистемы балансировки нагрузки, если это необходимо для реализации.

Действие	Параметры
Создание группы ресурсов Azure	<ul style="list-style-type: none"> ■ Создайте группу ресурсов с помощью портала Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Resource/Create resource group. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Вы можете запросить группу ресурсов после того, как свяжите ее со службой и правами. <p>Примечание Тип ресурса «Группа ресурсов» не поддерживается и недоступен для управления в решении vRealize Automation.</p>
Создание учетной записи хранения Azure	<ul style="list-style-type: none"> ■ Создайте учетную запись хранения с помощью Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Storage/Create storage account. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Вы можете запросить учетную запись хранения после того, как свяжите ее со службой и правами.
Создание группы безопасности сети Azure	<ul style="list-style-type: none"> ■ Создайте группу безопасности с помощью Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Network/Create Network security group. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Группу безопасности можно запросить после того, как она будет связана со службой и правами.

Настройка конечной точки Microsoft Azure

Чтобы создать конечную точку Microsoft Azure в vRealize Automation, необходимо собрать сведения и настроить некоторые параметры.

Процедура

1. Найдите и запишите идентификатор подписки и арендатора Microsoft Azure.

- Идентификатор подписки. Щелкните значок «Подписки» на левой панели инструментов на портале Azure, чтобы посмотреть идентификатор подписки.
- Идентификатор арендатора. Щелкните значок «Справка» и выберите «Показать данные диагностики» на портале Azure. Найдите арендатора и запишите его идентификатор.

2. Чтобы начать работу, можно создать новую учетную запись хранилища и группу ресурсов. Вы также можете создать их позже в схемах элементов.

- Учетная запись хранилища. Для настройки учетной записи выполните следующие действия.
 1. На портале Azure найдите на боковой панели значок «Учетные записи хранилища». Убедитесь, что выбрана верная подписка, и щелкните **Добавить**. Для поиска учетной записи хранилища также можно использовать поле поиска Azure.
 2. Введите необходимую информацию для учетной записи хранилища. Вам понадобится идентификатор подписки.
 3. Выберите, следует ли использовать существующую группу ресурсов или создать новую. Запишите имя группы ресурсов: она понадобится вам позже.

Примечание Сохраните расположение учетной записи хранилища (оно понадобится вам позже).

3. Создайте виртуальную сеть. Если у вас уже есть подходящая сеть, можно выбрать ее.

При создании сети необходимо выбрать параметр «Использовать существующую группу ресурсов» и указать группу, созданную на предыдущем этапе. Кроме того, необходимо выбрать расположение, которое вы указали ранее. Microsoft Azure не сможет развернуть виртуальные машины и другие объекты, если для всех применимых компонентов, которые будут использоваться объектом, не будет указано одно и то же расположение.

- а) Найдите значок «Виртуальная сеть» на левой панели и щелкните его или выполните поиск виртуальной сети. Убедитесь, что выбрана верная подписка, и нажмите **Добавить**.
- б) Введите неповторяющееся имя для новой виртуальной сети и запишите его для последующего использования.
- в) Введите соответствующий IP-адрес виртуальной сети в поле **Адресное пространство**.
- г) Убедитесь, что выбрана верная подписка, и щелкните **Добавить**.
- д) Укажите остальные параметры базовой конфигурации.
- е) Вы можете изменить остальные параметры, но в большинстве конфигураций можно оставить значения по умолчанию.
- ж) Щелкните **Создать**.

4. Настройте приложение Azure Active Directory для проверки подлинности в vRealize Automation.

- а) Найдите значок Active Directory в левом меню Azure и щелкните его.
- б) Щелкните **Регистрация приложений** и нажмите **Добавить**.
- в) Введите имя приложения, которое соответствует правилам именования Azure.
- г) Оставьте в параметре «Тип приложения» значение «Веб-приложение/API-интерфейс» (Web app/API).
- д) Можно указать любой URL-адрес входа, подходящий для вашего варианта использования.
- е) Щелкните **Создать**.

5. Создайте секретный ключ для проверки подлинности приложения в vRealize Automation.
 - а) Щелкните имя приложения в Azure.
Запишите идентификатор приложения, чтобы использовать его в дальнейшем.
 - б) Щелкните **Все настройки** в следующей панели и выберите в списке настроек элемент «Ключи».
 - в) Введите описание нового ключа и выберите продолжительность.
 - г) Щелкните **Сохранить** и скопируйте значение ключа в безопасное место, поскольку в дальнейшем получить его будет невозможно.
 - д) В меню слева выберите **Разрешения API-интерфейса** для данного приложения и щелкните **Добавить разрешение**, чтобы создать новое разрешение.
 - е) Выберите «Управление службами Azure» на странице «Выбор API-интерфейса».
 - ж) Щелкните **Делегированные разрешения**.
 - з) В разделе «Выбор разрешений» выберите user_impersonation, а затем щелкните **Добавить разрешения**.
6. Выполните проверку подлинности для подключения приложения Active Directory к подписке Azure, чтобы иметь возможность развертывать виртуальные машины и управлять ими.
 - а) В меню слева щелкните значок «Подписки» и выберите новую подписку.
Возможно, понадобится щелкнуть текст названия, чтобы выполнить прокрутку панели.
 - б) Чтобы отобразить разрешения для подписки, выберите параметр «Управление доступом (IAM)».
 - в) Щелкните **Добавить** в разделе «Добавить назначение ролей».
 - г) Выберите «Участник» в раскрывающемся списке «Роль».
 - д) Оставьте значение по умолчанию в раскрывающемся списке «Предоставить доступ».
 - е) В поле «Выбрать» введите имя приложения.
 - ж) Нажмите кнопку **Сохранить**.
 - з) Добавьте дополнительные роли: «Владелец», «Участник» и «Читатель».
 - и) Нажмите кнопку **Сохранить**.

Следующие шаги

Необходимо установить средства интерфейса командной строки Microsoft Azure. Эти средства доступны бесплатно для операционных систем Windows и Mac. Дополнительные сведения о загрузке и установке этих средств см. в документации Microsoft.

После установки интерфейса командной строки необходимо пройти проверку подлинности в новой подписке.

1. Откройте окно терминала и введите имя пользователя Microsoft Azure. Вам будет отправлен URL-адрес и шорткод для проверки подлинности.

2. Введите в браузере код, полученный из приложения на устройстве.
3. Введите код проверки подлинности и щелкните **Продолжить**.
4. Выберите учетную запись Azure и войдите в нее.

При наличии нескольких подписок убедитесь, что выбран правильный вариант, с помощью команды `azure account set <subscription-name>`.

5. Прежде чем продолжить, необходимо зарегистрировать поставщика Microsoft.Compute в новой подписке Azure с помощью команды `azure provider register microsoft.compute`.

Если при первом выполнении команды время ожидания истекает и появляется сообщение об ошибке, выполните команду снова.

После завершения настройки можно использовать команду `azure vm image list` для получения доступных имен образов виртуальных машин. Можно выбрать нужный образ, записать его URN, а затем использовать его в схемах элементов.

Создание конечной точки Puppet

Конечную точку Puppet можно создать для поддержки добавления компонентов управления конфигурацией Puppet в виртуальные машины vSphere. Эти компоненты позволяют с помощью главного узла Puppet применять управление конфигурацией на виртуальных машинах.

Конечная точка устанавливает соединение с внешним ресурсом (в данном случае — с экземпляром главного узла Puppet). Конечная точка позволяет размещать компоненты управления конфигурацией Puppet в схемах элементов виртуальных машин vSphere. Подготовленные на основе этих схем элементы виртуальные машины содержат агент Puppet, который облегчает управление, выполняемое с помощью связанного главного узла Puppet.

Дополнительные сведения о подключаемом модуле Puppet и демонстрацию его настройки см. в разделе <https://www.youtube.com/watch?v=P-VglzE9o-o>.

Необходимые условия

- Установите решение Puppet Enterprise и настройте его должным образом в своей среде.
- Загрузите и установите подключаемый модуль Puppet версии 3.0 в своем развертывании vRealize Orchestrator. Этот подключаемый модуль можно загрузить отсюда: <https://marketplace.vmware.com/vsx/solutions/puppet-plugin-for-vrealize-automation?ref=search>. Сведения о его установке и использовании см. в статье https://docs.puppet.com/pe/latest/vro_intro.html.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.
3. На вкладке «Подключаемый модуль» в раскрывающемся меню **Подключаемый модуль** выберите вариант **Подключаемый модуль Puppet**.
4. Нажмите кнопку **Далее**.

5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Заполните текстовые поля на вкладке **Сведения** в соответствии с требованиями конечной точки.

Параметр	Описание
Отображаемое имя для данного главного узла Puppet	Имя главного узла Puppet, связанного с подключением конечной точки. Это имя появится в интерфейсе vRealize Orchestrator, чтобы помочь определить конкретное подключение.
Имя узла или IP-адрес	Полное доменное имя или IP-адрес главного узла Puppet, используемого данной конечной точкой.
Порт SSH	Порт, используемый для безопасной связи для данного главного узла Puppet.
Управление доступом на основе ролей (RBAC) и имя пользователя SSH	Имя пользователя при управлении доступом на основе ролей, которое требуется для подключения к главному узлу Puppet.
Пароль для SSH и управления доступом на основе ролей (RBAC)	Имя пользователя при управлении доступом на основе ролей, которое требуется для выполнения безопасной настройки с помощью главного узла Puppet.
Использовать sudo для команд оболочки на этом главном узле?	Установите этот параметр, чтобы администраторы могли использовать команды Sudo на серверах Linux для обеспечения безопасности на виртуальных машинах на базе данной конечной точки.

8. Нажмите кнопку **ОК**.

Результаты

Теперь в схемы элементов vSphere можно добавить компоненты управления конфигурацией Puppet, чтобы иметь возможность развертывать виртуальные машины vSphere с агентами Puppet.

Создание конечной точки Ansible

Создание конечной точки Ansible позволяет добавлять в виртуальные машины vSphere компоненты управления конфигурацией Ansible. Эти компоненты позволяют использовать Ansible Tower для управления конфигурацией на виртуальных машинах.

Необходимые условия

- Установите и настройте Ansible Tower в соответствии с требованиями вашей среды.
- Загрузите и установите подключаемый модуль Ansible в своем развертывании vRealize Orchestrator. Для получения данного подключаемого модуля обратитесь к <https://marketplace.vmware.com/vsx/solutions/sovlabs-ansible-tower-plugin-in-for-vra-cm-framework-1?ref=search>.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.

2. Щелкните значок **Создать**.
3. На вкладке «Подключаемый модуль» в раскрывающемся меню выберите **Подключаемый модуль** и далее выберите «Подключаемый модуль Ansible».
4. Нажмите кнопку **Далее**.
5. На вкладке «Конечная точка» введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Заполните текстовые поля на вкладке «Сведения» в соответствии с требованиями данной конечной точки.

Вкладка «Сведения»	Описание
Конфигурация конечной точки Ansible Tower	<p>Добавьте сведения о конфигурации конечной точки.</p> <ul style="list-style-type: none"> ■ Конфигурация конечной точки Ansible Tower: введите в соответствующих текстовых полях имя, а также IP-адрес или имя узла. ■ Конфигурация учетных данных Ansible Tower: введите учетные данные для входа в экземпляр Ansible Tower, связанный с этой конечной точкой. ■ Импорт сертификата SSL: Выберите, нужно ли, чтобы сертификат Ansible Tower принимался в vRealize Orchestrator без уведомления.
Доступ к узлу Ansible Tower	Если нужно, введите учетные данные SSH для компьютера Ansible Tower, чтобы развернутый компьютер мог подключиться к нему и настроить собственный сценарий динамической иерархии.
Настройка иерархии и организации	Настройте название организации и иерархию. Добавьте параметры конфигурации динамической иерархии.
Фильтры и группы	Настройте фильтры свойств пары значений и динамические группы Ansible.
Запрос на переопределение запуска (не обязательно)	Настройте параметры задания Ansible, а также параметры компьютера, шаблона и иерархии.
Преобразование свойства vRA	При необходимости укажите нужную строку замены, которую после подготовки будет использовать Ansible во время обработки настраиваемых свойств.

8. Щелкните элемент **Готово**.

Создание конечной точки Hyper-V (SCVMM)

Вы можете создавать конечные точки, чтобы разрешить решению vRealize Automation обмениваться данными со средой SCVMM, обнаруживать вычислительные ресурсы, собирать данные и подготавливать компьютеры.

Необходимые условия

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

- Для управления конечной точкой Hyper-V (SCVMM) необходимо установить и настроить агент DEM. Дополнительные сведения см. в разделе требований к SCVMM в статье *Установка vRealize Automation*.

Дополнительные сведения см. в статье [Подготовка среды SCVMM](#).

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Виртуальный > Hyper-V (SCVMM)**.
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. В текстовом поле **Адрес** укажите URL-адрес конечной точки.
URL-адрес должен относиться к типу *Полное доменное имя* или *IP-адрес*.
Например, `mycompany-scvmm1.mycompany.local`.
6. Введите имя и пароль администратора, сохраненные для этой конечной точки.
Если вы до этого не хранили учетные данные, это можно начать делать сейчас.
7. (дополнительно) Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
8. Нажмите кнопку **ОК**.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки OpenStack

Вы можете создать конечную точку, которая позволит vRealize Automation обмениваться данными с вашим экземпляром OpenStack.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Убедитесь в том, что DEM vRealize Automation установлены на компьютере, который соответствует требованиям, предъявляемым OpenStack или PowerVC. См. раздел *Установка vRealize Automation*.
- Убедитесь в том, что ваша версия OpenStack поддерживается в настоящее время. См. раздел *Матрица поддержки vRealize Automation*.

Если после обновления или переноса из версии, предшествующей установке vRealize Automation, не выполняется сбор данных для конечных точек OpenStack, то к каждой конечной точке Keystone V3 OpenStack можно добавить настраиваемое свойство `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name`, чтобы указать допустимое имя домена и включить сбор данных.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.
2. Выберите **Создать > Облако > OpenStack**.
3. Введите имя и, при необходимости, описание.
4. В текстовом поле **Адрес** укажите URL-адрес конечной точки.

Параметр	Описание
PowerVC	URL-адрес нужно ввести в формате <code>http://myPowerVC.com:5000</code> или <code>http://FQDN:5000</code> .
Openstack	URL-адрес нужно ввести в формате <i>Полное доменное имя:5000</i> или <i>IP-адрес:5000</i> . В адрес конечной точки не нужно добавлять суффикс <i>/v2.0</i> .

5. Введите имя пользователя административного уровня и пароль.
Указываемые учетные данные должны быть связаны с правами администратора в арендаторе OpenStack, связанном с конечной точкой.
6. Введите имя арендатора OpenStack в текстовом поле **Проект OpenStack**.
Если вы настроили несколько конечных точек с разными арендаторами OpenStack, создайте политики резервирования для каждого арендатора. Благодаря этому компьютеры будут подготавливаться для соответствующих ресурсов арендатора.
7. Выберите элемент **Свойства** и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения свойств для конечной точки.
Если действует Keystone V3, добавьте настраиваемое свойство `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name` для назначения конкретного домена.
8. Нажмите кнопку **ОК**.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Создание конечной точки Hyper-V, XenServer или пула Xen

Вы можете создавать конечные точки, чтобы позволить решению vRealize Automation обмениваться данными со средой Hyper-V, XenServer или основной средой пула Xen, обнаруживать вычислительные ресурсы, собирать данные и подготавливать компьютеры.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Системный администратор должен установить прокси-агент с сохраненными учетными данными, которые соответствуют вашей конечной точке. См. раздел *Установка vRealize Automation*.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Агенты**.
2. Введите полное DNS-имя сервера Hyper-V, сервера Xen или основного пула Xen в текстовом поле **Вычислительный ресурс**.

Примечание Для конечной точки пула Xen необходимо ввести имя основного пула. Во избежание дублирования записей в таблице вычислительных ресурсов vRealize Automation, укажите адрес, соответствующий настроенному адресу основного пула Xen. Например, если в адресе основного пула Xen используется имя узла, введите имя узла, а не полное доменное имя. Если в адресе основного пула Xen используется полное доменное имя, введите это имя.

3. Выберите прокси-агент, установленный вашим системным администратором для этой конечной точки, в раскрывающемся меню **Имя прокси-агента**.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. Нажмите кнопку **ОК**.

Результаты

В vRealize Automation собираются данные из конечной точки и обнаруживаются вычислительные ресурсы.

Следующие шаги

Добавьте вычислительные ресурсы из конечной точки в группу структур. См. [Создание групп структур](#).

Факторы, которые следует учитывать при проверке подключения

Функцию проверки подключения можно использовать для проверки учетных данных, адреса конечной точки узла, а также сертификата для конечной точки vSphere, NSX for vSphere, NSX-T и vRealize Operations Manager.

Одновременно проверяется рабочее состояние службы диспетчера и агента, которое обеспечивает получение данных из конечной точки.

Команда **Проверить подключение** возвращает следующие возможные результаты проверки.

- Ошибка сертификата

Если сертификат не найден, признан ненадежным или срок его действия истек, отобразится запрос на принятие отпечатка сертификата. Если отпечаток не будет принят, конечную точку можно будет сохранить, но подготовка компьютера может быть не выполнена.

- Ошибка агента

Связанный агент vSphere не найден. Для успешной проверки требуется запущенный агент.

- Ошибка узла

Указанный адрес конечной точки недоступен, или не запущена связанная служба диспетчера. Для успешной проверки требуется запущенная служба диспетчера.

- Ошибка в учетных данных

Обнаружено недопустимое сочетание имени пользователя и пароля для конечной точки с указанным адресом.

- Timeout

Проверка не завершилась в течение отведенного времени (2 минуты).

При получении сообщений об ошибках во время **проверки подключения** на обновленных или перенесенных конечных точках см. действия для установления доверия сертификатов в разделе [Факторы, которые необходимо учитывать при работе с обновленными или перенесенными конечными точками](#).

Программный импорт и экспорт конечных точек

Для программного импорта и экспорта конечных точек в vRealize Automation 7.3 или более поздних версий необходимо использовать новые интерфейсы REST API службы настройки конечных точек vRealize Automation или vRealize CloudClient.

В документации vRealize CloudClient описаны все доступные команды и правила синтаксиса и приведены примеры использования команд.

Приложение vRealize CloudClient и документацию можно загрузить со страницы продукта vRealize CloudClient в <https://developercenter.vmware.com/tool/cloudclient>.

Просмотр вычислительных ресурсов и запуск сбора данных

Можно посмотреть компьютер и вычислительный ресурс, связанные с той или иной конечной точкой. Также можно вручную запустить сбор данных.

Необходимые условия

Удостоверьтесь, что имеется как минимум одна конечная точка.

Процедура

1. Выберите **Инфраструктура > Конечные точки > Конечные точки**.

Пользователи, у которых нет прав администратора инфраструктуры как услуги, могут перейти в раздел **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**, чтобы просмотреть ресурсы и запустить сбор данных из вычислительного ресурса.

2. Выберите **Инфраструктура > Конечные точки > Конечные точки**.

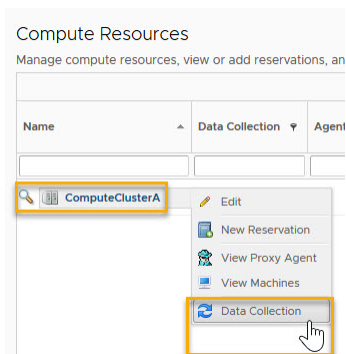
3. Выберите строку с существующей конечной точкой и щелкните **Действия**.

Выберите одно из следующих доступных действий.

- Щелкните **Просмотреть вычислительные ресурсы**, чтобы открыть страницу **Инфраструктура > Вычислительный ресурс**. На этой странице можно просмотреть и изменить параметры вычислительного ресурса. Кроме того, можно запустить сбор данных для выбранного вычислительного ресурса на странице **Вычислительные ресурсы**.
- Щелкните **Просмотреть компьютеры**, чтобы открыть страницу **Инфраструктура > Управляемые компьютеры**.
- Щелкните **Сбор данных**, чтобы открыть страницу сбора данных и запустить процесс сбора данных конечной точки. Для отображения текущего состояния запроса можно обновить страницу.

Сбор данных можно запустить из связанного с конечной точкой вычислительного ресурса.

Например, чтобы собрать данные о существующей конечной точке NSX-T, перейдите в раздел **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**, чтобы просмотреть ресурсы, а затем выберите **Сбор данных**, чтобы открыть страницу **Сбор данных** для конкретного вычислительного ресурса. Найдите в списке нужную конечную точку и нажмите **Запросить**.



Факторы, которые необходимо учитывать при работе с обновленными или перенесенными конечными точками

После обновления или переноса с более ранних версий до версии vRealize Automation 7.3 необходимо учитывать следующие важные моменты и принимать соответствующие меры.

Данная информация относится к конечным точкам, которые были обновлены или перенесены в эту версию vRealize Automation.

- При обновлении или переносе из версии, предшествующей версии vRealize Automation 7.3, каждая конечная точка vCloud Air, vCloud Director и Amazon, содержащая параметры прокси-сервера, обновляется с привязкой к новой конечной точке прокси-сервера, которая содержит его собственные параметры.

После обновления или переноса имя конечной точки прокси-сервера имеет вид Proxy_YYYYYY, где YYYYYY — хэш URL-адреса, порта и учетных данных прокси-сервера. Если использовались те же самые параметры прокси-сервера (например, те же URL-адрес, порт и учетные данные) для другой конечной точки (например, конечной точки vCloud Air или Amazon), то после обновления или переноса останется только одна конечная точка прокси-сервера и связь между конечной точкой vCloud Air или Amazon и новой конечной точкой прокси-сервера. Конечная точка прокси-сервера может быть связана с несколькими конечными точками Amazon, vCloud Air или vCloud Director.

- Когда выполняется обновление или перенос конечных точек vSphere, содержащих параметры NSX Manager, каждая обновленная конечная точка vSphere связывается с новой конечной точкой NSX, которая содержит собственные параметры NSX Manager.

После обновления или переноса имя конечной точки NSX имеет вид NSX_XXXXXX, где XXXXXX — имя родительской конечной точки vSphere в версии, предшествующей версии vRealize Automation 7.3.

- После завершения обновления или переноса vRealize Automation администратор инфраструктуры может изменить имена новой конечной точки NSX и конечной точки прокси-сервера.
- После обновления или переноса для конечных точек по умолчанию используется параметр безопасности, предполагающий запрет на использование сертификатов, не являющихся доверенными.
- После обновления или переноса из версии, предшествующей установке vRealize Automation, необходимо выполнить следующие действия для всех конечных точек vSphere и NSX, чтобы включить проверку сертификатов, если использовались сертификаты, не являющиеся доверенными. В противном случае в работе конечной точки возникают ошибки сертификатов. Дополнительные сведения см. в статьях базы знаний VMware: *Разрыв соединения с конечной точкой после обновления до vRA 7.3 (2150230)* (<http://kb.vmware.com/kb/2150230>) и *Загрузка и установка корневых сертификатов vCenter Server во избежание предупреждений о сертификате в веб-браузерах (2108294)* (<http://kb.vmware.com/kb/2108294>).

- а) После обновления или переноса выполните вход на компьютер агента vRealize Automation vSphere и перезапустите агенты vSphere на вкладке **Службы**.

При переносе могут перезапуститься не все агенты, и при необходимости их потребуется перезапустить вручную.

- б) Дождитесь завершения создания хотя бы одного отчета о проверке связи. Создание отчета о проверке связи занимает 1–2 минуты.
- в) Когда агенты vSphere начнут сбор данных, выполните вход в vRealize Automation с учетными данными администратора инфраструктуры как услуги.
- г) Выберите **Инфраструктура > Конечные точки > Конечные точки**.
- д) Измените конечную точку vSphere и нажмите **Проверить подключение**.
- е) Если отображается запрос на принятие сертификата, нажмите **ОК**, чтобы принять сертификат.

Если запрос на принятие сертификата не отображился, сертификат может в настоящее время храниться в доверенном корневом каталоге службы размещения для конечной точки на компьютере под управлением ОС Windows (например, компьютер агента прокси-сервера или компьютер DEM).

- ж) Нажмите **ОК**, чтобы принять сертификат и сохранить конечную точку.
- з) Выполните эту процедуру для каждой из конечных точек vSphere.
- и) Выполните эту процедуру для каждой из конечных точек NSX.
- к) Перейдите в раздел **Инфраструктура > Вычислительные ресурсы**, щелкните правой кнопкой мыши ресурс **Вычисления vCenter** и выполните команду **Сбор данных**.

Если действие **Проверить подключение** выполнено успешно, но при этом не удалось выполнить отдельные операции сбора данных или подготовки, можно установить тот же сертификат на все компьютеры агента, которые обслуживают конечную точку, и на все компьютеры DEM. Можно также удалить сертификат с существующих компьютеров и выполнить указанную выше процедуру повторно для той конечной точки, в работе которой возникли проблемы.

- API-интерфейсы REST vRealize Automation, которые использовались для программного создания, редактирования и удаления конечных точек в версии vRealize Automation 7.2 и более ранних версиях, больше не поддерживаются в версии vRealize Automation 7.3 и более поздних версиях. Чтобы программно создать, отредактировать или удалить конечные точки в версии vRealize Automation 7.3 и более поздних версиях, необходимо использовать API-интерфейсы REST новой службы конфигурации конечных точек vRealize Automation или vRealize CloudClient.
- Если после обновления или переноса из версии, предшествующей установке vRealize Automation, не выполняется сбор данных для конечных точек OpenStack, то к каждой конечной точке Keystone V3 OpenStack можно добавить настраиваемое свойство `VMware.Endpoint.Openstack.IdentityProvider.Domain.Name`, чтобы указать допустимое имя домена и включить сбор данных.
- Когда обновляется конечная точка стороннего поставщика решений для управления IP-адресами (например, Infoblox), то выполняется обновление пакета vRealize Orchestrator, содержащего рабочий процесс `RegisterIPAMEndpoint`. Может потребоваться перезапуск рабочего процесса в vRealize Orchestrator по завершении обновления vRealize Automation.
- Чтобы изменить учетные данные для нескольких конечных точек, можно либо изменить конечные точки по отдельности, либо выполнить групповое обновление с помощью vRealize CloudClient.
- Некоторые типы конечных точек (например, vCloud Air и vCloud Director) нельзя обновить или перенести непосредственно из версии vRealize Automation 6.2.x в версию vRealize Automation 7.3 или более поздние версии.
- Если после успешного обновления или переноса в версию vRealize Automation 7.3 на странице **Инфраструктура > Конечные точки** не отображаются конечные точки или отображаются только некоторые типы конечных точек, см. временное решение в [статье базы знаний 2150252](#).

Факторы, которые необходимо учитывать при удалении конечных точек

При определенных условиях можно удалять конечные точки определенных типов.

- Можно удалить конечные точки, не включенные в сбор данных.
- Можно удалить конечные точки OpenStack, Amazon и VRO, если они включены в сбор данных, но не имеют резервирований. Другие типы конечных точек нельзя удалить, если они включены в сбор данных.
- Можно удалить стороннюю конечную точку управления IP-адресами, если она не связана с сетевым профилем.
- При удалении конечной точки vSphere в запросе подтверждения отображаются следующие зависимости:
 - Конечная точка включена в сбор данных.
 - На данную конечную точку имеется ссылка в резервировании, которое сопоставляется с вычислительным ресурсом. Нельзя удалить конечную точку, если на нее есть ссылка в резервировании. Для резервирований требуется вычислительный ресурс.
 - Конечная точка содержит шаблон, на который имеется ссылка в существующей схеме элементов. Схема элементов не удаляется при удалении конечной точки.
 - Конечная точка используется виртуальной машиной, которая в данный момент работает.
- Можно удалить конечные точки программным путем, используя новые интерфейсы REST API CREATE, EDIT и DELETE службы настройки конечных точек vRealize Automation, которые появились в vRealize Automation 7.3, либо с помощью vRealize CloudClient. Нельзя удалить конечные точки с помощью интерфейсов REST API службы настройки конечных точек vRealize Automation версии до 7.3.

Устранение ошибки «Не удалось найти подключенную конечную точку vSphere»

Причиной сбоя в ходе сбора данных конечной точки vSphere может быть несоответствие имен прокси-сервера и конечной точки.

Проблема

Произошел сбой сбора данных конечной точки vSphere. Журнал возвращает сообщение об ошибке, аналогичное следующему:

Перехвачено внешнее исключение: присоединенная конечная точка vCenter не найдена.

Причина

Заданное имя конечной точки в vRealize Automation должно соответствовать имени, указанному для прокси-агента vSphere во время установки. Сбой сбора данных конечной точки vSphere происходит только при несоответствии имени конечной точки и прокси-агента. До тех пор, пока не будет настроена конечная точка с соответствующим именем, журнал будет возвращать сообщения об ошибке, аналогичные следующему:

Перехвачено внешнее исключение: присоединенная конечная точка *имя_конечной_точки* не найдена.

Решение

1. Выберите **Инфраструктура > Мониторинг > Журнал**.
2. Найдите сообщение об ошибке Присоединенная конечная точка не найдена.

Пример:

Перехвачено внешнее исключение: присоединенная конечная точка *имя_конечной_точки* не найдена.

3. Измените конечную точку vSphere так, чтобы она соответствовала необходимой конечной точке, показанной в сообщении журнала.
 - а) Выберите **Инфраструктура > Конечные точки > Конечные точки**.
 - б) Щелкните имя конечной точки, чтобы ее редактировать.
 - в) В текстовом поле **Имя** введите имя необходимой конечной точки.
 - г) Нажмите кнопку **ОК**.

Решение

Теперь прокси-агент может взаимодействовать с конечной точкой, и сбор данных выполняется успешно.

Создание групп структур

Ресурсы инфраструктуры можно объединить в группы структур, а затем назначить им одного или нескольких администраторов структуры для управления ресурсами в этих группах.

Группы структур необходимы для виртуальных и облачных конечных точек. Роль администратора структуры можно назначить нескольким пользователям. Пользователей можно добавить по очереди либо в составе группы хранилищ удостоверений или пользовательской группы в качестве администратора структуры.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора инфраструктуры как услуги**.
- Создайте по меньшей мере одну конечную точку. См. раздел [Выбор сценария конечной точки](#).

Процедура

1. Выберите **Инфраструктура > Конечные точки > Группы структур**.

2. Выберите значок **Создать** (+).
3. В текстовом поле **Имя** введите имя.
4. (дополнительно) В текстовом поле **Описание** введите описание.
5. Введите имя пользователя или адрес электронной почты пользователя в текстовом поле **Администраторы структуры**, щелкните значок «Поиск» и выберите адрес электронной почты указанного пользователя.

Повторите этот шаг, чтобы добавить несколько пользователей.

6. Выберите один или несколько **вычислительных ресурсов**, чтобы включить их в свою группу структур.

Во время сбора данных обнаруживаются только ресурсы, которые существуют в кластерах, выбранных для группы структур. Например, будут обнаружены только шаблоны, которые существуют в выбранных кластерах, и только они будут доступны для клонирования в резервированиях, созданных для бизнес-групп.

7. Нажмите кнопку **ОК**.

Результаты

Теперь администраторы структуры могут настроить префиксы компьютеров. См. раздел [Настройка префиксов компьютеров](#).

Пользователи, вошедшие в службу vRealize Automation, должны выйти и войти обратно в vRealize Automation, прежде чем переходить на страницы, к которым они получили доступ.

Настройка префиксов компьютеров

Можно создать префиксы компьютеров, используемые для создания имен компьютеров, подготовленных с помощью vRealize Automation. Префикс компьютера требуется при определении компонента компьютера на холсте проекта схемы элементов.

Префикс — это базовое имя, за которым должен следовать счетчик, включающий в себя заданное количество цифр. Когда будут использованы все цифры, vRealize Automation вернется к первому числу.

Префиксы компьютеров должны соответствовать следующим ограничениям:

- Должны содержать только буквы ASCII от а до z в любом регистре, цифры от 0 до 9 и дефисы (-).
- Не должны начинаться с дефиса.
- Другие символы, знаки пунктуации и пробелы использовать нельзя.
- Должны содержать не более 15 символов, в том числе цифр (15 — это максимально допустимое число символов в именах узлов в Windows).

Более длинные имена узлов усекаются при подготовке компьютера и обновляются при следующем сборе данных. Тем не менее, при подготовке WIM имена не усекаются, поэтому, когда указанное имя длиннее 15 символов, подготовку выполнить не удастся.

- vRealize Automation не поддерживает несколько виртуальных машин с одинаковыми именами в одном экземпляре. Если выбрано соглашение об именах, которое вызывает перекрытие имен компьютеров, vRealize Automation не подготавливает компьютер с избыточным именем. Если возможно, vRealize Automation пропускает имя, которое уже используется, и создает новое имя компьютера, используя для него определенный префикс. Если не удастся создать уникальное имя, выполнить подготовку не удастся.

Необходимые условия

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

Процедура

1. Щелкните **Инфраструктура > Администрирование > Префикс компьютера**
2. Выберите значок **Создать** (+).
3. В текстовом поле **Имя** введите префикс компьютера.
4. Укажите, должен ли префикс компьютера отображаться в столбце **Видимость** во всех арендаторах или только в текущем арендаторе.
5. Введите количество разрядов префикса компьютера в текстовом поле **Количество разрядов**.
6. Введите начальное значение счетчика в текстовом поле **Следующий номер**.
7. Щелкните значок **Сохранить** (✓).

Результаты

Администраторы арендатора могут создавать бизнес-группы, чтобы пользователи могли получить доступ к vRealize Automation для запроса компьютеров.

Создание профиля сети в vRealize Automation

Профиль сети содержит информацию об IP, такую как шлюз, подсеть и диапазон адресов. В соответствии с параметрами профиля сети vRealize Automation использует DHCP vSphere или указанного поставщика управления IP-адресами для назначения IP-адресов подготавливаемым компьютерам.

Для определения типа доступной сети можно создать профиль сети. Можно создать профили внешней сети и шаблоны для преобразования сетевых адресов (NAT) по требованию, а также профили маршрутизируемой или частной сети. Эти профили могут создать логические коммутаторы NSX и соответствующие параметры маршрутизации для сетевого пути.

Профили сетей используются для настройки параметров сети при подготовке компьютеров. В профилях сетей также указывается конфигурация устройств NSX Edge, создаваемых при подготовке компьютеров.

Доступные типы сетей

При определении профиля сети доступны следующие типы сетей:

- Существующая сеть
- Маршрутизируемая сеть по требованию

- Сеть NAT по требованию
- Частная сеть по требованию (только NSX for vSphere)

Таблица 2-14. Доступные типы сетей для профиля сети vRealize Automation

Тип сети	Описание
Внешнее	<p>Существующая сеть, настроенная на сервере vSphere. Они являются внешней частью сетей NAT и маршрутизируемых сетей. Профиль внешней сети может задать диапазон статических IP-адресов, доступных во внешней сети.</p> <p>Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.</p> <p>Профиль внешней сети с диапазоном статических IP-адресов является необходимым условием для сетей NAT и маршрутизируемых сетей.</p> <p>См. раздел Создание профиля внешней сети для существующей сети.</p>
NAT	<p>Во время подготовки создана сеть по требованию. Сети NAT, в которых один набор IP-адресов используется для внешнего обмена данными, а другой набор — для внутреннего.</p> <p>В сетях NAT «один к одному» каждой виртуальной машине назначается внешний IP-адрес из профиля внешней сети и внутренний IP-адрес из профиля сети NAT. В сетях NAT «один ко многим» для всех компьютеров задан один IP-адрес из профиля внешней сети для внешнего обмена данными.</p> <p>Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.</p> <p>Профиль сети NAT задает локальные и внешние сети, в которых для взаимного обмена данными используются таблицы преобразования.</p> <p>См. раздел Создание профиля сети NAT для сети по требованию.</p>
Маршрутизируемая	<p>Во время подготовки создана сеть по требованию. Маршрутизируемые сети содержат маршрутизируемое пространство IP-адресов, разделенное по подсетям, которые связаны друг с другом с помощью распределенного логического маршрутизатора (Distributed Logical Router, DLR).</p> <p>Каждой новой маршрутизируемой сети назначается следующая доступная подсеть. Она также связывается с другими маршрутизируемыми сетями, которые используют тот же самый профиль сети. Виртуальные машины, подготовленные с помощью маршрутизируемых сетей, имеющих один и тот же профиль сети, могут обмениваться данными между собой и с внешней сетью.</p> <p>Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.</p> <p>Профиль маршрутизируемой сети задает маршрутизируемое пространство и доступные подсети.</p> <p>См. раздел Создание профиля маршрутизируемой сети для сети по требованию.</p>
Частная (только NSX for vSphere)	<p>Во время подготовки создана сеть по требованию. Этот параметр доступен только для NSX for vSphere. Этот параметр недоступен для NSX-T.</p> <p>Для частных сетей характерны следующие моменты.</p> <ul style="list-style-type: none"> ■ В частных сетях отсутствуют входящие или исходящие подключения. Для частных сетей не подготавливается Edge. ■ Можно создать профиль частной сети с наличием или отсутствием статических IP-адресов или диапазонов. DHCP и стороннее управление IP-адресами не поддерживаются для частных сетей. <p>См. раздел Создание профиля частной сети для сети по требованию в vRealize Automation.</p>

Дополнительные сведения о сетях NSX см. в [документации по VMware NSX Data Center for vSphere](#) и [документации по VMware NSX-T Data Center](#).

Дополнительные сведения о настройке сети и безопасности для NSX-T в vRealize Automation см. в статье блога VMware [Application Networking and Security with vRealize Automation and NSX-T](#).

Использование имеющегося или стороннего поставщика управления IP-адресами

В профилях сетей также поддерживаются сторонние поставщики управления IP-адресами (IPAM), например Infoblox. При настройке профиля сети для управления IP-адресами подготовленные компьютеры могут получать данные о своих IP-адресах и связанную информацию, такую как DNS и шлюз, от настроенного решения по управлению IP-адресами. Чтобы сторонний поставщик управления IP-адресами (например, Infoblox) определял конечную точку управления IP-адресами, используемую с профилем сети, можно использовать внешний пакет по управлению IP-адресами.

Примечание Если используется сторонний поставщик управления IP-адресами и нужно указать сеть для развертывания компьютера, используйте отдельный профиль сети для каждой сети VLAN. Это позволит избежать известной проблемы, описанной в [статье базы знаний 2148656](#).

Если вместо конечной точки стороннего поставщика управления IP-адресами используется конечная точка управления IP-адресами от vRealize Automation, можно указать диапазоны IP-адресов, которые можно будет использовать профилям сети. Когда компьютер уничтожается, каждый IP-адрес в указанных диапазонах, назначаемых компьютеру, может быть реорганизован для переназначения. Можно создать профиль сети для определения диапазона статических IP-адресов, которые можно назначить компьютерам. При подготовке виртуальных машин путем клонирования или использования подготовки Kickstart или autoYaST владелец запрашивающего компьютера может назначить статические IP-адреса из предварительно заданного диапазона.

Указание профиля сети в резервировании или схеме элементов

Профиль сети указывается при создании резервирования и схем элементов. При резервировании можно назначить профиль сети для сетевого пути и указать любой из путей для компонента компьютера в схеме элементов. Профиль сети можно назначить определенному сетевому пути резервирования. Для некоторых типов компонентов компьютера, таких как vSphere, можно назначить профиль сети при создании или изменении схемы элементов.

При определении сетевых адаптеров и подсистем балансировки нагрузки для компьютера vSphere можно использовать существующий профиль сети и профиль сети по требованию.

Если профиль сети указан в резервировании и схеме элементов, то значения в схеме элементов имеет более высокий приоритет.

Внесение изменений после развертывания схемы элементов

Нельзя изменить профиль сети развернутой виртуальной машины, но можно изменить сеть, к которой подключена ВМ. Если сеть связана с другим профилем сети, vRealize Automation назначает виртуальной машине IP-адрес из этого профиля. ВМ продолжит использовать старый IP-адрес до тех пор, пока не будет обновлен IP-адрес в гостевой операционной системе. Если в развернутой ВМ используется действие «Перенастроить», необходимо обновить IP-адрес в гостевой операционной системе.

Использование профилей сети для управления диапазонами IP-адресов

Виртуальным машинам, подготовленным путем клонирования или с помощью Linux Kickstart или AutoYaST, а также облачным компьютерам, подготовленным в OpenStack с помощью Kickstart, с использованием профилей сети можно назначить статические IP-адреса в рамках предварительно определенного диапазона.

Для назначения IP-адресов подготовленным компьютерам vRealize Automation по умолчанию использует протокол DHCP.

Вы можете создать профили сетей, чтобы определить диапазон статических IP-адресов, которые можно назначить компьютерам. Определенным сетевым путям резервирования можно назначить профили сетей. Компьютеры, подготовленные путем клонирования либо с помощью Kickstart или AutoYaST и подключенные к сетевому пути с соответствующим профилем сети, подготавливаются с помощью назначенного статического IP-адреса. Для подготовки с использованием назначения статического IP-адреса необходимо использовать спецификацию настройки.

Можно назначить профиль сети компоненту компьютера vSphere в схеме элементов путем добавления существующего компонента сети «NAT по требованию» или «Маршрутизируемая сеть по требованию» на холст проекта и выбора профиля сети, к которому будет присоединен компонент компьютера vSphere. Также можно назначить профили сетей схемам элементов с помощью настраиваемого свойства `VirtualMachine.NetworkN.ProfileName`, где *N* — идентификатор сети.

Дополнительно можно использовать предоставляемую конечную точку управления IP-адресами vRealize Automation или зарегистрированную и настроенную стороннюю конечную точку поставщика службы управления IP-адресами в своем профиле сети, чтобы получить и настроить IP-адреса. Сведения о требованиях к внешнему управлению IP-адресами см. в разделе [Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами](#).

При выборе конечной точки стороннего поставщика управления IP-адресами в профиле сети vRealize Automation получает диапазоны IP-адресов из конечной точки зарегистрированного внешнего поставщика управления IP-адресами, например Infoblox. Далее с этой конечной точки выделяются значения IP-адресов. Заданная маска подсети диапазона используется для выделения подсетей из блока IP-адресов.

Если профиль сети указан в резервировании и схеме элементов, то значения в схеме элементов имеет более высокий приоритет.

Общие сведения о формате CSV для импорта IP-адресов профиля сети

Можно импортировать диапазоны IP-адресов в профиль сети vRealize Automation с помощью правильно отформатированного CSV-файла.

Записи CSV-файла должны придерживаться следующего формата.

Поле в CSV-файле	Описание
<code>ip_address</code>	IP-адрес в формате IPv4.
<code>machine_name</code>	Имя управляемой машины в vRealize Automation. Если поле пустое, то имя по умолчанию отсутствует. Если поле пустое, для поля <code>status</code> не может устанавливаться значение «Выделен».

Поле в CSV-файле	Описание
status	Доступны значения Allocated или Unallocated. В этом поле учитывается регистр. Если поле пустое, по умолчанию устанавливается значение «Не выделен». Если установлено состояние «Выделен», поле machine_name не может быть пустым.
NIC_offset	Неотрицательное целое число. Смещение сетевого адаптера указывает, какому сетевому адаптеру виртуальной машины назначен данный IP-адрес. Если виртуальная машина выделяет несколько IP-адресов для разных сетевых адаптеров, то для каждого сетевого адаптера, который содержит соответствующее смещение, создается отдельная запись IP-адреса. Значение 0 указывает на отсутствие смещения.

В следующем примере записи показан IP-адрес компьютера 100.10.100.1, имя компьютера mymachine01, состояние «Выделен» (Allocated) и «Без смещения сетевого адаптера» (No NIC Offset).

```
100.10.100.1,mymachine01,Unallocated,0
```

Сценарий: импорт IP-адресов в профиль сети из CSV-файла

Можно добавить IP-адреса в диапазон профиля сети путем импорта правильно отформатированного CSV-файла. Можно также изменить адреса в диапазоне профиля сети путем редактирования диапазона в vRealize Automation или импорта измененного или другого CSV-файла.

Можно добавить или изменить IP-адреса в диапазоне профиля сети путем импорта из CSV-файла или ввода значений вручную. Кроме того, можно разрешить стороннему поставщику управления IP-адресами предоставлять IP-адреса.

- Импортируйте первоначальный диапазон IP-адресов в профиль сети vRealize Automation.
- Создайте первый именованный диапазон в профиле сети на основе импортированных значений.
- Удалите один или несколько IP-адресов из диапазона сети vRealize Automation.
- Импортируйте измененный или другой CSV-файл, чтобы посмотреть, как изменятся значения диапазона сети.

Для профилей сети, которые используют стороннюю конечную точку управления IP-адресами, нельзя применять функцию **Импортировать из CSV**, так как управление IP-адресами осуществляется сторонним поставщиком управления IP-адресами, а не с помощью vRealize Automation.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте CSV-файл, содержащий IP-адреса для импорта в диапазон сети. См. [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#) и [Общие сведения о формате CSV для импорта IP-адресов профиля сети](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите тип профиля сети в раскрывающемся меню.
В этом примере выберите значение *Внешний*.
3. Введите значение **Профиль сети из CSV** в текстовом поле **Имя**.

4. Введите значение **Проверка IP-адресов диапазона сети с помощью CSV** в текстовом поле **Описание**.

Параметр импорта CSV-файла применяется к настройкам на страницах вкладок **Диапазоны сети** и **IP-адреса**.

5. (дополнительно) Выберите настроенную конечную точку управления IP-адресами, если она доступна. Если нет, пропустите этот шаг.
6. Введите соответствующее значение IP-адреса в текстовые поля **Маска подсети** и **Шлюз**.
7. Выберите вкладку **DNS**.
8. Введите применимую информацию, например суффикс DNS, и перейдите на вкладку **Диапазоны сети**.
Параметр **Импортировать из CSV** доступен при переходе на вкладку **Диапазоны сети**.
9. Чтобы указать новое имя диапазона сети и диапазон IP-адресов вручную, нажмите **Создать**, или выберите **Импортировать из CSV**, чтобы импортировать сведения об IP-адресе из должным образом отформатированного CSV-файла.

■ Нажмите кнопку **Создать**.

- а) Введите имя диапазона сети.
- б) Введите описание диапазона сети.
- в) Введите начальный IP-адрес диапазона.
- г) Введите конечный IP-адрес диапазона.

■ Щелкните **Импортировать из CSV**.

- а) Найдите и выберите CSV-файл или перетащите его в диалоговое окно **Импортировать из CSV**.

Строка в CSV-файле имеет следующий формат *ip_address, machine_name, status, NIC offset*. Пример:

```
100.10.100.1,mymachine01,Allocated,0
```

Поле в CSV-файле	Описание
ip_address	IP-адрес в формате IPv4.
machine_name	Имя управляемой машины в vRealize Automation. Если поле пустое, то имя по умолчанию отсутствует. Если поле пустое, для поля <i>status</i> не может устанавливаться значение «Выделен».

Поле в CSV-файле	Описание
status	Доступны значения Allocated или Unallocated. В этом поле учитывается регистр. Если поле пустое, по умолчанию устанавливается значение «Не выделен». Если установлено состояние «Выделен», поле machine_name не может быть пустым.
NIC_offset	Неотрицательное целое число. Смещение сетевого адаптера указывает, какому сетевому адаптеру виртуальной машины назначен данный IP-адрес. Если виртуальная машина выделяет несколько IP-адресов для разных сетевых адаптеров, то для каждого сетевого адаптера, который содержит соответствующее смещение, создается отдельная запись IP-адреса. Значение 0 указывает на отсутствие смещения.

б) Нажмите кнопку **Применить**.

10. Нажмите кнопку **ОК**.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

11. Чтобы отобразить данные IP-адреса для указанного адресного пространства диапазона, перейдите на вкладку **IP-адреса**.

Если информация об IP-адресе импортирована из CSV-файла, имя диапазона будет означать *Импортировано из CSV*.

12. (дополнительно) Чтобы отфильтровать записи IP-адресов, выберите IP-адрес в раскрывающемся меню **Диапазон сети**.

Можно отобразить информацию обо всех определенных диапазонах сети, диапазонах сети, импортированных из CSV-файла, или именованных диапазонах сети.

Следующие шаги

При повторном импорте IP-адресов из CSV-файла предыдущие IP-адреса заменяются информацией из импортируемого файла.

Создание профиля внешней сети для существующей сети

Профили внешней сети можно создавать, чтобы задавать параметры сети с целью настройки существующих сетей для подготовки компьютеров, в том числе настройки устройств NSX Edge, которые будут использоваться при подготовке.

Можно использовать указанную конечную точку поставщика управления IP-адресами vRealize Automation или конечную точку управления IP-адресами от стороннего поставщика, например Infoblox, зарегистрированную в vRealize Orchestrator.

Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами

Можно создать профиль внешней сети, чтобы задать свойства сети и диапазон статических IP-адресов, которые нужно использовать при подготовке компьютеров в существующей сети.

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Информацию о создании профиля внешней сети и использовании конечной точки внешнего поставщика управления IP-адресами см. в разделе [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#).

Процедура

1. Указание профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами

Профиль внешней сети определяет свойства и параметры внешней сети. Профиль внешней сети — это требование профилей NAT и профилей маршрутизируемой сети.

2. Настройка диапазонов IP-адресов профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Следующие шаги

Вы можете назначить профиль сети сетевому пути в резервировании, или архитектор схемы элементов может задать профиль сети в схеме элементов. Профиль внешней сети можно использовать при создании профиля сети NAT или маршрутизируемой сети по требованию.

Указание профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами

Профиль внешней сети определяет свойства и параметры внешней сети. Профиль внешней сети — это требование профилей NAT и профилей маршрутизируемой сети.

Информацию о том, как создать профиль внешней сети путем получения информации об управлении IP-адресами из конечной точки зарегистрированного стороннего поставщика управления IP-адресами, такого как Infoblox, см. в разделах [Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами](#) и [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#). Используйте следующую процедуру для создания профиля сети с помощью внутренней конечной точки управления IP-адресами VMware.

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **Внешняя** в раскрывающемся меню.

3. Введите имя и, при необходимости, описание.
4. Примите значение параметра **Конечная точка управления IP-адресами** по умолчанию для предоставленной конечной точки **Управление IP-адресами vRealize Automation**
5. В текстовом поле **Маска подсети** введите маску подсети IP-адреса.

Маска подсети определяет размер всего маршрутизируемого адресного пространства, которое нужно будет задать для профиля сети.

Например, 255.255.0.0.

6. В поле **Шлюз** введите адрес маршрутизируемого шлюза, например 10.10.110.1.

Заданный в профиле сети IP-адрес шлюза назначается сетевому адаптеру во время выделения. Шлюз требуется для сетевых профилей NAT.

Для NSX-T шлюз DHCP-сервера по умолчанию соответствует шлюзу NAT «один ко многим» по умолчанию. Шлюз пула IP-адресов по умолчанию соответствует шлюзу для сети NAT «один ко многим» по умолчанию в vRealize Automation.

Если в текстовом поле **Шлюз** профиля сети не задано значение, для указания шлюза используйте настраиваемое свойство `VirtualMachine.Network0.Gateway`.

7. Выберите вкладку **DNS**.
8. При необходимости введите значения DNS и WINS.

Используйте значения DNS для регистрации имени и разрешения. Эти значения не являются обязательными для внутреннего управления IP-адресами. Они предоставляются сторонним поставщиком управления IP-адресами для внешнего управления IP-адресами.

- а) (дополнительно) Введите значение в поле **Основной сервер DNS**.
- б) (дополнительно) Введите значение в поле **Дополнительный сервер DNS**.
- в) (дополнительно) Введите значение в поле **Суффиксы DNS**.
- г) (дополнительно) Введите значение в поле **Суффиксы поиска DNS**.
- д) (дополнительно) Введите значение в поле **Предпочитаемая служба WINS**.
- е) (дополнительно) Введите значение в поле **Альтернативная служба WINS**.

Следующие шаги

Вы можете настраивать IP-диапазоны для статических IP-адресов. См. раздел [Настройка диапазонов IP-адресов профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами](#).

Настройка диапазонов IP-адресов профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Вы можете задать значения диапазона IP-адресов вручную из импортированного файла CSV или с помощью IP-адресов, указанных внешним поставщиком управления IP-адресами. Можно объединить определенные вручную диапазоны IP-адресов и IP-адреса, импортированные с помощью CSV-файла. Например, одни диапазоны можно определить с помощью пользовательского интерфейса, а другие путем импорта из CSV-файла.

При импорте из CSV-файла во второй раз, независимо от имени этого файла, будут удалены диапазоны IP-адресов, импортированные из предыдущего CSV-файла, и добавлен новый диапазон IP-адресов. Таким образом, предыдущая импортированная информация перезаписывается при последующем импорте. Процесс обновления CSV-файла и его повторного импорта в профиль сети можно повторять любое количество раз.

Если в профиле внешней сети не указаны диапазоны IP-адресов, с его помощью можно указать, какая сеть выбирается для виртуального сетевого адаптера. Если вы хотите использовать профиль существующей сети в профиле маршрутизированной сети или сети NAT, он должен содержать по меньшей мере один диапазон статических IP-адресов.

Необходимые условия

[Указание профиля внешней сети с использованием предоставленной конечной точки управления IP-адресами.](#)

Процедура

1. Откройте вкладку **Диапазоны сети**.
2. Чтобы указать новое имя диапазона сети и диапазон IP-адресов вручную, нажмите **Создать**, или выберите **Импортировать из CSV**, чтобы импортировать сведения об IP-адресе из должным образом отформатированного CSV-файла.
 - Нажмите кнопку **Создать**.
 - а) Введите имя диапазона сети.
 - б) Введите описание диапазона сети.
 - в) Введите начальный IP-адрес диапазона.
 - г) Введите конечный IP-адрес диапазона.
 - Щелкните **Импортировать из CSV**.
 - а) Найдите и выберите CSV-файл или перетащите его в диалоговое окно **Импортировать из CSV**.

Строка в CSV-файле имеет следующий формат *ip_address, machine_name, status, NIC offset*. Пример:

```
100.10.100.1,mymachine01,Allocated,0
```

Поле в CSV-файле	Описание
ip_address	IP-адрес в формате IPv4.
machine_name	Имя управляемой машины в vRealize Automation. Если поле пустое, то имя по умолчанию отсутствует. Если поле пустое, для поля status не может устанавливаться значение «Выделен».
status	Доступны значения Allocated или Unallocated. В этом поле учитывается регистр. Если поле пустое, по умолчанию устанавливается значение «Не выделен». Если установлено состояние «Выделен», поле machine_name не может быть пустым.
NIC_offset	Неотрицательное целое число. Смещение сетевого адаптера указывает, какому сетевому адаптеру виртуальной машины назначен данный IP-адрес. Если виртуальная машина выделяет несколько IP-адресов для разных сетевых адаптеров, то для каждого сетевого адаптера, который содержит соответствующее смещение, создается отдельная запись IP-адреса. Значение 0 указывает на отсутствие смещения.

б) Нажмите кнопку **Применить**.

3. Нажмите кнопку ОК.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

4. Чтобы отобразить данные IP-адреса для указанного адресного пространства диапазона, перейдите на вкладку IP-адреса.

Если информация об IP-адресе импортирована из CSV-файла, имя диапазона будет означать *Импортировано из CSV*.

5. (дополнительно) Чтобы отфильтровать записи IP-адресов, выберите IP-адрес в раскрывающемся меню Диапазон сети.

Можно отобразить информацию обо всех определенных диапазонах сети, диапазонах сети, импортированных из CSV-файла, или именованных диапазонах сети.

6. (дополнительно) Чтобы отфильтровать IP-адреса по состоянию, выберите тип состояния в раскрывающемся меню Состояние IP-адреса.

Для IP-адресов с состоянием «Удален» (Destroyed) или «Просрочен» (Expired) можно щелкнуть **Реорганизовать**, чтобы сделать эти диапазоны IP-адресов доступными для выделения. Необходимо сохранить профиль, чтобы реорганизация вступила в силу. Обновление столбца «Состояние» (Status) с Expired или Destroyed на Allocated может занять до 1 минуты.

7. Чтобы завершить настройку профиля сети, нажмите ОК.

Результаты

Вы можете назначить профиль сети сетевому пути в резервировании, или архитектор схемы элементов может задать профиль сети в схеме элементов. Если вы создали профиль внешней сети, то можете использовать его при создании профиля сети NAT или маршрутизируемой сети.

Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами

Используя решение стороннего поставщика управления IP-адресами, которое импортировано, настроено и зарегистрировано в vRealize Orchestrator, можно получить IP-адреса у этого стороннего поставщика.

Можно создать профиль внешней сети, который будет получать параметры шлюза, маски подсети и DHCP/WINS с помощью конечной точки стороннего зарегистрированного поставщика решения для управления IP-адресами.

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Информацию о создании профиля внешней сети без использования поставщика управления IP-адресами или с использованием указанной внутренней конечной точки поставщика управления IP-адресами см. в разделе [Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами](#).

Процедура

1. Задание сведений профиля внешней сети с помощью сторонней конечной точки управления IP-адресами

Профиль внешней сети определяет свойства и параметры внешней сети. Профиль внешней сети — это требование профилей NAT и профилей маршрутизируемой сети. Если в vRealize Orchestrator зарегистрирована и настроена конечная точка управления IP-адресами, можно указать, что информация об IP-адресах указывается поставщиком управления IP-адресами.

2. Настройка диапазонов IP-адресов профиля внешней сети с использованием конечной точки стороннего поставщика услуг управления IP-адресами

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Следующие шаги

Вы можете назначить профиль сети сетевому пути в резервировании, или архитектор схемы элементов может задать профиль сети в схеме элементов. Профиль внешней сети можно использовать при создании профиля сети NAT или маршрутизируемой сети по требованию.

Задание сведений профиля внешней сети с помощью сторонней конечной точки управления IP-адресами
Профиль внешней сети определяет свойства и параметры внешней сети. Профиль внешней сети — это требование профилей NAT и профилей маршрутизируемой сети. Если в vRealize Orchestrator зарегистрирована и настроена конечная точка управления IP-адресами, можно указать, что информация об IP-адресах указывается поставщиком управления IP-адресами.

Необходимые условия

- Убедитесь, что подключаемый модуль внешнего поставщика управления IP-адресами импортирован и настроен в vRealize Orchestrator, а тип конечной точки поставщика управления IP-адресами зарегистрирован в vRealize Orchestrator. В этом примере поддерживаемым внешним поставщиком управления IP-адресами является Infoblox. См. раздел [Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами](#).
- [Создание конечной точки стороннего поставщика управления IP-адресами](#).
- Настройте vRealize Orchestrator Appliance с помощью рабочего процесса конечной точки управления IP-адресами, зарегистрированной в качестве автономного оркестратора в глобальном арендаторе (administrator@vsphere.local).
- Войдите в службу vRealize Automation в качестве **администратора структуры**.

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **Внешняя** в раскрывающемся меню.
3. Введите имя и, при необходимости, описание.
4. Если настроена одна или несколько конечных точек стороннего поставщика управления IP-адресами, выберите необходимую конечную точку стороннего поставщика управления IP-адресами в раскрывающемся меню **Конечная точка управления IP-адресами**.

При выборе конечной точки стороннего поставщика управления IP-адресами, зарегистрированной в vRealize Orchestrator, IP-адреса будут получены от указанного поставщика управления IP-адресами.

Следующие шаги

Теперь можно определять диапазоны сетей для всех IP-адресов, чтобы закончить определение профиля сети.

Настройка диапазонов IP-адресов профиля внешней сети с использованием конечной точки стороннего поставщика услуг управления IP-адресами

Вы можете задать один или несколько диапазонов сети статических IP-адресов в профиле сети, чтобы с их помощью подготовить компьютер. Если диапазон не указывается, профиль сети можно использовать в качестве политики резервирования сети для выбора сетевого пути резервирования для сетевого адаптера виртуальной машины.

Можно задавать диапазоны, используя IP-адреса, полученные от стороннего поставщика управления IP-адресами.

vRealize Automation сохраняет в базе данных только идентификаторы диапазона управления IP-адресами внешней сети, а не сведения о диапазоне. Если изменить профиль сети на этой странице или в схеме элементов, в vRealize Automation будет вызвана служба управления IP-адресами для получения сведений о диапазоне на основе идентификаторов выбранного диапазона.

Примечание Существует определенная проблема с некоторыми сторонними поставщиками управления IP-адресами, из-за которой при получении диапазонов сети может закончиться время ожидания запроса, в результате чего будет возвращен пустой список. В качестве решения можно задать критерии поиска, позволяющие избежать завершения времени ожидания и получить сведения о диапазонах сети.

К примеру, в зависимости от поставщика управления IP-адресами можно добавить свойство с именем VLAN для каждой сети в приложении поставщика и установить для этого свойства значение, например 4. Затем можно фильтровать результаты по свойству и значению, например VLAN=4, в текстовом поле **Выберите диапазон сети** на странице профиля сети vRealize Automation.

Либо можно увеличить значение параметра времени ожидания, выполнив следующие действия.

1. На каждом узле cnode устройства vRealize Automation откройте файл `/etc/vcac/webapps/o11n-gateway-service/WEB-INF/classes/META-INF/spring/root/o11n-gateway-service-context.xml`.
2. Установите для времени ожидания значение больше 30 секунд.
3. Перезапустите vcac-сервер, выполнив команду `service vcac-server restart`.

Необходимые условия

Задание сведений профиля внешней сети с помощью сторонней конечной точки управления IP-адресами.

Процедура

1. Чтобы создать новый или выбрать существующий сетевой диапазон, перейдите на вкладку **Диапазоны сети**.
2. В раскрывающемся меню **Адресное пространство** выберите адресное пространство из списка всех адресных пространств, которые доступны для конечной точки.
3. Щелкните **Добавить** и выберите один или несколько диапазонов сети для указанного адресного пространства.

После выбора диапазона сети может отобразиться пустой список при использовании стороннего поставщика управления IP-адресами. Дополнительные сведения см. в статье базы знаний 2148656 по адресу <http://kb.vmware.com/kb/2148656>.

4. Нажмите кнопку **ОК**.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

5. Чтобы завершить настройку профиля сети, нажмите **ОК**.

Следующие шаги

Вы можете назначить профиль сети сетевому пути в резервировании, или архитектор схемы элементов может задать профиль сети в схеме элементов.

Создание профиля маршрутизируемой сети для сети по требованию

Вы можете создать профиль маршрутизируемой сети по требованию с использованием предоставленной конечной точки управления IP-адресами vRealize Automation или правильно настроенной и зарегистрированной сторонней конечной точки управления IP-адресами.

Профиль маршрутизируемой сети представляет собой маршрутизируемое пространство IP-адресов, разделенное между несколькими сетями. Каждая новая маршрутизируемая сеть выделяет следующую доступную подсеть из маршрутизируемого пространства IP-адресов. Маршрутизируемая сеть имеет доступ ко всем остальным маршрутизируемым сетям, использующим тот же профиль сети. Каждая маршрутизируемая подсеть имеет доступ ко всем остальным подсетям, созданным тем же профилем сети.

Если используется сторонний поставщик управления IP-адресами, то маршрутизируемое пространство IP-адресов создается и контролируется этим сторонним поставщиком. Администратор сети использует стороннего поставщика управления IP-адресами для определения маршрутизируемого пространства IP-адресов и создания для него блока IP-адресов. При создании или редактировании профиля маршрутизируемой сети можно выбрать один или несколько блоков IP-адресов, полученных от стороннего поставщика управления IP-адресами.

Если новый экземпляр профиля маршрутизируемой сети выделяется сторонним поставщиком управления IP-адресами, в vRealize Automation поставщику отправляется запрос зарезервировать следующую доступную подсеть и создается диапазон с использованием блоков IP-адресов, которые определяются профилем маршрутизируемой сети и размером подсети. Полученный диапазон используется для выделения IP-адресов компьютерам, назначенным маршрутизируемой сети в том же развертывании.

Создание профиля маршрутизируемой сети с помощью указанной конечной точки управления IP-адресами

При использовании профиля маршрутизируемой сети с указанной конечной точкой управления IP-адресами можно определить маршрутизируемое пространство IP-адресов и доступные подсети для маршрутизируемой сети по требованию.

С помощью указанной конечной точки управления IP-адресами vRealize Automation профилю маршрутизируемой сети можно назначить диапазоны статических IP-адресов и базовый IP-адрес.

Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.

Процедура

1. Указание сведений о профиле маршрутизируемой сети при использовании конечной точки управления IP-адресами vRealize Automation

Информация о профиле сети определяет свойства маршрутизируемой сети, профиль внешней базовой сети и другие значения, используемые при подготовке сети с предоставленной конечной точкой управления IP-адресами.

2. Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием конечной точки управления IP-адресами vRealize Automation

Вы можете задать один или несколько диапазонов статических IP-адресов, чтобы с их помощью подготовить сеть.

Указание сведений о профиле маршрутизируемой сети при использовании конечной точки управления IP-адресами vRealize Automation

Информация о профиле сети определяет свойства маршрутизируемой сети, профиль внешней базовой сети и другие значения, используемые при подготовке сети с предоставленной конечной точкой управления IP-адресами.

Инструкции по созданию профиля маршрутизируемой сети с помощью конечной точки управления IP-адресами стороннего разработчика приведены в разделе [Ввод сведений о профиле маршрутизируемой сети при использовании сторонней конечной точки управления IP-адресами](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте профиль внешней сети. См. раздел [Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **Направлено по маршруту** в раскрывающемся меню.
3. Введите имя и, при необходимости, описание.
4. Примите значение параметра **Конечная точка управления IP-адресами** по умолчанию для предоставленной конечной точки **Управление IP-адресами vRealize Automation**.
5. Выберите профиль существующей внешней сети в раскрывающемся меню **Профиль внешней сети**.
6. В текстовом поле **Маска подсети** введите маску подсети, связанную с профилем внешней сети.

Маска подсети определяет размер всего маршрутизируемого адресного пространства, которое нужно задать для профиля сети.

Например, 255.255.0.0.

7. Выберите значение в раскрывающемся меню **Маска подсети диапазона.**

Например, 255.255.255.0.

Маска подсети диапазона определяет способ разделения пространства сети на отдельные блоки адресов. Блоки выделяются каждому экземпляру развертывания профиля сети.

Диапазон используется для каждого развертывания, в котором используется профиль маршрутизируемой сети. Количество доступных маршрутизируемых диапазонов равно значению маски подсети, поделенному на значение маски подсети диапазона, например $255.255.0.0 / 255.255.255.0 = 256$.

8. Введите первый доступный IP-адрес в текстовом поле **Базовый IP-адрес.**

Для некоторых сторонних конечных точек этот параметр недоступен.

Например, 120.120.0.1.

9. Выберите вкладку **DNS.**

10. При необходимости введите значения DNS и WINS.

Используйте значения DNS для регистрации имени и разрешения. Эти значения не являются обязательными для внутреннего управления IP-адресами. Они предоставляются сторонним поставщиком управления IP-адресами для внешнего управления IP-адресами.

- а) (дополнительно) Введите значение в поле **Основной сервер DNS**.
- б) (дополнительно) Введите значение в поле **Дополнительный сервер DNS**.
- в) (дополнительно) Введите значение в поле **Суффиксы DNS**.
- г) (дополнительно) Введите значение в поле **Суффиксы поиска DNS**.
- д) (дополнительно) Введите значение в поле **Предпочитаемая служба WINS**.
- е) (дополнительно) Введите значение в поле **Альтернативная служба WINS**.

Следующие шаги

[Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием конечной точки управления IP-адресами vRealize Automation.](#)

Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием конечной точки управления IP-адресами vRealize Automation

Вы можете задать один или несколько диапазонов статических IP-адресов, чтобы с их помощью подготовить сеть.

Во время подготовки каждая новая маршрутизируемая сеть выделяет следующий доступный диапазон и использует его в качестве IP-пространства.

Необходимые условия

[Указание сведений о профиле маршрутизируемой сети при использовании конечной точки управления IP-адресами vRealize Automation.](#)

Процедура

1. Чтобы создать новый или выбрать существующий сетевой диапазон, перейдите на вкладку **Диапазоны сети**.
2. Щелкните **Создать диапазоны**, чтобы создать диапазоны сети на основе маски подсети, маски подсети диапазона и базового IP-адреса, введенных на вкладке «Общие».

Начиная с базового IP-адреса, vRealize Automation создает диапазоны, основанные на маске подсети диапазона.

Например, если маска подсети 255.255.0.0, а маска подсети диапазона 255.255.255.0, vRealize Automation создает 255 диапазонов IP-адресов, используя имя от Диапазон1 до Диапазонл.

3. Нажмите кнопку **ОК**.

Создание профиля маршрутизируемой сети с помощью сторонней конечной точки управления IP-адресами

При использовании профиля маршрутизируемой сети со сторонней конечной точкой управления IP-адресами маршрутизируемое пространство IP-адресов создается и управляется сторонним поставщиком управления IP-адресами.

Если в профиле маршрутизируемой сети используется сторонняя конечная точка управления IP-адресами, поставщик создает новые диапазоны IP-адресов для каждого экземпляра сети по требованию.

Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.

Процедура

1. [Ввод сведений о профиле маршрутизируемой сети при использовании сторонней конечной точки управления IP-адресами](#)

Информация о профиле сети определяет свойства маршрутизируемой сети, профиль внешней базовой сети и другие значения, используемые при подготовке сети со сторонней конечной точкой управления IP-адресами.

2. [Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием сторонней конечной точки управления IP-адресами](#)

Можно управлять одним или несколькими именованными диапазонами статических сетевых адресов в формате IPv4, чтобы с их помощью подготавливать сеть.

Ввод сведений о профиле маршрутизируемой сети при использовании сторонней конечной точки управления IP-адресами

Информация о профиле сети определяет свойства маршрутизируемой сети, профиль внешней базовой сети и другие значения, используемые при подготовке сети со сторонней конечной точкой управления IP-адресами.

Необходимые условия

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

- Создайте профиль внешней сети. См. раздел [Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами](#) или [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#).
- Создайте и настройте стороннюю конечную точку управления IP-адресами. См. раздел [Создание конечной точки стороннего поставщика управления IP-адресами](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **Направлено по маршруту** в раскрывающемся меню.
3. Введите имя и, при необходимости, описание.
4. Если настроена одна или несколько конечных точек стороннего поставщика управления IP-адресами, выберите необходимую конечную точку стороннего поставщика управления IP-адресами в раскрывающемся меню **Конечная точка управления IP-адресами**.

При выборе конечной точки стороннего поставщика управления IP-адресами, зарегистрированной в vRealize Orchestrator, IP-адреса будут получены от указанного поставщика управления IP-адресами.

5. Выберите профиль существующей внешней сети в раскрывающемся меню **Профиль внешней сети**.

В списке представлены и доступны для выбора только профили внешних сетей, настройки которых предполагают использование заданной конечной точки управления IP-адресами.

6. Чтобы задать количество создаваемых подсетей в сети, выберите значение в раскрывающемся меню **Маска подсети диапазона**.

Например, 255.255.255.0.

С помощью маски подсети диапазона задается способ разделения этого пространства на отдельные блоки адресов, которые выделяются для каждого экземпляра развертывания данного профиля сети. При выборе значения для маски подсети диапазона определитесь с количеством развертываний, в которых будет задействована маршрутизируемая сеть.

Диапазон используется для каждого развертывания, где применяется профиль маршрутизируемой сети. Количество доступных маршрутизируемых диапазонов равно значению маски подсети, поделенному на значение маски подсети диапазона, например $255.255.0.0 / 255.255.255.0 = 256$.

7. Для определения адресного пространства и управления одним или несколькими именованными диапазонами статических сетевых адресов IPv4 перейдите на вкладку **Блоки IP-адресов**.

Создание и выделение диапазонов IP-адресов для маршрутизации по требованию выполняется на основе доступных блоков IP-адресов.

Следующие шаги

[Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием сторонней конечной точки управления IP-адресами.](#)

Настройка диапазонов IP-адресов профиля маршрутизируемой сети с использованием сторонней конечной точки управления IP-адресами

Можно управлять одним или несколькими именованными диапазонами статических сетевых адресов в формате IPv4, чтобы с их помощью подготавливать сеть.

Во время подготовки каждая новая маршрутизируемая сеть выделяет следующий доступный диапазон и использует этот выделенный диапазон в качестве IP-пространства. Блоки IP-адресов предоставляет сторонний поставщик управления IP-адресами. Во время подготовки маршрутизируемая сеть выделяется из блока с маской подсети, соответствующей предоставленной маске подсети диапазона.

Необходимые условия

[Ввод сведений о профиле маршрутизируемой сети при использовании сторонней конечной точки управления IP-адресами.](#)

Процедура

1. Чтобы ограничить блоки IP-адресов, доступные для подготовки, выберите адресное пространство в раскрывающемся меню **Адресное пространство**.

После добавления блоков IP-адресов выбрать адресное пространство невозможно. Профиль маршрутизируемой сети не может охватывать несколько адресных пространств.

2. Добавьте один или несколько блоков IP-адресов или диапазонов поставщика управления IP-адресами.

Блоки IP-адресов предоставляет сторонний поставщик управления IP-адресами.

После выбора диапазона сети может отобразиться пустой список при использовании стороннего поставщика управления IP-адресами. Дополнительные сведения см. в статье базы знаний 2148656 по адресу <http://kb.vmware.com/kb/2148656>.

а) Нажмите кнопку **Добавить**.

б) Нажмите **Поиск**.

в) Введите синтаксис поиска или выберите блоки IP-адресов из раскрывающегося меню.

г) Нажмите кнопку **ОК**.

3. Нажмите кнопку **Применить**.

4. Нажмите кнопку **ОК**.

Создание профиля сети NAT для сети по требованию

Вы можете создать профиль сети NAT по требованию с использованием предоставленной конечной точки управления IP-адресами vRealize Automation или правильно настроенной и зарегистрированной сторонней конечной точки управления IP-адресами.

Создание профиля сети NAT с помощью указанной конечной точки управления IP-адресами

Можно создать профиль сети NAT NSX по требованию, связанный с профилем внешней сети. С помощью указанной конечной точки управления IP-адресами vRealize Automation профилю сети NAT можно назначить диапазоны статических IP-адресов и DHCP-адресов.

В сетях NAT один набор IP-адресов используется для внешнего обмена данными, а другой — для внутреннего. Внешние IP-адреса выделяются из внешнего профиля сети, а внутренние IP-адреса NAT определяет профиль сети NAT. При подготовке новой сети NAT создается новый экземпляр профиля сети NAT, который используется для выделения IP-адресов компьютерам.

Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.

Для сети NAT «один ко многим» можно определить правила NAT, которые настраиваются при добавлении компонента сети NAT в схему элементов. Правило NAT можно изменить при редактировании сети NAT в развертывании.

Процедура

1. Указание сведений о профиле сети NAT при использовании конечной точки управления IP-адресами vRealize Automation

Профиль сети определяет свойства сети NAT по требованию, профиль внешней базовой сети, тип NAT и другие значения, используемые при подготовке сети с помощью встроенной службы управления IP-адресами vRealize Automation.

2. Настройка диапазонов IP-адресов профиля сети NAT с использованием конечной точки управления IP-адресами vRealize Automation

Вы можете задать один или несколько диапазонов статических IP-адресов, чтобы с их помощью подготовить сеть.

Указание сведений о профиле сети NAT при использовании конечной точки управления IP-адресами vRealize Automation

Профиль сети определяет свойства сети NAT по требованию, профиль внешней базовой сети, тип NAT и другие значения, используемые при подготовке сети с помощью встроенной службы управления IP-адресами vRealize Automation.

Если требуется создать профиль сети NAT, который использует стороннюю конечную точку управления IP-адресами, см. раздел [Указание сведений о профиле сети NAT при использовании сторонней конечной точки управления IP-адресами](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте профиль внешней сети. См. раздел [Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **NAT** в раскрывающемся меню.
3. Введите имя и, при необходимости, описание.

4. Примите значение параметра **Конечная точка управления IP-адресами** по умолчанию для предоставленной конечной точки **Управление IP-адресами vRealize Automation**
5. Выберите профиль существующей внешней сети в раскрывающемся меню **Профиль внешней сети**.
6. В раскрывающемся списке **Тип NAT** выберите тип преобразования сетевых адресов «Один к одному» или «Один ко многим».

Параметр	Описание
Один к одному	<p>Назначьте внешний статический IP-адрес каждому сетевому адаптеру. К внешней сети можно получить доступ с помощью любого компьютера, и сами компьютеры доступны через эту сеть.</p> <p>Все внешние IP-адреса, назначенные исходящему подключению NSX Edge, должны принадлежать одной и той же подсети. При использовании NAT типа «один к одному» в vRealize Automation соответствующий профиль внешней сети должен содержать только те диапазоны IP-адресов, которые присутствуют в одной подсети.</p>
Один к многим	<p>Все компьютеры в сети будут использовать общий внешний IP-адрес. Во внутренней сети компьютеры смогут использовать адреса DHCP или статические IP-адреса. К внешней сети можно получить доступ с помощью любого компьютера, но к компьютерам нельзя получить доступ через эту сеть. Если выбрать этот параметр, в группе DHCP будет установлен флажок Включено.</p> <p>В NSX for vSphere преобразование NAT типа «один ко многим» дает возможность определить правила NAT при добавлении компонента сети NAT в схему элементов.</p> <p>NSX for vSphere поддерживает сети NAT «один к одному» и «один ко многим», но NSX-T поддерживает только сети NAT «один ко многим».</p>

7. В текстовом поле **Маска подсети** введите маску подсети IP-адреса.

Маска подсети определяет размер всего маршрутизируемого адресного пространства, которое нужно будет задать для профиля сети.

Например, 255.255.0.0.

8. В поле **Шлюз** введите адрес маршрутизируемого шлюза, например 10.10.110.1.

Заданный в профиле сети IP-адрес шлюза назначается сетевому адаптеру во время выделения. Шлюз требуется для сетевых профилей NAT.

Для NSX-T шлюз DHCP-сервера по умолчанию соответствует шлюзу NAT «один ко многим» по умолчанию. Шлюз пула IP-адресов по умолчанию соответствует шлюзу для сети NAT «один ко многим» по умолчанию в vRealize Automation.

Если в текстовом поле **Шлюз** профиля сети не задано значение, для указания шлюза используйте настраиваемое свойство `VirtualMachine.Network0.Gateway`.

9. (дополнительно) В группе DHCP установите флажок **Включен** и введите значения в поля **Начало диапазона IP-адресов** и **Конец диапазона IP-адресов**.

Установить флажок можно, только если для параметра «Тип NAT» установлено значение «Один ко многим».

Для NSX-T первый IP-адрес в диапазоне пула IP-адресов совпадает с IP-адресом DHCP-сервера, который задан параметром <FirstIpInPool>/<subnetMaskOfNat>. Пул IP-адресов в NSX-T начинается со второго IP-адреса.

10. (дополнительно) Задайте время аренды DHCP, чтобы указать, как долго компьютер может использовать IP-адрес.
11. Выберите вкладку **DNS**.
12. При необходимости введите значения DNS и WINS.

Используйте значения DNS для регистрации имени и разрешения. Эти значения не являются обязательными для внутреннего управления IP-адресами. Они предоставляются сторонним поставщиком управления IP-адресами для внешнего управления IP-адресами.

- а) (дополнительно) Введите значение в поле **Основной сервер DNS**.
- б) (дополнительно) Введите значение в поле **Дополнительный сервер DNS**.
- в) (дополнительно) Введите значение в поле **Суффиксы DNS**.
- г) (дополнительно) Введите значение в поле **Суффиксы поиска DNS**.
- д) (дополнительно) Введите значение в поле **Предпочитаемая служба WINS**.
- е) (дополнительно) Введите значение в поле **Альтернативная служба WINS**.

Следующие шаги

[Настройка диапазонов IP-адресов профиля сети NAT с использованием конечной точки управления IP-адресами vRealize Automation.](#)

Настройка диапазонов IP-адресов профиля сети NAT с использованием конечной точки управления IP-адресами vRealize Automation

Вы можете задать один или несколько диапазонов статических IP-адресов, чтобы с их помощью подготовить сеть.

Начальный и конечный IP-адреса диапазона сети не могут перекрывать адреса DHCP. При попытке сохранить профиль, который содержит перекрывающиеся диапазоны адресов, vRealize Automation показывает ошибку проверки.

Необходимые условия

[Указание сведений о профиле сети NAT при использовании конечной точки управления IP-адресами vRealize Automation.](#)

Процедура

1. Чтобы создать новый или выбрать существующий сетевой диапазон, перейдите на вкладку **Диапазоны сети**.

2. Чтобы указать новое имя диапазона сети и диапазон IP-адресов вручную, нажмите **Создать**, или выберите **Импортировать из CSV**, чтобы импортировать сведения об IP-адресе из должным образом отформатированного CSV-файла.

- Нажмите кнопку **Создать**.

- а) Введите имя диапазона сети.
- б) Введите описание диапазона сети.
- в) Введите начальный IP-адрес диапазона.
- г) Введите конечный IP-адрес диапазона.

- Щелкните **Импортировать из CSV**.

- а) Найдите и выберите CSV-файл или перетащите его в диалоговое окно **Импортировать из CSV**.

Строка в CSV-файле имеет следующий формат *ip_address, machine_name, status, NIC_offset*. Пример:

```
100.10.100.1,mymachine01,Allocated,0
```

Поле в CSV-файле	Описание
ip_address	IP-адрес в формате IPv4.
machine_name	Имя управляемой машины в vRealize Automation. Если поле пустое, то имя по умолчанию отсутствует. Если поле пустое, для поля <i>status</i> не может устанавливаться значение «Выделен».
status	Доступны значения <i>Allocated</i> или <i>Unallocated</i> . В этом поле учитывается регистр. Если поле пустое, по умолчанию устанавливается значение «Не выделен». Если установлено состояние «Выделен», поле <i>machine_name</i> не может быть пустым.
NIC_offset	Неотрицательное целое число. Смещение сетевого адаптера указывает, какому сетевому адаптеру виртуальной машины назначен данный IP-адрес. Если виртуальная машина выделяет несколько IP-адресов для разных сетевых адаптеров, то для каждого сетевого адаптера, который содержит соответствующее смещение, создается отдельная запись IP-адреса. Значение 0 указывает на отсутствие смещения.

- б) Нажмите кнопку **Применить**.

3. Нажмите кнопку **ОК**.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

4. Чтобы отобразить IP-адреса для именованного сетевого диапазона, перейдите на вкладку **IP-адреса**.

5. (дополнительно) Чтобы отфильтровать записи IP-адресов, выберите IP-адрес в раскрывающемся меню **Диапазон сети**.

Можно отобразить информацию обо всех определенных диапазонах сети, диапазонах сети, импортированных из CSV-файла, или именованных диапазонах сети.

6. (дополнительно) Чтобы отфильтровать IP-адреса по состоянию, выберите тип состояния в раскрывающемся меню **Состояние IP-адреса**.

Для IP-адресов с состоянием «Удален» (Destroyed) или «Просрочен» (Expired) можно щелкнуть **Реорганизовать**, чтобы сделать эти диапазоны IP-адресов доступными для выделения. Необходимо сохранить профиль, чтобы реорганизация вступила в силу. Обновление столбца «Состояние» (Status) с Expired или Destroyed на Allocated может занять до 1 минуты.

7. Нажмите кнопку **ОК**.

Создание профиля сети NAT в vRealize Automation с помощью сторонней конечной точки управления IP-адресами

В vRealize Automation можно создать профиль сети NAT NSX по требованию, связанный с профилем внешней сети. При использовании профиля сети NAT NSX со сторонним поставщиком управления IP-адресами пространство IP-адресов создается и управляется этим поставщиком.

Если в профиле сети NAT используется сторонняя конечная точка управления IP-адресами, поставщик создает новые диапазоны IP-адресов для каждого экземпляра сети по требованию. Внутренний набор IP-адресов, для которого задан один или несколько диапазонов, создается в сторонней конечной точке поставщика управления IP-адресами для каждого экземпляра сети. Диапазоны IP-адресов определяют IP-адреса компьютеров в сети в одном и том же развертывании. Так как в пределах одного адресного пространства не может быть повторяющихся IP-адресов, поставщик создает новое адресное пространство для каждого экземпляра сети. При удалении сети NAT ее диапазоны удаляются в конечной точке поставщика управления IP-адресами и в новом адресном пространстве.

Можно использовать диапазоны IP-адресов, полученные из настроенной конечной точки управления IP-адресами VMware или конечной точки стороннего поставщика управления IP-адресами, который зарегистрирован и настроен в vRealize Orchestrator, например управление IP-адресами Infoblox. Диапазон IP-адресов создается из блока IP-адресов во время выделения.

Для сети NAT «один ко многим» можно определить правила NAT, которые настраиваются при добавлении компонента сети NAT в схему элементов. Правило NAT можно изменить при редактировании сети NAT в развертывании.

Процедура

1. [Указание сведений о профиле сети NAT при использовании сторонней конечной точки управления IP-адресами](#)

Сведения о профиле сети определяют свойства сети NAT, профиль внешней базовой сети для нее и другие значения, используемые при подготовке сети со сторонней конечной точкой управления IP-адресами.

2. Настройка диапазонов IP-адресов профиля сети NAT с использованием сторонней конечной точки управления IP-адресами

Вы можете определить один или несколько диапазонов IP-адресов для использования в подготовке сети с помощью NAT.

Указание сведений о профиле сети NAT при использовании сторонней конечной точки управления IP-адресами

Сведения о профиле сети определяют свойства сети NAT, профиль внешней базовой сети для нее и другие значения, используемые при подготовке сети со сторонней конечной точкой управления IP-адресами.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте профиль внешней сети. См. раздел [Создание профиля внешней сети с помощью указанной конечной точки управления IP-адресами](#) или [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#).
- Создайте и настройте стороннюю конечную точку управления IP-адресами. См. раздел [Создание конечной точки стороннего поставщика управления IP-адресами](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и выберите **NAT** в раскрывающемся меню.
3. Введите имя и, при необходимости, описание.
4. Если настроена одна или несколько конечных точек стороннего поставщика управления IP-адресами, выберите необходимую конечную точку стороннего поставщика управления IP-адресами в раскрывающемся меню **Конечная точка управления IP-адресами**.

При выборе конечной точки стороннего поставщика управления IP-адресами, зарегистрированной в vRealize Orchestrator, IP-адреса будут получены от указанного поставщика управления IP-адресами.

5. Выберите профиль существующей внешней сети в раскрывающемся меню **Профиль внешней сети**.

В списке представлены и доступны для выбора только профили внешних сетей, настройки которых предполагают использование заданной конечной точки управления IP-адресами.

6. В раскрывающемся списке **Тип NAT** выберите тип преобразования сетевых адресов «Один к одному» или «Один ко многим».

Параметр	Описание
Один к одному	<p>Назначьте внешний статический IP-адрес каждому сетевому адаптеру. К внешней сети можно получить доступ с помощью любого компьютера, и сами компьютеры доступны через эту сеть.</p> <p>Все внешние IP-адреса, назначенные исходящему подключению NSX Edge, должны принадлежать одной и той же подсети. При использовании NAT типа «один к одному» в vRealize Automation соответствующий профиль внешней сети должен содержать только те диапазоны IP-адресов, которые присутствуют в одной подсети.</p>
Один к многим	<p>Все компьютеры в сети будут использовать общий внешний IP-адрес. Во внутренней сети компьютеры могут использовать только статические IP-адреса. К внешней сети можно получить доступ с помощью любого компьютера, но к компьютерам нельзя получить доступ через эту сеть.</p> <p>DHCP не поддерживается при использовании NAT со сторонним поставщиком управления IP-адресами.</p> <p>В NSX for vSphere преобразование NAT типа «один ко многим» дает возможность определить правила NAT при добавлении компонента сети NAT в схему элементов.</p> <p>NSX for vSphere поддерживает сети NAT «один к одному» и «один ко многим», но NSX-T поддерживает только сети NAT «один ко многим».</p>

7. В текстовом поле **Маска подсети** введите маску подсети IP-адреса.

Маска подсети определяет размер всего маршрутизируемого адресного пространства, которое нужно будет задать для профиля сети.

Например, 255.255.0.0.

8. В поле **Шлюз** введите адрес маршрутизируемого шлюза, например 10.10.110.1.

Заданный в профиле сети IP-адрес шлюза назначается сетевому адаптеру во время выделения. Шлюз требуется для сетевых профилей NAT.

Для NSX-T шлюз DHCP-сервера по умолчанию соответствует шлюзу NAT «один ко многим» по умолчанию. Шлюз пула IP-адресов по умолчанию соответствует шлюзу для сети NAT «один ко многим» по умолчанию в vRealize Automation.

Если в текстовом поле **Шлюз** профиля сети не задано значение, для указания шлюза используйте настраиваемое свойство `VirtualMachine.Network0.Gateway`.

9. Выберите вкладку **DNS**.

10. При необходимости введите значения DNS и WINS.

Используйте значения DNS для регистрации имени и разрешения. Эти значения не являются обязательными для внутреннего управления IP-адресами. Они предоставляются сторонним поставщиком управления IP-адресами для внешнего управления IP-адресами.

- (дополнительно) Введите значение в поле **Основной сервер DNS**.
- (дополнительно) Введите значение в поле **Дополнительный сервер DNS**.

- в) (дополнительно) Введите значение в поле **Суффиксы DNS**.
- г) (дополнительно) Введите значение в поле **Суффиксы поиска DNS**.
- д) (дополнительно) Введите значение в поле **Предпочитаемая служба WINS**.
- е) (дополнительно) Введите значение в поле **Альтернативная служба WINS**.

Следующие шаги

[Настройка диапазонов IP-адресов профиля сети NAT с использованием сторонней конечной точки управления IP-адресами.](#)

Настройка диапазонов IP-адресов профиля сети NAT с использованием сторонней конечной точки управления IP-адресами

Вы можете определить один или несколько диапазонов IP-адресов для использования в подготовке сети с помощью NAT.

Необходимые условия

[Указание сведений о профиле сети NAT при использовании сторонней конечной точки управления IP-адресами.](#)

Процедура

1. Чтобы создать новый или выбрать существующий сетевой диапазон, перейдите на вкладку **Диапазоны сети**.
2. Щелкните **Создать** и задайте диапазон сети.
 - а) Введите имя и описание диапазона сети.
 - б) Введите начальный и конечный IP-адреса, определяющие диапазон сети.
 - в) Нажмите кнопку **Применить**.

3. Нажмите кнопку **ОК**.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

4. Чтобы отобразить IP-адреса для именованного сетевого диапазона, перейдите на вкладку **IP-адреса**.
5. (дополнительно) Чтобы отфильтровать записи IP-адресов, выберите IP-адрес в раскрывающемся меню **Диапазон сети**.

Можно отобразить информацию обо всех определенных диапазонах сети, диапазонах сети, импортированных из CSV-файла, или именованных диапазонах сети.

6. (дополнительно) Чтобы отфильтровать IP-адреса по состоянию, выберите тип состояния в раскрывающемся меню **Состояние IP-адреса**.

Для IP-адресов с состоянием «Удален» (Destroyed) или «Просрочен» (Expired) можно щелкнуть **Реорганизовать**, чтобы сделать эти диапазоны IP-адресов доступными для выделения. Необходимо сохранить профиль, чтобы реорганизация вступила в силу. Обновление столбца «Состояние» (Status) с Expired или Destroyed на Allocated может занять до 1 минуты.

7. Нажмите кнопку **ОК**.

Создание профиля частной сети для сети по требованию в vRealize Automation

Можно создать частную сеть для NSX for vSphere, которая использует спецификацию управления IP-адресами, входящую в состав vRealize Automation.

Можно создать профиль частной сети по требованию для NSX for vSphere, связанный с профилем внешней сети.

Частные сети недоступны для NSX-T.

Стороннее управление IP-адресами недоступно для частных сетей.

Вы можете задать один или несколько диапазонов статических IP-адресов, чтобы с их помощью подготовить сеть.

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Резервирования > Профили сетей**.
2. Щелкните **Создать** и в раскрывающемся меню выберите **Частная**.
3. Введите имя и, при необходимости, описание.
4. Примите значение параметра **Конечная точка управления IP-адресами** по умолчанию для предоставленной конечной точки **Управление IP-адресами vRealize Automation**.
5. Выберите идентификатор арендатора при появлении соответствующего запроса.
6. В текстовом поле **Маска подсети** введите маску подсети IP-адреса.

Маска подсети определяет размер всего маршрутизируемого адресного пространства, которое нужно будет задать для профиля сети.

Например, 255.255.0.0.

7. В поле **Шлюз** введите адрес маршрутизируемого шлюза, например 10.10.110.1.

Заданный в профиле сети IP-адрес шлюза назначается сетевому адаптеру во время выделения. Если в текстовом поле **Шлюз** профиля сети не задано значение, для указания шлюза используйте настраиваемое свойство `VirtualMachine.Network0.Gateway`.

8. Выберите вкладку **DNS**.

9. При необходимости введите значения DNS и WINS.

При попытке сохранить профиль, который содержит перекрывающиеся диапазоны адресов, vRealize Automation показывает ошибку проверки.

10. Чтобы создать новый или выбрать существующий сетевой диапазон, перейдите на вкладку **Диапазоны сети**.**11.** Чтобы указать новое имя диапазона сети и диапазон IP-адресов вручную, нажмите **Создать**, или выберите **Импортировать из CSV**, чтобы импортировать сведения об IP-адресе из должным образом отформатированного CSV-файла.■ Нажмите кнопку **Создать**.

- а) Введите имя диапазона сети.
- б) Введите описание диапазона сети.
- в) Введите начальный IP-адрес диапазона.
- г) Введите конечный IP-адрес диапазона.

■ Щелкните **Импортировать из CSV**.

- а) Найдите и выберите CSV-файл или перетащите его в диалоговое окно **Импортировать из CSV**.

Строка в CSV-файле имеет следующий формат *ip_address, machine_name, status, NIC_offset*. Пример:

```
100.10.100.1,mymachine01,Allocated,0
```

Поле в CSV-файле	Описание
ip_address	IP-адрес в формате IPv4.
machine_name	Имя управляемой машины в vRealize Automation. Если поле пустое, то имя по умолчанию отсутствует. Если поле пустое, для поля <i>status</i> не может устанавливаться значение «Выделен».
status	Доступны значения <i>Allocated</i> или <i>Unallocated</i> . В этом поле учитывается регистр. Если поле пустое, по умолчанию устанавливается значение «Не выделен». Если установлено состояние «Выделен», поле <i>machine_name</i> не может быть пустым.
NIC_offset	Неотрицательное целое число. Смещение сетевого адаптера указывает, какому сетевому адаптеру виртуальной машины назначен данный IP-адрес. Если виртуальная машина выделяет несколько IP-адресов для разных сетевых адаптеров, то для каждого сетевого адаптера, который содержит соответствующее смещение, создается отдельная запись IP-адреса. Значение 0 указывает на отсутствие смещения.

- б) Нажмите кнопку **Применить**.

12. Нажмите кнопку **ОК**.

IP-адреса в диапазоне отображаются в списке «Определенные IP-адреса».

IP-адреса отображаются после нажатия кнопки **Применить** или после сохранения и последующего редактирования профиля сети.

13. Чтобы отобразить IP-адреса для именованного сетевого диапазона, перейдите на вкладку **IP-адреса**.

14. (дополнительно) Чтобы отфильтровать записи IP-адресов, выберите IP-адрес в раскрывающемся меню **Диапазон сети**.

Можно отобразить информацию обо всех определенных диапазонах сети, диапазонах сети, импортированных из CSV-файла, или именованных диапазонах сети.

15. (дополнительно) Чтобы отфильтровать IP-адреса по состоянию, выберите тип состояния в раскрывающемся меню **Состояние IP-адреса**.

Для IP-адресов с состоянием «Удален» (Destroyed) или «Просрочен» (Expired) можно щелкнуть **Реорганизовать**, чтобы сделать эти диапазоны IP-адресов доступными для выделения. Необходимо сохранить профиль, чтобы реорганизация вступила в силу. Обновление столбца «Состояние» (Status) с Expired или Destroyed на Allocated может занять до 1 минуты.

16. Нажмите кнопку **ОК**.

Освобождение IP-адресов путем удаления подготовленных компьютеров

В случае удаления развертывания его IP-адреса также удаляются. Выделенные IP-адреса, например IP-адреса в диапазоне профиля сети, освобождаются и становятся доступными для последующих операций по подготовке.

При удалении компьютера его статический IP-адрес становится доступным для использования другими компьютерами. Неиспользованные адреса могут не сразу стать доступными, поскольку процедура реорганизации статических IP-адресов выполняется с интервалом в 30 минут.

Если используется управление IP-адресами от стороннего поставщика, в vRealize Automation соответствующие IP-адреса удаляются с помощью рабочего процесса vRealize Orchestrator в подключаемом модуле или пакете стороннего поставщика управления IP-адресами.

Настройка резервирований и их политик

Резервирование vRealize Automation может определять политики, приоритеты и квоты, от которых зависит размещение компьютеров при поступлении запросов на подготовку.

Политики резервирования ограничивают подготовку компьютеров набором доступных резервирований. Политики резервирования хранилищ позволяют разработчикам схем элементов назначать тома компьютеров различным хранилищам данных.

Для успешной подготовки необходимо наличие в хранилище достаточного объема памяти для резервирования. Доступность хранилища для резервирования зависит от следующих факторов.

- Какой объем пространства доступен в хранилище данных или кластере.
- Какой объем этого пространства зарезервирован для данного хранилища данных или кластера.
- Какой объем этого пространства уже выделен в vRealize Automation

Так, даже если в vCenter Server имеется доступное пространство для хранилища данных или кластера, но не выделено достаточно свободного пространства для резервирования, подготовка завершится с ошибкой («Нет доступного резервирования для выделения...»). Объем пространства, выделяемого для конкретного резервирования, зависит от количества виртуальных машин (в любом состоянии) в этом резервировании. Дополнительные сведения см. в статье базы знаний VMware «Компьютер XXX: нет доступного резервирования для выделения в группе XXX». *Всего запрошено XX ГБ свободного пространства (2151030)* по адресу <http://kb.vmware.com/kb/2151030>.

Резервирования

Вы можете создать резервирование vRealize Automation, чтобы выделить подготавливаемые ресурсы из группы структур определенной бизнес-группе.

Например, с помощью резервирования можно указать, что часть памяти, ЦП, сети и хранилища вычислительного ресурса принадлежит определенной бизнес-группе или что определенные компьютеры нужно назначить определенной бизнес-группе.

Используйте политику резервирования сети, чтобы управлять передачей данных по сети для развертываний схем элементов. Когда отправляется запрос на подготовку компьютера, политика резервирования используется для группировки резервирований, которые можно учесть для развертывания.

Для нескольких бизнес-групп нельзя использовать общие резервирования.

Примечание Хранилище и память, назначенные подготовленному компьютеру путем резервирования, освобождаются, когда компьютер, которому они назначены, удаляется в vRealize Automation. Хранилище и память не освобождаются, если компьютер удален в vCenter Server.

Вы можете создать резервирование для следующих типов компьютеров:

- vSphere
- vCloud Air
- vCloud Director
- Amazon EC2
- Microsoft Azure
- Hyper V (SCVMM)
- Hyper-V (автономное решение)
- KVM (RHEV)
- OpenStack
- XenServer

Для настройки параметров безопасности можно указать сведения в резервировании, схеме элементов или сценарии гостевого агента. Если для компьютеров требуется гостевой агент, добавьте правило безопасности в резервирование или в схему элементов.

Выбор сценария резервирования

Чтобы назначать ресурсы бизнес-группам, можно создавать резервирования. Процесс создания резервирования зависит от сценария.

Выберите сценарий резервирования на основании типа конечной точки назначения.

У каждой бизнес-группы должно быть по крайней мере одно резервирование, чтобы ее участники могли подготавливать компьютеры этого типа. Например, бизнес-группа с резервированием OpenStack (а не Amazon) не может запрашивать компьютер у компании Amazon. В этом примере бизнес-группе нужно назначить специальное резервирование для ресурсов Amazon.

Таблица 2-15. Выбор сценария резервирования

Сценарий	Процедура
Создание резервирования vSphere.	Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer
Создание резервирования для выделения ресурсов для конечной точки vCloud Air.	Создание резервирования vCloud Air
Создание резервирования для выделения ресурсов для конечной точки vCloud Director.	Создание резервирования vCloud Director
Создание резервирования для выделения ресурсов для ресурса Amazon (при этом можно пользоваться виртуальным частным облаком Amazon или обойтись без него).	Создание резервирования Amazon EC2
Создание резервирования для выделения ресурсов для ресурса OpenStack.	Создание резервирования OpenStack
Создание резервирования для выделения ресурсов для Hyper-V.	Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer
Создание резервирования для выделения ресурсов для KVM.	Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer
Создание резервирования для выделения ресурсов для ресурса OpenStack.	Создание резервирования OpenStack
Создание резервирования для выделения ресурсов для SCVMM.	Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer
Создание резервирования для выделения ресурсов для XenServer.	Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer
Создание резервирования для выделения ресурсов для Microsoft Azure.	Создание резервирования для Microsoft Azure

Создание облачных резервирований категорий

Облачное резервирование типов категорий предоставляет доступ к службам подготовки учетной записи для облачных служб для определенной бизнес-группы vRealize Automation. Среди доступных типов облачных резервирований — Amazon, OpenStack, vCloud Air и vCloud Director.

Резервирование — это совместное использование ресурсов памяти, ЦП, сети и хранилища одного вычислительного ресурса, выделенного для определенной бизнес-группы vRealize Automation.

У бизнес-группы может быть несколько резервирований на одной конечной точке или на нескольких.

Модель выделения для резервирования зависит от модели выделения в связанном центре данных.

Доступные модели выделения — это пул выделения, повременная оплата и пул резервирования. Сведения о моделях выделения см. в документации по vCloud Director или vCloud Air.

Резервирование задает не только объем ресурсов структуры, которые выделяются для бизнес-группы, но и политики, приоритеты и квоты, от которых зависит размещение компьютеров.

Для успешной подготовки необходимо наличие в хранилище достаточного объема памяти для резервирования. Доступность хранилища для резервирования зависит от следующих факторов.

- Какой объем пространства доступен в хранилище данных или кластере.
- Какой объем этого пространства зарезервирован для данного хранилища данных или кластера.
- Какой объем этого пространства уже выделен в vRealize Automation

Так, даже если в vCenter Server имеется доступное пространство для хранилища данных или кластера, но не выделено достаточно свободного пространства для резервирования, подготовка завершится с ошибкой («Нет доступного резервирования для выделения...»). Объем пространства, выделяемого для конкретного резервирования, зависит от количества виртуальных машин (в любом состоянии) в этом резервировании. Дополнительные сведения см. в статье базы знаний VMware «Компьютер XXX: нет доступного резервирования для выделения в группе XXX». *Всего запрошено XX ГБ свободного пространства (2151030)* по адресу <http://kb.vmware.com/kb/2151030>.

Общие сведения о логике выбора для облачных резервирований

Когда участник бизнес-группы создает запрос на подготовку облачного компьютера, vRealize Automation выбирает компьютер из одного из резервирований, доступных для этой бизнес-группы. Облачные резервирования включают в себя Amazon, OpenStack, vCloud Air и vCloud Director.

Резервирование, к которому подготавливается компьютер, должно соответствовать следующим критериям.

- У резервирования и схемы элементов, с которой поступил запрос на компьютер, должен быть одинаковый тип платформы.
- Резервирование должно быть включено.
- Объем резервирования должен находиться в пределах квоты на компьютеры или квота должна быть неограниченна.

Выделенная квота на компьютеры распространяется только на включенные компьютеры. Например, если квота резервирования — 50 компьютеров, 40 подготовлены, но только 20 из них включены, выделяется 40%, а не 80% квоты резервирования.

- В запросе компьютеров должны быть указаны группы безопасности резервирования.
- Резервирование должно быть связано с областью, в которой имеется образ компьютера, указанный в схеме элементов.
- Резервирование должно располагать объемом невыделенных памяти и ресурсов хранилища, достаточным для подготовки компьютера.

В резервированиях с оплатой мере использования может отсутствовать ограничение по ресурсам.

- Для компьютеров Amazon в запросе указывается зона доступности и расположение, в котором следует инициализировать компьютер — в подсети в виртуальном частном облаке (Virtual Private Cloud, VPC) или вне его. Резервирование должно соответствовать типу сети (VPC или вне VPC).
- Если в vCloud Air или vCloud Director запрос определяет модель выделения, ей должна соответствовать модель выделения виртуального ЦОД, связанного с резервированием.
- Для vCloud Director или vCloud Air должна быть включена указанная организация.
- Для резервирования должны быть доступны все шаблоны схемы элементов. Если политика резервирования сопоставляется с несколькими источниками ресурсов, шаблоны должны быть общедоступными.
- Если поставщик облачных служб поддерживает выбор сети, а схема элементов предусматривает специальные параметры сети, соответствующие сети должны быть в резервировании.

Если в схеме элементов или резервировании указан профиль сети для назначения статического IP-адреса, этот адрес должен быть доступен для назначения новому компьютеру.

- Если в запросе определена модель выделения, ей должна соответствовать модель выделения в резервировании.
- Если в схеме элементов указана политика резервирования, резервирование должно к ней принадлежать.

Политики резервирования — это залог того, что выбранное резервирование будет соответствовать дополнительным требованиям к подготовке компьютеров на основе определенной схемы элементов. Например, если схема элементов использует определенный образ компьютера, политики резервирования можно использовать, чтобы ограничить подготовку резервированиями, связанными с областями, в которых находится необходимый образ.

При отсутствии доступных резервирований, отвечающих всем критериям выбора, происходит сбой подготовки.

Если несколько резервирований соответствуют всем критериям, резервирование, с помощью которого будет подготавливаться запрошенный компьютер, определяется по следующей логике.

- Резервирование с более низким значением приоритета выбирается до резервирования с более высоким значением.
- Если у нескольких резервирований одинаковый приоритет, будет выбрано то, у которого самый низкий процент выделенной квоты на компьютеры.
- Если у нескольких резервирований одинаковые приоритет и квоты, компьютеры циклично распределяются по резервированиям.

Примечание Хотя циклический выбор профилей сети не поддерживается, поддерживается циклический выбор сетей (если они доступны), которые можно связать с различными профилями сетей.

Если в резервировании доступны несколько путей к хранилищам с достаточной емкостью для подготовки томов компьютера, их выбирают по следующей логике.

- Путь к хранилищу с более низким значением приоритета выбирается до пути с более высоким значением.
- Если в схеме элементов или запросе указана политика резервирования хранилища, путь к хранилищу должен принадлежать этой политике.

Если для настраиваемого свойства `VirtualMachine.DiskN.StorageReservationPolicyMode` установлено значение «Не определено» и в политике резервирования хранилища нет доступного пути к хранилищу с достаточной емкостью, для подготовки будет выбран путь вне указанной политики резервирования хранилища. По умолчанию значение свойства `VirtualMachine.DiskN.StorageReservationPolicyMode` — `Exact`.

- Если у нескольких путей к хранилищам одинаковый приоритет, компьютеры распределяются по соответствующим путям согласно циклическому расписанию.

Создание резервирования Amazon EC2

Чтобы участники бизнес-группы могли запрашивать подготовку компьютеров, нужно выделить ресурсы компьютерам путем создания резервирования.

Работать можно с резервированиями Amazon для Amazon Virtual Private Cloud или резервированиями Amazon вне VPC. Пользователи Amazon Web Services могут создать облако Amazon Virtual Private Cloud, чтобы спроектировать топологию виртуальной сети, соответствующую указанным характеристикам. Если планируется использовать Amazon VPC, нужно назначить Amazon VPC резервированию vRealize Automation.

При создании резервирования Amazon или настройке компонента компьютера в схеме элементов можно выбрать одну из групп безопасности, которые доступны в определенной области Amazon. Группы безопасности импортируются во время сбора данных.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Сведения о создании Amazon VPC посредством AWS Management Console см. в документации по Amazon Web Services.

Процедура

1. Ввод данных о резервировании Amazon

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

2. Указание параметров ресурсов и сети для резервирований Amazon

Укажите параметры ресурса и сети для подготовки компьютеров на базе этого резервирования vRealize Automation.

3. Указание настраиваемых свойств и оповещений для резервирования Amazon

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Ввод данных о резервировании Amazon

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- Убедитесь, что вычислительный ресурс существует.
- Настройте сеть.
- (дополнительно) Настройте сведения о профиле сети.
- Убедитесь, что у вас есть доступ к нужной сети Amazon. Например, если нужно использовать VPC, убедитесь, что у вас есть доступ к сети Amazon Virtual Private Cloud (VPC).
- Убедитесь, что существуют все требуемые пары ключей. См. раздел [Управление парами ключей](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.
Выберите **Amazon EC2**.
3. В текстовом поле **Имя** введите имя.
4. В раскрывающемся меню **Арендатор** выберите арендатора.
5. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.

Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.

6. (дополнительно) В раскрывающемся меню **Политика резервирования** выберите политику резервирования.

Для применения этого параметра требуется наличие одной или нескольких политик резервирования. Резервирование можно изменить позже, чтобы задать политику резервирования.

Политика резервирования используется для ограничения инициализации конкретными резервированиями.

7. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирование с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

8. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

Результаты

Не переходите никуда с этой страницы. Ваше резервирование не завершено.

Указание параметров ресурсов и сети для резервирований Amazon

Укажите параметры ресурса и сети для подготовки компьютеров на базе этого резервирования vRealize Automation.

При создании резервирования Amazon или настройке компонента компьютера в схеме элементов можно выбрать одну из групп безопасности, которые доступны учетной записи в определенной области Amazon. Группы безопасности импортируются во время сбора данных. Группа безопасности выступает в качестве брандмауэра для контроля доступа к компьютеру. Каждая область включает в себя как минимум группу безопасности по умолчанию. Администраторы могут использовать Amazon Web Services Management Console, чтобы создавать дополнительные группы безопасности, настраивать порты для Microsoft Remote Desktop Protocol или SSH и виртуальные частные сети для Amazon VPN. Дополнительные сведения о создании и использовании групп безопасности в Amazon Web Services см. в документации Amazon.

Дополнительные сведения о подсистемах балансировки нагрузки см. в разделе *Настройка vRealize Automation*.

Необходимые условия

[Ввод данных о резервировании Amazon](#).

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Перечислены доступные области Amazon.

3. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.

4. В раскрывающемся меню **Пара ключей** выберите способ назначения пар ключей вычислительным экземплярам.

Параметр	Описание
Не указано	Управляет поведением пары ключей на уровне схемы элементов, а не на уровне резервирования.
Автоматически создаются для каждой бизнес-группы	Каждый компьютер, инициализированный в одной и той же бизнес-группе, имеет одинаковую пару ключей, включая компьютеры, инициализированные в других резервированиях, если он имеет одни и те же вычислительный ресурс и бизнес-группу. Так как пары ключей, созданные таким образом, связаны с бизнес-группой, они удаляются при удалении бизнес-группы.
Автоматически создаются для каждого компьютера	Уникальная пара ключей есть у каждого компьютера. Это наиболее безопасный метод, поскольку компьютеры не используют одинаковые пары ключей.
Специальная пара ключей	Каждый компьютер, инициализированный в этом резервировании, имеет одинаковую пару ключей. Найдите пару ключей, используемую для этого резервирования.

5. Если в раскрывающемся списке **Пара ключей** выбран пункт **Специальная пара ключей**, выберите значение пары ключей в раскрывающемся меню **Специальная пара ключей**.
6. Если у вас настроено виртуальное частное облако Amazon Virtual Private Cloud, установите флажок **Назначить в подсеть в VPC**. Если облако не настроено, не ставьте флажок.

Если установить флажок **Назначить в подсеть в VPC**, следующие расположения или подсети, группы безопасности и подсистемы балансировки нагрузки отобразятся во всплывающем меню, а не на этой странице.

В случае резервирования VPC укажите группы безопасности и подсети для каждого облака VPC, разрешенного в резервировании.

7. Выберите доступные расположения (вне VPC) или подсети (VPC) в списке **Расположения или Подсети**.

Выберите все доступные расположения или подсети, которые нужно сделать доступными для подготовки.

8. В списке **Группы безопасности** выберите одну или несколько групп безопасности, которые можно назначить компьютеру при инициализации.

Выберите все группы безопасности, которые можно назначить компьютеру во время подготовки. Для каждой доступной области следует указать как минимум одну группу безопасности.

9. В списке **Подсистемы балансировки нагрузки** выберите одну или несколько доступных подсистем балансировки нагрузки.

Если используется функция эластичной подсистемы балансировки нагрузки, выберите доступные подсистемы, применимые к выбранным расположениям или подсетям.

Результаты

Можно сохранить резервирование сейчас, нажав элемент **Сохранить**. Также можно добавить настраиваемые свойства для дополнительного контроля над спецификациями резервирования. Кроме того, можно настроить отправку уведомлений с оповещениями по электронной почте, если ресурсов, выделенных для этого резервирования, недостаточно.

Указание настраиваемых свойств и оповещений для резервирований Amazon

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Настраиваемые свойства и оповещения по электронной почте — необязательные настройки для резервирования. Если вам не нужно связывать настраиваемые свойства или настраивать предупреждения, щелкните **Сохранить**, чтобы завершить создание резервирования.

Вы можете добавить нужное количество настраиваемых свойств.

Если уведомления настроены, они создаются ежедневно, а не при достижении указанного порогового значения.

Важно! Оповещения отправляются, только если настроены уведомления по электронной почте и включены оповещения.

Необходимые условия

[Указание параметров ресурсов и сети для резервирований Amazon.](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Введите действительное имя настраиваемого свойства.
4. При необходимости введите значение свойства.
5. Нажмите кнопку **Сохранить**.
6. (дополнительно) Добавьте любые дополнительные настраиваемые свойства.
7. Перейдите на вкладку **Предупреждения**.
8. Установите флажок **Оповещения о емкости**, чтобы настроить отправку оповещений.
9. С помощью ползунка установите пороговые значения для распределения доступных ресурсов.

10. Введите в текстовом поле **Получатели** имена пользователей или групп AD (не электронные адреса), чтобы получать оповещения.

Вводите каждое имя в отдельной строке. Нажмите клавишу ВВОД, чтобы разделить несколько записей.

11. Выберите элемент **Отправлять оповещения диспетчеру групп**, чтобы включить диспетчеров групп в оповещения по электронной почте.

Эти оповещения отправляются по электронной почте пользователям, включенным в список бизнес-группы **Получатель эл. сообщений диспетчера**.

12. Укажите частоту напоминаний (дн.).

13. Нажмите кнопку **Сохранить**.

Результаты

Резервирование сохраняется и появляется в списке резервирований.

Следующие шаги

Можно настроить дополнительные политики резервирования или начать подготовку к инициализации.

Пользователи, авторизованные для создания схем элементов, могут создать их сейчас.

Создание резервирования OpenStack

Чтобы участники бизнес-группы могли запрашивать подготовку компьютеров, нужно выделить ресурсы компьютерам путем создания резервирования.

Создайте резервирование OpenStack.

Процедура

1. Указание информации о резервировании OpenStack

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

2. Указание ресурсов и параметров сети для резервирований OpenStack

Укажите параметры ресурсов и сети, доступные для компьютеров, которые подготавливаются на базе этого резервирования vRealize Automation.

3. Указание настраиваемых свойств и оповещений для резервирований OpenStack

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Указание информации о резервировании OpenStack

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.


Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- Убедитесь, что вычислительный ресурс существует.
- Убедитесь, что настроены необязательные группы безопасности и плавающие IP-адреса.
- Убедитесь, что существуют все требуемые пары ключей. См. раздел [Управление парами ключей](#).
- Убедитесь, что вычислительный ресурс существует.
- Настройте сеть.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Щелкните значок **Создать** () и выберите тип создаваемого резервирования.
Выберите **OpenStack**.
3. В текстовом поле **Имя** введите имя.
4. В раскрывающемся меню **Арендатор** выберите арендатора.
5. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.
Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.
6. (дополнительно) В раскрывающемся меню **Политика резервирования** выберите политику резервирования.
Для применения этого параметра требуется наличие одной или нескольких политик резервирования. Резервирование можно изменить позже, чтобы задать политику резервирования.
Политика резервирования используется для ограничения инициализации конкретными резервированиями.

7. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирование с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

8. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

Результаты

Не переходите никуда с этой страницы. Ваше резервирование не завершено.

Указание ресурсов и параметров сети для резервирований OpenStack

Укажите параметры ресурсов и сети, доступные для компьютеров, которые подготавливаются на базе этого резервирования vRealize Automation.

Необходимые условия

[Указание информации о резервировании OpenStack.](#)

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Для этого резервирования можно клонировать только шаблоны, расположенные в выбранном кластере.

Во время подготовки компьютеры размещаются на узле, подключенном к локальному хранилищу. Если при резервировании используется локальное хранилище, все компьютеры, которые подготовлены путем резервирования, создаются на узле, содержащем это локальное хранилище. Однако если используется настраиваемое свойство `VirtualMachine.Admin.ForceHost`, которое принудительно подготавливает компьютер на другом узле, подготовка завершается ошибкой. Подготовка также завершается ошибкой, если шаблон, из которого компьютер клонируется, находится в локальном хранилище, но подключен к компьютеру из другого кластера. В этом случае ошибка возникает из-за отсутствия доступа к шаблону.

3. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.

4. В раскрывающемся меню **Пара ключей** выберите способ назначения пар ключей вычислительным экземплярам.

Параметр	Описание
Не указано	Управляет поведением пары ключей на уровне схемы элементов, а не на уровне резервирования.
Автоматически создаются для каждой бизнес-группы	Каждый компьютер, инициализированный в одной и той же бизнес-группе, имеет одинаковую пару ключей, включая компьютеры, инициализированные в других резервированиях, если он имеет одни и те же вычислительный ресурс и бизнес-группу. Так как пары ключей, созданные таким образом, связаны с бизнес-группой, они удаляются при удалении бизнес-группы.
Автоматически создаются для каждого компьютера	Уникальная пара ключей есть у каждого компьютера. Это наиболее безопасный метод, поскольку компьютеры не используют одинаковые пары ключей.
Специальная пара ключей	Каждый компьютер, инициализированный в этом резервировании, имеет одинаковую пару ключей. Найдите пару ключей, используемую для этого резервирования.

5. Если в раскрывающемся списке **Пара ключей** выбран пункт **Специальная пара ключей**, выберите значение пары ключей в раскрывающемся меню **Специальная пара ключей**.
6. В списке **Группы безопасности** выберите одну или несколько групп безопасности, которые можно назначить компьютеру при инициализации.
7. Перейдите на вкладку **Сеть**.
8. Настройте сетевой путь для компьютеров, инициализированных с использованием этого резервирования.

- а) (дополнительно) Если параметр доступен, в раскрывающемся меню **Конечная точка** выберите конечную точку хранилища.

Параметр FlexClone отображается в столбце конечной точки, если конечная точка NetApp ONTAP существует и если используется виртуальный узел. Если конечная точка NetApp ONTAP существует, на странице резервирований отображается конечная точка, назначенная пути к хранилищу. При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается во всех соответствующих резервированиях.

При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается на странице резервирования.

- б) Выберите один или несколько **сетевых адаптеров** для компьютеров, которые нужно подготовить для этого резервирования.

- в) (дополнительно) Выберите доступный **профиль сети** для каждого выбранного сетевого адаптера.
- г) (дополнительно) Если доступны дополнительные настройки, выберите **транспортную зону** и один или несколько **логических маршрутизаторов уровня 0**, которые будут использоваться при развертывании схемы элементов, содержащей подсистемы балансировки нагрузки.

Транспортная зона определяет, какие кластеры могут охватывать сетевые адаптеры. Если транспортная зона указана в резервировании и схеме элементов, значения транспортной зоны должны совпадать.

Вы можете выбрать несколько сетевых адаптеров в резервировании, но при подготовке компьютера будет использоваться только одна сеть.

Результаты

Можно сохранить резервирование сейчас, нажав элемент **Сохранить**. Также можно добавить настраиваемые свойства для дополнительного контроля над спецификациями резервирования. Кроме того, можно настроить отправку уведомлений с оповещениями по электронной почте, если ресурсов, выделенных для этого резервирования, недостаточно.

Указание настраиваемых свойств и оповещений для резервирований OpenStack

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Настраиваемые свойства и оповещения по электронной почте — необязательные настройки для резервирования. Если вам не нужно связывать настраиваемые свойства или настраивать предупреждения, щелкните **Сохранить**, чтобы завершить создание резервирования.

Вы можете добавить нужное количество настраиваемых свойств.

Важно! Оповещения отправляются, только если настроены уведомления по электронной почте и включены оповещения.

Если уведомления настроены, они создаются ежедневно, а не при достижении указанного порогового значения.

Необходимые условия

[Указание ресурсов и параметров сети для резервирований OpenStack.](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Введите действительное имя настраиваемого свойства.
4. При необходимости введите значение свойства.
5. Нажмите кнопку **Сохранить**.
6. (дополнительно) Добавьте любые дополнительные настраиваемые свойства.

7. Перейдите на вкладку **Предупреждения**.
8. Установите флажок **Оповещения о емкости**, чтобы настроить отправку оповещений.
9. С помощью ползунка установите пороговые значения для распределения доступных ресурсов.
10. Введите в текстовом поле **Получатели** имена пользователей или групп AD (не электронные адреса), чтобы получать оповещения.

Вводите каждое имя в отдельной строке. Нажмите клавишу ВВОД, чтобы разделить несколько записей.

11. Выберите элемент **Отправлять оповещения диспетчеру групп**, чтобы включить диспетчеров групп в оповещения по электронной почте.

Эти оповещения отправляются по электронной почте пользователям, включенным в список бизнес-группы **Получатель эл. сообщений диспетчера**.

12. Укажите частоту напоминаний (дн.).
13. Нажмите кнопку **Сохранить**.

Результаты

Резервирование сохраняется и появляется в списке резервирований.

Следующие шаги

Можно настроить дополнительные политики резервирования или начать подготовку к инициализации.

Пользователи, авторизованные для создания схем элементов, могут создать их сейчас.

Создание резервирования vCloud Air

Чтобы участники бизнес-группы могли запрашивать подготовку компьютеров, нужно выделить ресурсы компьютерам путем создания резервирования vRealize Automation.

У каждой бизнес-группы должно быть по крайней мере одно резервирование, чтобы ее участники могли подготавливать компьютеры этого типа.

Процедура

1. Ввод информации о резервировании vCloud Air

Можно создать резервирование для каждой подписки на компьютер vCloud Air или каждого ресурса, предоставляемого по требованию. Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры.

2. Указание ресурсов и параметров сети для резервирования vCloud Air

Укажите параметры ресурсов и сети, доступные для компьютеров vCloud Air, которые подготавливаются на базе этого резервирования vRealize Automation.

3. Указание настраиваемых свойств и оповещений для резервирования vCloud Air

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Ввод информации о резервировании vCloud Air

Можно создать резервирование для каждой подписки на компьютер vCloud Air или каждого ресурса, предоставляемого по требованию. Каждое резервирование настроено для определенной бизнес-группы, которой оно даст возможность запрашивать компьютеры.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- Убедитесь, что вычислительный ресурс существует.
- Настройте сеть.
- (дополнительно) Настройте сведения о профиле сети.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.

2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.

Доступны такие типы облачного резервирования: Amazon, OpenStack, vCloud Air и vCloud Director.

Выберите **vCloud Air**.

3. В текстовом поле **Имя** введите имя.
4. В раскрывающемся меню **Арендатор** выберите арендатора.
5. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.

Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.

6. (дополнительно) В раскрывающемся меню **Политика резервирования** выберите политику резервирования.

Для применения этого параметра требуется наличие одной или нескольких политик резервирования. Резервирование можно изменить позже, чтобы задать политику резервирования.

Политика резервирования используется для ограничения инициализации конкретными резервированиями.

7. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирования с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

8. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

Результаты

Не переходите никуда с этой страницы. Ваше резервирование не завершено.

Указание ресурсов и параметров сети для резервирования vCloud Air

Укажите параметры ресурсов и сети, доступные для компьютеров vCloud Air, которые подготавливаются на базе этого резервирования vRealize Automation.

Доступные модели выделения ресурсов для компьютеров, подготовленных на базе резервирования vCloud Director — это пул выделений, оплата по факту использования и пул резервирования. Для модели «оплата по факту использования» не нужно указывать объемы памяти или хранилища, но нужно указать приоритет для пути хранилища. Сведения об этих моделях выделения см. в документации по vCloud Air.

Можно задать стандартный профиль хранилища или профиль хранилища на уровне дисков. Для конечных точек vCloud Air доступно многоуровневое дисковое хранилище.

Для интеграции, при которой используются хранилища с технологией Distributed Resource Scheduler (SDRS), можно выбрать кластер хранилища, чтобы разрешить SDRS автоматически выполнять размещение в хранилище и балансировку нагрузки для компьютеров, подготовленных из этого резервирования. Для режима автоматизации SDRS должен быть установлен параметр «Автоматически». В ином случае необходимо выбрать хранилище данных в кластере для автономного режима работы хранилища данных. Устройства хранения FlexClone не поддерживают SDRS.

Примечание Резервирования, определенные для конечных точек vCloud Air и конечных точек vCloud Director, не поддерживают использование профилей сети для подготавливаемых компьютеров.

Необходимые условия

[Ввод информации о резервировании vCloud Director](#).

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Для этого резервирования можно клонировать только шаблоны, расположенные в выбранном кластере.
3. Выберите модель выделения.
4. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.

5. В таблице «Память» укажите количество гигабайтов памяти, выделяемых для этого резервирования.

Общий объем памяти для резервирования зависит от выбранных вычислительных ресурсов.

6. Выберите один или несколько из перечисленных путей к хранилищам.

Доступные варианты пути к хранилищу зависят от выбранных вычислительных ресурсов.

- а) Чтобы указать объем памяти, выделяемый для этого резервирования, введите значение в текстовом поле **Это резервирование зарезервировано**.
- б) Чтобы указать значение приоритета для пути к хранилищу относительно других путей к хранилищам, которые относятся к этому резервированию, введите значение в текстовом поле **Приоритет**.

Приоритет используется для нескольких путей к хранилищам. Сначала используется путь к хранилищу с приоритетом 0, а затем — с приоритетом 1.

- в) Если не нужно включать путь к хранилищу, используемый этим резервированием, щелкните параметр **Отключить**.
- г) Повторите этот шаг, чтобы настроить кластеры и хранилища данных, если это необходимо.

7. Перейдите на вкладку **Сеть**.

8. Настройте сетевой путь для компьютеров, инициализированных с использованием этого резервирования.

- а) (дополнительно) Если параметр доступен, в раскрывающемся меню **Конечная точка** выберите конечную точку хранилища.

Параметр FlexClone отображается в столбце конечной точки, если конечная точка NetApp ONTAP существует и если используется виртуальный узел. Если конечная точка NetApp ONTAP существует, на странице резервирований отображается конечная точка, назначенная пути к хранилищу. При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается во всех соответствующих резервированиях.

При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается на странице резервирования.

- б) Выберите один или несколько **сетевых адаптеров** для компьютеров, которые нужно подготовить для этого резервирования.
- в) (дополнительно) Выберите доступный **профиль сети** для каждого выбранного сетевого адаптера.
- г) (дополнительно) Если доступны дополнительные настройки, выберите **транспортную зону** и один или несколько **логических маршрутизаторов уровня 0**, которые будут использоваться при развертывании схемы элементов, содержащей подсистемы балансировки нагрузки.

Транспортная зона определяет, какие кластеры могут охватывать сетевые адаптеры. Если транспортная зона указана в резервировании и схеме элементов, значения транспортной зоны должны совпадать.

Вы можете выбрать несколько сетевых адаптеров в резервировании, но при подготовке компьютера будет использоваться только одна сеть.

Результаты

Можно сохранить резервирование сейчас, нажав элемент **Сохранить**. Также можно добавить настраиваемые свойства для дополнительного контроля над спецификациями резервирования. Кроме того, можно настроить отправку уведомлений с оповещениями по электронной почте, если ресурсов, выделенных для этого резервирования, недостаточно.

Указание настраиваемых свойств и оповещений для резервирования vCloud Air

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Настраиваемые свойства и оповещения по электронной почте — необязательные настройки для резервирования. Если вам не нужно связывать настраиваемые свойства или настраивать предупреждения, щелкните **Сохранить**, чтобы завершить создание резервирования.

Вы можете добавить нужное количество настраиваемых свойств.

Если уведомления настроены, они создаются ежедневно, а не при достижении указанного порогового значения.

Важно! Оповещения отправляются, только если настроены уведомления по электронной почте и включены оповещения.

Уведомления недоступны для резервирований с повременной оплатой, которые были созданы без каких-либо установленных пределов.

Необходимые условия

[Указание ресурсов и параметров сети для резервирования vCloud Air](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Введите действительное имя настраиваемого свойства.
4. При необходимости введите значение свойства.
5. (дополнительно) Установите флажок **Зашифровано**, чтобы зашифровать значение свойства.
6. (дополнительно) Установите флажок **Запросить пользователя**, чтобы пользователю отображался запрос на ввод значения.

Этот параметр нельзя переопределить во время подготовки.

7. Нажмите кнопку **Сохранить**.
8. (дополнительно) Добавьте любые дополнительные настраиваемые свойства.
9. Перейдите на вкладку **Предупреждения**.
10. Установите флажок **Оповещения о емкости**, чтобы настроить отправку оповещений.

11. С помощью ползунка установите пороговые значения для распределения доступных ресурсов.
12. Введите в текстовом поле **Получатели** имена пользователей или групп AD (не электронные адреса), чтобы получать оповещения.

Вводите каждое имя в отдельной строке. Нажмите клавишу ВВОД, чтобы разделить несколько записей.
13. Выберите элемент **Отправлять оповещения диспетчеру групп**, чтобы включить диспетчеров групп в оповещения по электронной почте.

Эти оповещения отправляются по электронной почте пользователям, включенным в список бизнес-группы **Получатель эл. сообщений диспетчера**.
14. Укажите частоту напоминаний (дн.).
15. Нажмите кнопку **Сохранить**.

Результаты

Резервирование сохраняется и появляется в списке резервирований.

Создание резервирования vCloud Director

Чтобы участники бизнес-группы могли запрашивать подготовку компьютеров, нужно выделить ресурсы компьютерам путем создания резервирования vRealize Automation.

У каждой бизнес-группы должно быть по крайней мере одно резервирование, чтобы ее участники могли подготавливать компьютеры этого типа.

Процедура

1. Ввод информации о резервировании vCloud Director

Можно создать резервирование для каждого виртуального центра обработки данных (VDC) организации vCloud Director. Каждое резервирование настроено для определенной бизнес-группы, которой оно даст возможность запрашивать компьютеры в указанном вычислительном ресурсе.

2. Указание ресурсов и параметров сети для резервирования vCloud Director

Укажите параметры ресурсов и сети, доступные для компьютеров vCloud Director, которые подготавливаются на базе этого резервирования vRealize Automation.

3. Указание настраиваемых свойств и оповещений для резервирований vCloud Director

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Следующие шаги

Можно настроить дополнительные политики резервирования или начать подготовку к инициализации.

Пользователи, авторизованные для создания схем элементов, могут создать их сейчас.

Ввод информации о резервировании vCloud Director

Можно создать резервирование для каждого виртуального центра обработки данных (VDC) организации vCloud Director. Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- Убедитесь, что вычислительный ресурс существует.
- Настройте сеть.
- (дополнительно) Настройте сведения о профиле сети.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.

2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.

Доступны такие типы облачного резервирования: Amazon, OpenStack, vCloud Air и vCloud Director.

Выберите **vCloud Director**.

3. В текстовом поле **Имя** введите имя.
4. В раскрывающемся меню **Арендатор** выберите арендатора.
5. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.

Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.

6. (дополнительно) В раскрывающемся меню **Политика резервирования** выберите политику резервирования.

Для применения этого параметра требуется наличие одной или нескольких политик резервирования. Резервирование можно изменить позже, чтобы задать политику резервирования.

Политика резервирования используется для ограничения инициализации конкретными резервированиями.

7. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирования с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

8. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

Результаты

Не переходите никуда с этой страницы. Ваше резервирование не завершено.

Указание ресурсов и параметров сети для резервирования vCloud Director

Укажите параметры ресурсов и сети, доступные для компьютеров vCloud Director, которые подготавливаются на базе этого резервирования vRealize Automation.

Доступные модели выделения ресурсов для компьютеров, подготовленных на базе резервирования vCloud Director — это пул выделений, оплата по факту использования и пул резервирования. Для модели «оплата по факту использования» не нужно указывать объемы памяти или хранилища, но нужно указать приоритет для пути хранилища. Сведения об этих моделях выделения см. в документации по vCloud Director.

Можно задать стандартный профиль хранилища или профиль хранилища на уровне дисков.

Многоуровневое дисковое хранилище доступно для конечных точек vCloud Director 5.6 и более поздних версий. Многоуровневое дисковое хранилище не поддерживается для конечных точек vCloud Director 5.5.

Для интеграции, при которой используются хранилища с технологией Distributed Resource Scheduler (SDRS), можно выбрать кластер хранилища, чтобы разрешить SDRS автоматически выполнять размещение в хранилище и балансировку нагрузки для компьютеров, подготовленных из этого резервирования. Для режима автоматизации SDRS должен быть установлен параметр «Автоматически». В ином случае необходимо выбрать хранилище данных в кластере для автономного режима работы хранилища данных. Устройства хранения FlexClone не поддерживают SDRS.

Примечание Резервирования, определенные для конечных точек vCloud Air и конечных точек vCloud Director, не поддерживают использование профилей сети для подготавливаемых компьютеров.

Необходимые условия

[Ввод информации о резервировании vCloud Director.](#)

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Для этого резервирования можно клонировать только шаблоны, расположенные в выбранном кластере.
3. Выберите модель выделения.

4. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.

5. В таблице «Память» укажите количество гигабайтов памяти, выделяемых для этого резервирования.

Общий объем памяти для резервирования зависит от выбранных вычислительных ресурсов.

6. Выберите один или несколько из перечисленных путей к хранилищам.

Доступные варианты пути к хранилищу зависят от выбранных вычислительных ресурсов.

- а) Чтобы указать объем памяти, выделяемый для этого резервирования, введите значение в текстовом поле **Это резервирование зарезервировано**.
- б) Чтобы указать значение приоритета для пути к хранилищу относительно других путей к хранилищам, которые относятся к этому резервированию, введите значение в текстовом поле **Приоритет**.

Приоритет используется для нескольких путей к хранилищам. Сначала используется путь к хранилищу с приоритетом 0, а затем — с приоритетом 1.

- в) Если не нужно включать путь к хранилищу, используемый этим резервированием, щелкните параметр **Отключить**.

- г) Повторите этот шаг, чтобы настроить кластеры и хранилища данных, если это необходимо.

7. Перейдите на вкладку **Сеть**.

8. Настройте сетевой путь для компьютеров, инициализированных с использованием этого резервирования.

- а) (дополнительно) Если параметр доступен, в раскрывающемся меню **Конечная точка** выберите конечную точку хранилища.

Параметр FlexClone отображается в столбце конечной точки, если конечная точка NetApp ONTAP существует и если используется виртуальный узел. Если конечная точка NetApp ONTAP существует, на странице резервирований отображается конечная точка, назначенная пути к хранилищу. При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается во всех соответствующих резервированиях.

При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается на странице резервирования.

- б) Выберите один или несколько **сетевых адаптеров** для компьютеров, которые нужно подготовить для этого резервирования.

- в) (дополнительно) Выберите доступный **профиль сети** для каждого выбранного сетевого адаптера.
- г) (дополнительно) Если доступны дополнительные настройки, выберите **транспортную зону** и один или несколько **логических маршрутизаторов уровня 0**, которые будут использоваться при развертывании схемы элементов, содержащей подсистемы балансировки нагрузки.

Транспортная зона определяет, какие кластеры могут охватывать сетевые адаптеры. Если транспортная зона указана в резервировании и схеме элементов, значения транспортной зоны должны совпадать.

Вы можете выбрать несколько сетевых адаптеров в резервировании, но при подготовке компьютера будет использоваться только одна сеть.

Результаты

Можно сохранить резервирование сейчас, нажав элемент **Сохранить**. Также можно добавить настраиваемые свойства для дополнительного контроля над спецификациями резервирования. Кроме того, можно настроить отправку уведомлений с оповещениями по электронной почте, если ресурсов, выделенных для этого резервирования, недостаточно.

Указание настраиваемых свойств и оповещений для резервирований vCloud Director

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Настраиваемые свойства и оповещения по электронной почте — необязательные настройки для резервирования. Если вам не нужно связывать настраиваемые свойства или настраивать предупреждения, щелкните **Сохранить**, чтобы завершить создание резервирования.

Вы можете добавить нужное количество настраиваемых свойств.

Если уведомления настроены, они создаются ежедневно, а не при достижении указанного порогового значения.

Важно! Оповещения отправляются, только если настроены уведомления по электронной почте и включены оповещения.

Уведомления недоступны для резервирований с повременной оплатой, которые были созданы без каких-либо установленных пределов.

Необходимые условия

[Указание ресурсов и параметров сети для резервирования vCloud Director.](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Введите действительное имя настраиваемого свойства.
4. При необходимости введите значение свойства.

5. (дополнительно) Установите флажок **Зашифровано**, чтобы зашифровать значение свойства.
6. (дополнительно) Установите флажок **Запросить пользователя**, чтобы пользователю отображался запрос на ввод значения.
Этот параметр нельзя переопределить во время подготовки.
7. Нажмите кнопку **Сохранить**.
8. (дополнительно) Добавьте любые дополнительные настраиваемые свойства.
9. Перейдите на вкладку **Предупреждения**.
10. Установите флажок **Оповещения о емкости**, чтобы настроить отправку оповещений.
11. С помощью ползунка установите пороговые значения для распределения доступных ресурсов.
12. Введите в текстовом поле **Получатели** имена пользователей или групп AD (не электронные адреса), чтобы получать оповещения.
Вводите каждое имя в отдельной строке. Нажмите клавишу ВВОД, чтобы разделить несколько записей.
13. Выберите элемент **Отправлять оповещения диспетчеру групп**, чтобы включить диспетчеров групп в оповещения по электронной почте.
Эти оповещения отправляются по электронной почте пользователям, включенным в список бизнес-группы **Получатель эл. сообщений диспетчера**.
14. Укажите частоту напоминаний (дн.).
15. Нажмите кнопку **Сохранить**.

Результаты

Резервирование сохраняется и появляется в списке резервирований.

Создание резервирования для Microsoft Azure

Создайте резервирование Azure для конкретной бизнес-группы, чтобы дать пользователям в этой группе возможность запрашивать виртуальные машины Azure на заданном вычислительном ресурсе.

Если в развертывании поддерживается единый вход через VPN-туннель, поддержку этой функции можно настроить с помощью виртуальных машин Azure, используя параметры на вкладке «Свойства».

Примечание При создании резервирования Azure игнорируйте вкладку «Предупреждения», так как она не применяется. После создания резервирования нельзя изменить связи с бизнес-группами. Кроме того, в отличие от других типов компьютеров, между резервированием Azure и схемой элементов нет прямой связи.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- (дополнительно) Настройте сведения о профиле сети.
- Убедитесь, что у вас есть доступ к любым необходимым ресурсам Azure.
- Убедитесь, что существуют все требуемые пары ключей. Сведения о парах ключей см. в разделе *Настройка vRealize Automation*.
- Получите действующий идентификатор подписки Azure, совпадающий с тем, который используется с соответствующей конечной точкой Azure. Если используется несколько подписок Azure, необходимо создать резервирование для каждой подписки.
- Если в развертывании поддерживается единый вход через VPN-туннель, то перед созданием резервирования необходимо настроить соответствующее подключение к VPC. См. раздел [Настройка подключения VPC «сеть к Azure»](#).

Процедура

1. [Настройка основных сведений о резервировании Microsoft Azure](#)

Укажите основные сведения для резервирования Microsoft Azure.

2. [Указание сведений о ресурсах для резервирования Azure](#)

При настройке резервирования Azure можно указать группу ресурсов и учетную запись хранения на основе используемого экземпляра Azure. Во время настройки резервирования алгоритм подготовки vRealize Automation запускает выделение ресурсов, например групп ресурсов и учетных записей хранения, в соответствии с информацией о ресурсах, заданной на основе резервирования в процессе подготовки виртуальной машины.

3. [Настройка свойств Azure](#)

Можно добавить настраиваемые свойства для резервирования Azure, чтобы обеспечить поддержку таких параметров, как туннелирование VPN, которое позволяет осуществлять обмен данными между несколькими сетями. Эта функция также упрощает добавление компонентов программного обеспечения в схемы элементов.

4. [Указание сведений о сети для резервирования Azure](#)

Для виртуальной машины Azure, заданной в резервировании, можно указать сведения о виртуальной сети и средстве балансировки нагрузки.

Настройка основных сведений о резервировании Microsoft Azure

Укажите основные сведения для резервирования Microsoft Azure.

Все сведения на странице «Сведения о резервировании» являются обязательными, кроме политики резервирования. Все сведения на последующих страницах резервирования Azure необязательные.

Процедура

1. Выберите элементы **Инфраструктура > Администрирование > Резервирования**.

2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.

Выберите **Azure**.

3. В текстовом поле **Имя** введите имя.

4. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.

Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.

5. Не обращайте внимания на текстовое поле **Политика резервирования**, так как оно не относится к резервированиям Azure.

6. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирование с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

7. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

8. Нажмите кнопку **ОК**.

Указание сведений о ресурсах для резервирования Azure

При настройке резервирования Azure можно указать группу ресурсов и учетную запись хранения на основе используемого экземпляра Azure. Во время настройки резервирования алгоритм подготовки vRealize Automation запускает выделение ресурсов, например групп ресурсов и учетных записей хранения, в соответствии с информацией о ресурсах, заданной на основе резервирования в процессе подготовки виртуальной машины.

Можно указать в резервировании информацию о группе ресурсов и учетной записи хранения для виртуальной машины Azure, а можно оставить эти поля пустыми. Если оставить поля пустыми, для всех соответствующих схем элементов будут использоваться заданные по умолчанию сведения о группе ресурсов и учетной записи хранения, относящиеся к данному идентификатору подписки Azure. Эту информацию можно указать также при создании схемы элементов или при подготовке виртуальной машины.

Необходимые условия

Получите идентификатор подписки для своего экземпляра Azure.

Процедура

1. Введите свой идентификатор подписки Azure в текстовом поле **Идентификатор подписки**.
2. Выберите расположение для резервирования, щелкнув раскрывающийся список **Расположение**.

Это поле можно оставить пустым для создания резервирования независимо от расположения, однако в этом случае информацию о расположении необходимо указать либо при создании схемы элементов, либо при подготовке виртуальной машины Azure.

3. Щелкните элемент **Создать в таблице групп ресурсов.**

- а) Введите в текстовом поле **Имя** нужное имя группы ресурсов из вашего экземпляра Azure.

Примечание Поле **Имя** не может быть пустым.

- б) Задайте числовое значение приоритета в текстовом поле **Приоритет**.

Это значение определяет приоритет, когда используется больше одной группы ресурсов. Чем меньше число, тем выше приоритет.

- в) Щелкните элемент **Сохранить**, чтобы добавить группу ресурсов к резервированию.

4. Щелкните элемент **Создать в таблице учетных записей хранения.**

- а) Введите в текстовом поле **Имя** нужное имя учетной записи хранения из вашего экземпляра Azure.

Примечание Поле **Имя** не может быть пустым.

- б) Задайте числовое значение приоритета в текстовом поле **Приоритет**.

- в) Щелкните элемент **Сохранить**, чтобы добавить учетную запись хранения к резервированию.

Это значение определяет приоритет, когда для резервирования используется больше одной учетной записи хранения. Чем меньше число, тем выше приоритет.

5. Нажмите кнопку **ОК, чтобы перейти к следующей вкладке.****Настройка свойств Azure**

Можно добавить настраиваемые свойства для резервирования Azure, чтобы обеспечить поддержку таких параметров, как туннелирование VPN, которое позволяет осуществлять обмен данными между несколькими сетями. Эта функция также упрощает добавление компонентов программного обеспечения в схемы элементов.

Необходимо создать настраиваемые свойства, которые определяют соответствующие URL-адреса для поддержки туннелирования VPN в сети. Кроме того, необходимо создать свойства, определяющие путь к загруженным ранее сценариям конфигурации туннелирования Azure.

Используйте частный IP-адрес физического компьютера с туннельным подключением Azure и порт 1443, назначенный для *vRealize_automation_appliance_fqdn*, при вызове SSH-туннеля.

В следующей таблице представлены имена и значения свойств, необходимых для поддержки туннелирования VPN.

Имя	Значение
Azure.Windows.ScriptPath	Указывает путь к загруженному сценарию, который используется для настройки туннелирования в системах на базе Windows. Измените этот путь, как это требуется для вашего развертывания.
Azure.Linux.ScriptPath	Указывает путь к загруженному сценарию, который используется для настройки туннелирования в системах на базе Linux. Измените этот путь, как это требуется для вашего развертывания.

Имя	Значение
agent.download.url	Указывает URL-адрес для агента VPN вашего развертывания. Формат URL-адреса имеет вид <code>https:// Внутренний_IP-адрес:1443/software-service//resources/noble-agent.jar</code>
software.agent.service.url	Укажите URL-адрес службы агента программного обеспечения VPN для развертывания. Формат URL-адреса: <code>https:// Private_IP:1443/software-service/api</code>
software.ebs.url	Укажите URL-адрес брокера событий для развертывания. Формат URL-адреса: <code>https:// Private_IP:1443/event-broker-service/api</code>

Необходимые условия

- Загрузите предоставляемые VMware сценарии Azure на странице **Программы установки компонентов «Гостевой агент» и «Программный агент»** на устройстве vRealize Automation.
Эти сценарии выполняют установку расширений Azure, требуемых для поддержки туннелирования VPN. Доступно два сценария: `script.ps1` и `script.sh`. Файл с расширением `.ps1` предназначен для ОС Windows, а файл с расширением `.sh` — для ОС Linux.
 - а) Перейдите на веб-страницу `https://vrealize-automation-appliance-fqdn/software`, чтобы открыть страницу устройства VMware vRealize Automation.
 - б) Перейдите по ссылке **Компоненты «Гостевой агент» и «Программный агент»** под заголовком «Установка компонентов vRealize Automation («Инфраструктура как услуга», «Гостевые и программные агенты», «Инструменты»).
 - в) Загрузите файлы сценариев Azure под заголовком «Компьютеры Azure». Сохраните файлы сценариев в соответствующей папке. Выбранную для сохранения папку необходимо указать при задании настраиваемых свойств резервирования Azure.

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Укажите соответствующее имя и значение для настраиваемого свойства в диалоговом окне «Свойства».
4. После создания каждого свойства необходимо нажать **ОК** в диалоговом окне соответствующего свойства.
5. После добавления всех обязательных свойств нажмите **ОК**, чтобы сохранить настройки.

Следующие шаги

После создания настраиваемых свойств для поддержки туннелирования VPN можно создать программные компоненты для схем элементов Azure. Дополнительные сведения см. в разделе *Настройка vRealize Automation*.

При настройке компонента программного обеспечения для Azure выберите **Виртуальная машина Azure** в раскрывающемся меню «Контейнер» на странице «Создать программное обеспечение».

Указание сведений о сети для резервирования Azure

Для виртуальной машины Azure, заданной в резервировании, можно указать сведения о виртуальной сети и средстве балансировки нагрузки.

Эту страницу можно оставить частично или полностью пустой и указать сведения о виртуальной сети и средстве балансировки нагрузки при подготовке виртуальной машины.

Если указать профиль сети и не указать подсеть, то в качестве имени подсети будет использовано имя первого из имеющихся диапазонов сети в указанном профиле. Если профиль сети указан, то можно оставить текстовое поле «Виртуальная сеть» пустым. В этом случае в качестве имени подсети будет использовано имя первого из имеющихся диапазонов сети в указанном профиле, а в качестве имени виртуальной сети — имя первой виртуальной сети Azure, которая содержит соответствующую подсеть.

Необходимые условия

Получите соответствующие сведения о виртуальной сети и средстве балансировки нагрузки из экземпляра Azure (если есть).

Процедура

1. Щелкните элемент **Создать** в таблице сетей, чтобы настроить соответствующую виртуальную сеть Azure для использования на своей виртуальной машине.

- а) Вставьте в текстовое поле **Виртуальная сеть** необходимое имя виртуальной сети из экземпляра Azure.

- б) Вставьте в текстовое поле **Подсеть** необходимое имя подсети из экземпляра Azure.

Задать подсеть можно по желанию. Если оставить это поле пустым, по умолчанию будет использована подсеть указанной виртуальной сети.

- в) Введите или вставьте необходимое имя в текстовое поле **Профиль сети**. Можно использовать профиль сети из схемы элементов, чтобы связать сетевой адаптер с сетью.

Задать профиль сети можно по желанию. Используйте этот параметр, если необходимо создать схему элементов на основе профиля сети, заданного в vRealize Automation, а не привязывать ее к сетевой конструкции Azure.

- г) При необходимости задайте числовое значение приоритета в текстовом поле **Приоритет**.

Это значение определяет приоритет, когда для виртуальной сети используется несколько резервирований. Чем меньше число, тем выше приоритет.

- д) Щелкните элемент **Сохранить**, чтобы добавить группу ресурсов к резервированию.

2. Щелкните элемент **Создать** в таблице средств балансировки нагрузки, если вы развертываете несколько компьютеров и используете средство балансировки нагрузки.

- а) Вставьте в текстовое поле **Имя** необходимое имя средства балансировки нагрузки из экземпляра Azure.
- б) Вставьте в текстовое поле **Пул внутренних адресов** необходимое имя из экземпляра Azure.
- в) При необходимости задайте числовое значение приоритета в текстовом поле **Приоритет**.
Это значение определяет приоритет, когда для виртуальной сети используется несколько средств балансировки нагрузки. Чем меньше число, тем выше приоритет.
- г) Щелкните элемент **Сохранить**, чтобы добавить средство балансировки нагрузки к резервированию.

3. Щелкните элемент **Создать** в таблице групп безопасности, если вы развертываете несколько компьютеров, которые должны связываться друг с другом через брандмауэр.

- а) Вставьте в текстовое поле **Имя** необходимое имя группы безопасности из экземпляра Azure.
- б) При необходимости задайте числовое значение приоритета в текстовом поле **Приоритет**.
Это значение определяет приоритет, когда для виртуальной сети используется несколько групп безопасности. Чем меньше число, тем выше приоритет.
- в) Щелкните элемент **Сохранить**, чтобы добавить группу безопасности к резервированию.

4. Нажмите кнопку **ОК**.

Сценарий: создание резервирования Amazon для экспериментальной среды

Для того чтобы обеспечить обмен информацией для агента начальной загрузки Программное обеспечение и гостевого агента через туннель при использовали SSH-туннеля для временного подключения сети экспериментальной среды к Amazon VPC, нужно добавить настраиваемые свойства в резервирования Amazon.

Подключение сети к Amazon VPC потребуется только тогда, когда нужно использовать гостевой агент для настройки подготовленных компьютеров или когда нужно включить в схемы элементов компоненты Программное обеспечение. Для производственной среды нужно настроить это подключение официально через Amazon Web Services, однако при работе в экспериментальной среде допускается вместо этого настроить временный SSH-туннель.

Используя права администратора структуры, можно создать резервирование для выделения ресурсов Amazon Web Services и добавить нескольких настраиваемых свойств для поддержки туннелирования SSH. Также нужно настроить резервирование в той же области и VPC, что и компьютер с туннельным подключением.

Необходимые условия

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

- Для установления соединения сети к Amazon VPC настройте SSH туннель. Запишите подсеть, группу безопасности и частный IP-адрес компьютера Amazon Web Services с туннельным подключением. См. раздел [Настройка подключения между сетью и Amazon VPC для среды демонстрационной установки](#).
- Создайте бизнес-группу для членов вашей ИТ-организации, которым нужно разрабатывать схемы элементов в экспериментальной среде. См. раздел [Создание бизнес-группы](#).
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.

Процедура

1. [Сценарий: указание данных о резервировании Amazon Web Services для экспериментальной среды](#)
Резервирование ресурсов для команды разработчиков схем элементов, чтобы они могли проверить функциональность в экспериментальной среде, поэтому это резервирование будет настроено на выделение ресурсов для бизнес-группы разработчиков.
2. [Сценарий: настройка параметров сети Amazon Web Services для экспериментальной среды](#)
Производится настройка резервирования, чтобы оно использовало ту же область и сетевые настройки, что и компьютер с туннельным подключением, и ограничивается количество компьютеров, которые могут быть включены в данное резервирование для управления использованием ресурсов.
3. [Сценарий: изменение настраиваемых свойств для запуска обмена данными с агентом через туннельное подключение](#)
После настройки подключения сети к Amazon VPC было настроено перенаправление портов, чтобы компьютер с туннельным подключением Amazon Web Services имел доступ к ресурсам vRealize Automation.

Сценарий: указание данных о резервировании Amazon Web Services для экспериментальной среды
Резервирование ресурсов для команды разработчиков схем элементов, чтобы они могли проверить функциональность в экспериментальной среде, поэтому это резервирование будет настроено на выделение ресурсов для бизнес-группы разработчиков.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.
Выберите **Amazon**.
3. В текстовом поле **Имя** введите **Amazon Tunnel POC**.
4. Из раскрывающегося меню **Бизнес-группа** выберите бизнес-группу, созданную для разработчиков схем элементов.
5. Введите **1** в текстовое поле **Приоритет**, чтобы настроить это резервирование с наивысшим приоритетом.

Результаты

Бизнес-группа и приоритет для резервирования настроены, осталось распределить ресурсы и изменить настраиваемые свойства для SSH-туннеля.

Сценарий: настройка параметров сети Amazon Web Services для экспериментальной среды
Производится настройка резервирования, чтобы оно использовало ту же область и сетевые настройки, что и компьютер с туннельным подключением, и ограничивается количество компьютеров, которые могут быть включены в данное резервирование для управления использованием ресурсов.

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Выберите область Amazon Web Services, в которой находится компьютер с туннельным подключением.
3. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.
4. Выберите **Указать пару ключей** в раскрывающемся меню **Пара ключей**.

Так как настраивается экспериментальная среда, то можно использовать одну пару ключей для всех подготовленных с использованием данного резервирования компьютеров.
5. Из раскрывающегося меню **Пара ключей** выберите пару ключей, которая будет совместно использоваться с другими разработчиками архитектуры.
6. Установите флажок **Назначить в подсеть в VPC**.
7. Выберите ту же подсеть и группы безопасности, что и на компьютере с туннельным подключением.

Результаты

Теперь резервирование будет использовать ту же область и сетевые настройки, что и компьютер с туннельным подключением, однако еще нужно добавить настраиваемые свойства для обеспечения обмена данными между агентом начальной загрузки Программное обеспечение и гостевым агентом через туннель.

Сценарий: изменение настраиваемых свойств для запуска обмена данными с агентом через туннельное подключение

После настройки подключения сети к Amazon VPC было настроено перенаправление портов, чтобы компьютер с туннельным подключением Amazon Web Services имел доступ к ресурсам vRealize Automation.

Чтобы настроить доступ агентов к этим портам, необходимо добавить настраиваемые свойства туннеля в резервирование.

Примечание Если между корпоративной сетью и сетью vRealize Automation используется сеть системы PAT или NAT, можно применить эти свойства, чтобы получить доступ к частному IP-адресу и порту.

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Изменение настраиваемых свойств туннеля.

Используйте частный IP-адрес компьютера с туннельным подключением Amazon Web Services и порт 1443, назначенный для *vRealize_appliance_fqdn* при вызове SSH-туннеля.

Параметр	Значение
<code>software.ebs.url</code>	<code>https://Private_IP:1443/event-broker-service/api</code>
<code>software.agent.service.url</code>	<code>https://Private_IP:1443/software-service/api</code>
<code>agent.download.url</code>	<code>https://Private_IP:1443/software-service/resources/nobel-agent.jar</code>

4. Нажмите кнопку **Сохранить**.

Результаты

Создано резервирование для выделения ресурсов Amazon Web Services для бизнес-группы разработчиков. Резервирование настроено для поддержки гостевого агента и агента начальной загрузки Программное обеспечение. Разработчики могут создавать схемы элементов, которые используют гостевой агент для настройки развернутых компьютеров или включают компоненты Программное обеспечение.

Создание виртуальных резервирований категорий

Виртуальное резервирование типов категорий предоставляет доступ к службам подготовки развертывания виртуальных машин для определенной бизнес-группы vRealize Automation. Доступны такие типы виртуального резервирования: vSphere, Hyper-V, KVM, SCVMM и XenServer.

Резервирование — это совместное использование ресурсов памяти, ЦП, сети и хранилища одного вычислительного ресурса, выделенного для определенной бизнес-группы vRealize Automation.

У бизнес-группы может быть несколько резервирований на одной конечной точке или на нескольких.

Для подготовки виртуальных машин у бизнес-группы должно быть по крайней мере одно резервирование в виртуальном вычислительном ресурсе. Каждое резервирование предназначено только для одной бизнес-группы, но у группы может быть несколько резервирований на одном вычислительном ресурсе или несколько резервирований на нескольких вычислительных ресурсах разных типов.

Резервирование задает не только объем ресурсов структуры, которые выделяются для бизнес-группы, но и политики, приоритеты и квоты, от которых зависит размещение компьютеров.

Для успешной подготовки необходимо наличие в хранилище достаточного объема памяти для резервирования. Доступность хранилища для резервирования зависит от следующих факторов.

- Какой объем пространства доступен в хранилище данных или кластере.
- Какой объем этого пространства зарезервирован для данного хранилища данных или кластера.
- Какой объем этого пространства уже выделен в vRealize Automation

Так, даже если в vCenter Server имеется доступное пространство для хранилища данных или кластера, но не выделено достаточно свободного пространства для резервирования, подготовка завершится с ошибкой («Нет доступного резервирования для выделения...»). Объем пространства, выделяемого для конкретного резервирования, зависит от количества виртуальных машин (в любом состоянии) в этом резервировании. Дополнительные сведения см. в статье базы знаний VMware «Компьютер XXX: нет доступного резервирования для выделения в группе XXX». *Всего запрошено XX ГБ свободного пространства (2151030)* по адресу <http://kb.vmware.com/kb/2151030>.

Общие сведения о выборе логики для резервирований

Когда участник бизнес-группы создает запрос на подготовку виртуальной машины, vRealize Automation выбирает компьютер из одного из резервирований, доступных для этой бизнес-группы.

Резервирование, к которому подготавливается компьютер, должно соответствовать следующим критериям.

- У резервирования и схемы элементов, с которой поступил запрос на компьютер, должен быть одинаковый тип платформы.

Универсальную виртуальную схему элементов можно инициализировать в виртуальном резервировании любого типа.

- Резервирование должно быть включено.
- Вычислительные ресурсы должны быть доступны и не должны находиться в режиме обслуживания.
- Объем резервирования должен находиться в пределах квоты на компьютеры или квота должна быть неограниченна.

Выделенная квота на компьютеры распространяется только на включенные компьютеры. Например, если квота резервирования — 50 компьютеров, 40 подготовлены, но только 20 из них включены, выделяется 40%, а не 80% квоты резервирования.

- Резервирование должно располагать объемом невыделенных памяти и ресурсов хранилища, достаточным для подготовки компьютера.

Если для виртуального резервирования полностью выделены квота на компьютеры, память или хранилище, вы не сможете с его помощью инициализировать виртуальные машины. Ресурсы можно зарезервировать с превышением физического объема вычислительных ресурсов виртуализации. Но если выделено 100% физического объема вычислительных ресурсов, с помощью этого вычислительного ресурса ни в одном из резервирований невозможно будет инициализировать никакие компьютеры, пока ресурсы не будут реорганизованы.

- Если для схемы элементов настроены определенные параметры сети, резервирование должно включать те же сети.

Если в схеме элементов или резервировании указан профиль сети для назначения статического IP-адреса, этот адрес должен быть доступен для назначения новому компьютеру.

- Если в схеме элементов или запросе указано размещение, вычислительный ресурс должен быть связан с ним.

Если для настраиваемого свойства `Vrm.DataCenter.Policy` задано значение **Exact** и отсутствуют резервирования для вычислительного ресурса, связанного с этим размещением, которые удовлетворяют всем остальным критериям, происходит сбой предоставления.

Если для параметра `Vrm.DataCenter.Policy` задано значение **NotExact** и отсутствуют резервирования для вычислительного ресурса, связанного с этим размещением, которые удовлетворяют всем остальным критериям, предоставление продолжится в другом резервировании вне зависимости от размещения. Этот параметр используется по умолчанию.

- Если в схеме элементов или запросе указано настраиваемое свойство `VirtualMachine.Host.TpmEnabled`, на вычислительный ресурс для данного резервирования необходимо установить надежное оборудование.
- Если в схеме элементов указана политика резервирования, резервирование должно к ней принадлежать.

Политики резервирования — это залог того, что выбранное резервирование будет соответствовать дополнительным требованиям к подготовке компьютеров на основе определенной схемы элементов.

Например, можно использовать политики резервирования, чтобы ограничить инициализацию вычислительными ресурсами с определенным шаблоном для клонирования.

При отсутствии доступных резервирований, отвечающих всем критериям выбора, происходит сбой подготовки.

Если несколько резервирований соответствуют всем критериям, резервирование, с помощью которого будет подготавливаться запрошенный компьютер, определяется по следующей логике.

- Резервирование с более низким значением приоритета выбирается до резервирования с более высоким значением.
- Если у нескольких резервирований одинаковый приоритет, будет выбрано то, у которого самый низкий процент выделенной квоты на компьютеры.
- Если у нескольких резервирований одинаковые приоритет и квоты, компьютеры циклично распределяются по резервированиям.

Примечание Хотя циклический выбор профилей сети не поддерживается, поддерживается циклический выбор сетей (если они доступны), которые можно связать с различными профилями сетей.

Если в резервировании доступны несколько путей к хранилищам с достаточной емкостью для подготовки томов компьютера, их выбирают по следующей логике.

- Если в схеме элементов или запросе указана политика резервирования хранилища, путь к хранилищу должен принадлежать этой политике.

Если для настраиваемого свойства `VirtualMachine.DiskN.StorageReservationPolicyMode` задано значение **NotExact** и в выбранной политике резервирования хранилища отсутствует путь к хранилищу достаточного объема, предоставление продолжится с использованием пути к хранилищу вне указанной политики резервирования. Значение свойства `VirtualMachine.DiskN.StorageReservationPolicyMode` по умолчанию — **Exact**.

- Путь к хранилищу с более низким значением приоритета выбирается до пути с более высоким значением.
- Если у нескольких путей к хранилищам одинаковый приоритет, компьютеры распределяются по соответствующим путям циклично.

Создание резервирования vSphere для сети и безопасности NSX в vRealize Automation

В vRealize Automation можно создать резервирование vSphere, которое будет использоваться для работы со связанным элементом NSX-T или конечной точкой NSX for vSphere.

Общие рекомендации по NSX

Если были настроены параметры NSX, то при создании или редактировании схемы элементов можно указать зону транспорта NSX, политику резервирования сети и параметры изоляции приложений. Эти настройки доступны на вкладке **Параметры NSX** на страницах **Схема элементов** и **Свойства схемы элементов**.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

Для успешной подготовки нужно, чтобы транспортная зона резервирования соответствовала транспортной зоне схемы элементов компьютера, если эта схема определяет сети компьютеров. Аналогично для подготовки маршрутизируемого компьютером шлюза необходимо, чтобы транспортная зона, определенная в резервировании, соответствовала транспортной зоне, определенной для схемы элементов.

Дополнительные рекомендации по использованию топологий NSX-T в развертываниях см. в разделе [Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Факторы, касающиеся NSX for vSphere

Когда решение vRealize Automation подготавливает компьютеры с помощью сети NAT или маршрутизируемой сети, оно подготавливает маршрутизируемый шлюз в качестве сетевого маршрутизатора. Пограничный или маршрутизируемый шлюз — это управляющий компьютер, потребляющий вычислительные ресурсы. Кроме того, он управляет обменом данными в сети, который происходит между подготовленными компонентами компьютеров. Резервирование, обеспечивающее подготовку пограничного или маршрутизируемого шлюза, определяет внешнюю сеть, используемую для сетевых профилей сетей NAT и маршрутизируемых сетей. Оно также определяет пограничный или маршрутизируемый шлюз резервирования, используемый для настройки маршрутизируемых сетей. Маршрутизируемый шлюз резервирования связывает вместе маршрутизируемые сети с записями в таблице маршрутизации.

При выборе пограничного или маршрутизируемого шлюза и профиля сети в резервировании для маршрутизируемых сетей необходимо выбрать сетевой путь, который будет использоваться при связывании маршрутизируемых сетей. Назначьте сетевой путь профилю внешней сети, который используется для настройки профиля маршрутизируемой сети. Список профилей сети, которые можно назначить сетевому пути, фильтруется, чтобы соответствовать подсети сетевого пути на основе маски подсети и основного IP-адреса, выбранного для сетевого интерфейса.

Вы можете задать политику резервирования пограничного или маршрутизируемого шлюза. Это позволяет задать резервирования, которые нужно использовать при подготовке компьютеров с помощью такого шлюза. По умолчанию решение vRealize Automation использует одни и те же резервирования для маршрутизируемых шлюзов и компонентов компьютеров.

Если в резервированиях vRealize Automation нужно использовать Edge или маршрутизируемый шлюз, выполните внешнюю настройку маршрутизируемого шлюза в среде NSX и запустите сбор данных иерархии. Чтобы настроить шлюз по умолчанию для статических маршрутов или указать сведения о динамической маршрутизации для шлюза служб Edge или распределенного маршрутизатора, понадобится рабочий экземпляр NSX Edge для NSX. См. *NSXруководство администратора*.

Вы выбираете группы безопасности в резервировании, чтобы применить базовую политику безопасности для всех компьютеров компонента, подготовленных с помощью этого резервирования в vRealize Automation. Каждый подготовленный компьютер добавляется в эти указанные группы безопасности.

Факторы, касающиеся NSX-T

При создании резервирования для конечной точки vSphere, которая связана с конечной точкой NSX-T, необходимо задать следующие параметры резервирования.

- Определите транспортную зону для данной схемы элементов.
- Выберите логический маршрутизатор уровня 0, к которому должны подключаться подготовленные развертывания.
- Сопоставьте профиль внешней сети этому логическому маршрутизатору уровня 0.

Группы NS NSX-T не поддерживаются в резервированиях.

Дополнительные сведения о NSX-Tконкретном развертывании и особенности топологии см. в разделе [Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer

Чтобы участники бизнес-группы могли запрашивать подготовку компьютеров, нужно выделить ресурсы компьютерам путем создания резервирования.

У каждой бизнес-группы должно быть по крайней мере одно резервирование, чтобы ее участники могли подготавливать компьютеры этого типа. Например, бизнес-группа с резервированием vSphere, а не KVM (RHEV), не может запрашивать виртуальную машину KVM (RHEV). В этом примере бизнес-группе нужно назначить специальное резервирование для ресурсов KVM (RHEV).

Процедура

1. Ввод данных о виртуальном резервировании

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

2. Указание параметров ресурсов и сети для виртуального резервирования

Укажите параметры ресурса и сети для подготовки компьютеров на базе этого резервирования vRealize Automation.

3. Указание настраиваемых свойств и оповещений для виртуальных резервирований

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Ввод данных о виртуальном резервировании

Каждое резервирование настроено для определенной бизнес-группы, которой оно дает возможность запрашивать компьютеры в указанном вычислительном ресурсе.

Вы можете управлять отображением резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по категориям»** на странице «Резервирования». Обратите внимание, что резервирования тестового агента не отображаются в списке резервирований при фильтрации по категориям.

Примечание После создания резервирования нельзя изменить связи с бизнес-группами или вычислительными ресурсами.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Убедитесь, что администратор арендатора создал по крайней мере одну бизнес-группу.
- Убедитесь, что вычислительный ресурс существует.
- Настройте сеть.
- (дополнительно) Настройте сведения о профиле сети.

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.

2. Щелкните значок **Создать** (+) и выберите тип создаваемого резервирования.

Доступны следующие типы виртуального резервирования: Hyper-V, KVM, SCVMM, vSphere и XenServer.

Например, выберите **vSphere**.

3. В текстовом поле **Имя** введите имя.
4. В раскрывающемся меню **Арендатор** выберите арендатора.
5. В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.

Инициализировать компьютеры с помощью этого резервирования могут только пользователи в этой бизнес-группе.

6. (дополнительно) В раскрывающемся меню **Политика резервирования** выберите политику резервирования.

Для применения этого параметра требуется наличие одной или нескольких политик резервирования. Резервирование можно изменить позже, чтобы задать политику резервирования.

Политика резервирования используется для ограничения инициализации конкретными резервированиями.

7. Чтобы задать приоритет для резервирования, введите число в текстовом поле **Приоритет**.

Приоритет используется, если бизнес-группа содержит несколько резервирований. Для инициализации резервирование с приоритетом 1 является более приоритетным, чем резервирование с приоритетом 2.

8. (дополнительно) Если нужно отключить это резервирование, снимите флажок **Включить это резервирование**.

Результаты

Не переходите никуда с этой страницы. Ваше резервирование не завершено.

Указание параметров ресурсов и сети для виртуального резервирования

Укажите параметры ресурса и сети для подготовки компьютеров на базе этого резервирования vRealize Automation.

В резервировании можно выбрать хранилище данных FlexClone при наличии среды vSphere и устройств хранения, использующих технологию Net App FlexClone. Устройства хранения FlexClone не поддерживают SDRS.

Для успешной подготовки необходимо наличие в хранилище достаточного объема памяти для резервирования. Доступность хранилища для резервирования зависит от следующих факторов.

- Какой объем пространства доступен в хранилище данных или кластере.
- Какой объем этого пространства зарезервирован для данного хранилища данных или кластера.
- Какой объем этого пространства уже выделен в vRealize Automation

Так, даже если в vCenter Server имеется доступное пространство для хранилища данных или кластера, но не выделено достаточно свободного пространства для резервирования, подготовка завершится с ошибкой («Нет доступного резервирования для выделения...»). Объем пространства, выделяемого для конкретного резервирования, зависит от количества виртуальных машин (в любом состоянии) в этом резервировании. Дополнительные сведения см. в статье базы знаний VMware «Компьютер XXX: нет доступного резервирования для выделения в группе XXX». *Всего запрошено XX ГБ свободного пространства (2151030)* по адресу <http://kb.vmware.com/kb/2151030>.

При создании или изменении резервирования vSphere (vCenter) для использования с NSX for vSphere или NSX-T можно указать информацию о зоне переноса и логическом маршрутизаторе уровня 1 с помощью расширенных параметров для выбранной сети.

Необходимые условия

[Ввод данных о виртуальном резервировании.](#)

Процедура

1. Перейдите на вкладку **Ресурсы**.
2. В раскрывающемся меню **Вычислительный ресурс** выберите вычислительный ресурс, в котором нужно инициализировать компьютеры.

Для этого резервирования можно клонировать только шаблоны, расположенные в выбранном кластере.

Во время подготовки компьютеры размещаются на узле, подключенном к локальному хранилищу. Если при резервировании используется локальное хранилище, все компьютеры, которые подготовлены путем резервирования, создаются на узле, содержащем это локальное хранилище. Однако если используется настраиваемое свойство `VirtualMachine.Admin.ForceHost`, которое принудительно подготавливает компьютер на другом узле, подготовка завершается ошибкой. Подготовка также завершается ошибкой, если шаблон, из которого компьютер клонируется, находится в локальном хранилище, но подключен к компьютеру из другого кластера. В этом случае ошибка возникает из-за отсутствия доступа к шаблону.

3. (дополнительно) Чтобы задать максимальное число компьютеров, которые можно инициализировать в этом резервировании, введите число в текстовом поле **Квота на компьютеры**.

В квоте учитываются только включенные компьютеры. Оставьте поле пустым, чтобы снять ограничение для резервирований.

4. В таблице «Память» укажите количество гигабайтов памяти, выделяемых для этого резервирования.

Общий объем памяти для резервирования зависит от выбранных вычислительных ресурсов.

5. В таблице «Память» укажите количество гигабайтов памяти, выделяемых для этого резервирования.

Общий объем памяти для резервирования зависит от выбранных вычислительных ресурсов.

6. Выберите один или несколько из перечисленных путей к хранилищам.

Доступные варианты пути к хранилищу зависят от выбранных вычислительных ресурсов.

Для интеграции, при которой используются хранилища с технологией Distributed Resource Scheduler (SDRS), можно выбрать кластер хранилища, чтобы разрешить SDRS автоматически выполнять размещение в хранилище и балансировку нагрузки для компьютеров, подготовленных из этого резервирования. Для режима автоматизации SDRS должен быть установлен параметр «Автоматически». В ином случае необходимо выбрать хранилище данных в кластере для автономного режима работы хранилища данных. Устройства хранения FlexClone не поддерживают SDRS.

Можно выбрать либо отдельные диски в кластере, либо кластер хранилища, но не то и другое. Если выбрать кластер хранилища, в SDRS будет осуществляться управление размещением в хранилище и балансировкой нагрузки для компьютеров, подготовленных из этого резервирования.

7. Если это доступно для вычислительного ресурса, выберите пул ресурсов в раскрывающемся меню **Пул ресурсов**.
8. Перейдите на вкладку **Сеть**.
9. Настройте сетевой путь для компьютеров, инициализированных с использованием этого резервирования.

- а) (дополнительно) Если параметр доступен, в раскрывающемся меню **Конечная точка** выберите конечную точку хранилища.

Параметр FlexClone отображается в столбце конечной точки, если конечная точка NetApp ONTAP существует и если используется виртуальный узел. Если конечная точка NetApp ONTAP существует, на странице резервирования отображается конечная точка, назначенная пути к хранилищу. При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается во всех соответствующих резервированиях.

При добавлении, обновлении или удалении конечной точки для пути к хранилищу соответствующее изменение отображается на странице резервирования.

- б) Выберите один или несколько **сетевых адаптеров** для компьютеров, которые нужно подготовить для этого резервирования.
- в) (дополнительно) Выберите доступный **профиль сети** для каждого выбранного сетевого адаптера.
- г) (дополнительно) Если доступны дополнительные настройки, выберите **транспортную зону** и один или несколько **логических маршрутизаторов уровня 0**, которые будут использоваться при развертывании схемы элементов, содержащей подсистемы балансировки нагрузки.

Транспортная зона определяет, какие кластеры могут охватывать сетевые адаптеры. Если транспортная зона указана в резервировании и схеме элементов, значения транспортной зоны должны совпадать.

Вы можете выбрать несколько сетевых адаптеров в резервировании, но при подготовке компьютера будет использоваться только одна сеть.

Результаты

Можно сохранить резервирование сейчас, нажав элемент **Сохранить**. Также можно добавить настраиваемые свойства для дополнительного контроля над спецификациями резервирования. Кроме того, можно настроить отправку уведомлений с оповещениями по электронной почте, если ресурсов, выделенных для этого резервирования, недостаточно.

Указание настраиваемых свойств и оповещений для виртуальных резервирований

Вы можете связать настраиваемые свойства с резервированием vRealize Automation. Кроме того, вы можете настроить оповещения, чтобы отправлять уведомления по электронной почте, когда ресурсов резервирования мало.

Настраиваемые свойства и оповещения по электронной почте — необязательные настройки для резервирования. Если вам не нужно связывать настраиваемые свойства или настраивать предупреждения, щелкните **Сохранить**, чтобы завершить создание резервирования.

Вы можете добавить нужное количество настраиваемых свойств.

Важно! Оповещения отправляются, только если настроены уведомления по электронной почте и включены оповещения.

Если уведомления настроены, они создаются ежедневно, а не при достижении указанного порогового значения.

Необходимые условия

[Указание параметров ресурсов и сети для виртуального резервирования.](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Нажмите кнопку **Создать**.
3. Введите действительное имя настраиваемого свойства.
4. При необходимости введите значение свойства.
5. (дополнительно) Установите флажок **Зашифровано**, чтобы зашифровать значение свойства.
6. (дополнительно) Установите флажок **Запросить пользователя**, чтобы пользователю отображался запрос на ввод значения.

Этот параметр нельзя переопределить во время подготовки.

7. (дополнительно) Добавьте любые дополнительные настраиваемые свойства.
8. Перейдите на вкладку **Предупреждения**.
9. Установите флажок **Оповещения о емкости**, чтобы настроить отправку оповещений.
10. С помощью ползунка установите пороговые значения для распределения доступных ресурсов.

11. Введите в текстовом поле **Получатели** имена пользователей или групп AD (не электронные адреса), чтобы получать оповещения.

Вводите каждое имя в отдельной строке. Нажмите клавишу ВВОД, чтобы разделить несколько записей.

12. Выберите элемент **Отправлять оповещения диспетчеру групп**, чтобы включить диспетчеров групп в оповещения по электронной почте.

Эти оповещения отправляются по электронной почте пользователям, включенным в список бизнес-группы **Получатель эл. сообщений диспетчера**.

13. Укажите частоту напоминаний (дн.).

14. Нажмите кнопку **Сохранить**.

Результаты

Резервирование сохраняется и появляется в списке резервирований.

Следующие шаги

Можно настроить дополнительные политики резервирования или начать подготовку к инициализации.

Пользователи, авторизованные для создания схем элементов, могут создать их сейчас.

Изменение резервирования для назначения профиля сети

Резервированию можно назначить профиль сети, например чтобы включить назначение статического IP-адреса компьютеру, подготовленному для этого резервирования.

Чтобы назначить схеме элементов профиль сети, можно также воспользоваться настраиваемым свойством `VirtualMachine.NetworkN.ProfileName` на вкладке **Свойства** страницы **Новая схема элементов** или **Свойства схемы элементов**.

Если профиль сети указан в резервировании и схеме элементов, то значения в схеме элементов имеет более высокий приоритет.

Примечание Эта информация не распространяется на Amazon Web Services.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте профиль сети. См. [Создание профиля сети в vRealize Automation](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Наведите указатель на резервирование и щелкните **Изменить**.
3. Перейдите на вкладку **Сеть**.

4. Назначьте профиль сети сетевому пути.

- а) Выберите сетевой путь, для которого необходимо включить статические IP-адреса.
Параметры сетевого пути определяются на основе настроек на вкладке **Ресурсы**.
- б) Чтобы сопоставить доступный профиль сети с путем, выберите профиль в раскрывающемся меню **Профиль сети**.
- в) (дополнительно) Повторите этот шаг, чтобы назначить профили сетей дополнительным сетевым путям для этого резервирования.

5. Нажмите кнопку **ОК**.

Политики резервирования

Использование политики резервирования дает возможность управлять обработкой запросов на резервирование. При подготовке компьютеров на основе схемы элементов подготавливаются только ресурсы, указанные в политике резервирования.

Политики резервирования предоставляют дополнительные средства управления обработкой запросов на резервирование. Можно применить политику резервирования к схеме элементов, чтобы компьютеры, подготовленные с использованием этой схемы, были ограничены набором доступных резервирований.

Политику резервирования можно использовать с целью сбора ресурсов в группы для разных уровней обслуживания или с целью обеспечения легкого доступа к ресурсу определенного типа для определенной цели. Когда пользователь запрашивает компьютер, он может быть подготовлен в любом резервировании соответствующего типа, которое располагает достаточными ресурсами для компьютера. Следующие сценарии содержат несколько примеров возможного использования политик резервирования.

- Чтобы убедиться, что подготовленные компьютеры размещаются в резервированиях с конкретными устройствами, которые поддерживают технологию NetApp FlexClone.
- Чтобы ограничить подготовку облачных компьютеров определенным регионом, содержащим образ компьютера, который необходим для конкретной схемы.
- В качестве дополнительных средств использования модели выделения с повременной оплатой для типов компьютеров, которые поддерживают эту возможность.

В политику резервирования можно добавить несколько резервирований, однако резервирование может принадлежать только одной политике. Одну политику резервирования можно назначить нескольким схемам элементов. Схема элементов может содержать только одну политику резервирования.

Примечание Резервирования, определенные для конечных точек vCloud Air и конечных точек vCloud Director, не поддерживают использование профилей сети для подготавливаемых компьютеров.

Примечание Если на платформе включена функция SDRS, с ее помощью можно выполнять балансировку нагрузки на хранилище для отдельных дисков виртуальных машин или на все ресурсы хранилища виртуальной машины. Если применяются кластеры хранилища данных SDRS, могут возникать конфликты при использовании политик резервирования и политик резервирования хранилища. Например, если в одном из резервирований в политике или в политике хранилища выбрано отдельное хранилище данных или хранилище данных в рамках кластера SDRS, хранилище виртуальной машины может быть заморожено, вместо того чтобы быть под управлением SDRS. При запросе повторной подготовки компьютера с размещением хранилища в кластере SDRS компьютер удаляется, если деактивирован уровень автоматизации SDRS. Дополнительные сведения о предоставлении и SDRS см. в настраиваемом свойстве `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

Настройка политик резервирования

Политика резервирования используется с целью сбора ресурсов в группы для разных уровней обслуживания или с целью обеспечения легкого доступа к ресурсу определенного типа для определенной цели. Чтобы администраторы арендаторов и диспетчеры бизнес-групп могли эффективно использовать политику резервирования в схеме элементов, нужно после создания политики заполнить ее резервированиями.

Политика резервирования может включать в себя резервирования разных типов, но при выборе резервирования для конкретного запроса учитываются только резервирования, которые соответствуют типу схемы элементов.

Процедура

1. Создание политики резервирования

Политики резервирования можно использовать для группировки похожих резервирований.

2. Назначение политики резервирования резервированию

Политику резервирования можно назначить резервированию при его создании. Можно также изменить существующее резервирование, чтобы назначить для него политику резервирования, или изменить назначение политики резервирования.

Создание политики резервирования

Политики резервирования можно использовать для группировки похожих резервирований.

Сначала создайте политику резервирования, а затем добавьте ее к резервированиям, чтобы создатель схемы элементов мог использовать политику резервирования в схеме элементов.

Политика создается как пустой контейнер.

Вы можете управлять отображением политик резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по типам»** на странице «Политики резервирования».

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Резервирования > Политики резервирования**.
2. Выберите значок **Создать** (+).
3. В текстовом поле **Имя** введите имя.
4. Выберите пункт **Политика резервирования** в раскрывающемся меню **Тип**.
5. В текстовом поле **Описание** введите описание.
6. Нажмите кнопку **ОК**.

Назначение политики резервирования резервированию

Политику резервирования можно назначить резервированию при его создании. Можно также изменить существующее резервирование, чтобы назначить для него политику резервирования, или изменить назначение политики резервирования.

Необходимые условия

[Создание политики резервирования](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Резервирования**.
2. Наведите указатель на резервирование и щелкните **Изменить**.
3. В раскрывающемся меню **Политика резервирования** выберите политику резервирования.
4. Нажмите кнопку **Сохранить**.

Политики резервирования хранилищ

Чтобы разработчики схем элементов могли назначать тома виртуальной машины различным хранилищам данных для платформ типа vSphere, KVM (RHEV) и SCVMM, а также назначать различные профили хранилища другим ресурсам, например vCloud Air или vCloud Director, можно создать политики резервирования хранилища.

Назначая тома виртуальной машины различным хранилищам данных или другому профилю хранилища, разработчики схемы элементов могут эффективнее использовать пространство хранилища и управлять им. Например, можно развернуть том операционной системы в более медленном и менее дорогом хранилище данных или профиле хранилища, а том базы данных — в более быстром хранилище данных или профиле хранилища.

Некоторые конечные точки компьютеров поддерживают только один профиль хранилища, в то время как другие — многоуровневое дисковое хранилище. Многоуровневое дисковое хранилище доступно для конечных точек vCloud Director 5.6 и более новых версий, а также для конечных точек vCloud Air. Многоуровневое дисковое хранилище не поддерживается для конечных точек vCloud Director 5.5.

При создании схемы элементов можно назначить одну политику хранилища данных или резервирования хранилища, которая представляет несколько хранилищ данных для тома. При назначении одного хранилища данных или профиля хранилища тому это хранилище данных или профиль хранилища используется vRealize Automation во время подготовки, если это возможно. Если они назначают тому политику резервирования хранилища, во время подготовки vRealize Automation использует одно из своих хранилищ данных или один из профилей хранилища при работе с другими ресурсами, например vCloud Air или vCloud Director.

Политика резервирования хранилища, по сути, является меткой, которую администратор структуры применяет к одному или нескольким хранилищам данных или профилям хранилища для группирования хранилищ данных или профилей хранилища с аналогичными характеристиками, например схожей скоростью или ценой. Хранилище данных или профиль хранилища нельзя назначить несколькими политикам резервирования хранилища одновременно, но одну политику резервирования хранилища можно назначить нескольким хранилищам данных или профилям хранилища.

Можно создать политику резервирования хранилища и назначить ее одному или нескольким хранилищам данных или профилям хранилища. Создатель схемы элементов может назначить политику резервирования хранилища тому в виртуальной схеме элементов. Когда пользователь запрашивает компьютер, использующий схему элементов, при выборе хранилища данных или профиля хранилища для тома компьютера vRealize Automation использует политику резервирования хранилища, указанную в этой схеме.

Примечание Если на платформе включена функция SDRS, с ее помощью можно выполнять балансировку нагрузки на хранилище для отдельных дисков виртуальных машин или на все ресурсы хранилища виртуальной машины. Если применяются кластеры хранилища данных SDRS, могут возникать конфликты при использовании политик резервирования и политик резервирования хранилища. Например, если в одном из резервирований в политике или в политике хранилища выбрано отдельное хранилище данных или хранилище данных в рамках кластера SDRS, хранилище виртуальной машины может быть заморожено, вместо того чтобы быть под управлением SDRS. При запросе повторной подготовки компьютера с размещением хранилища в кластере SDRS компьютер удаляется, если деактивирован уровень автоматизации SDRS. Дополнительные сведения о предоставлении и SDRS см. в настраиваемом свойстве `VirtualMachine.Admin.Datastore.Cluster.ResourceLeaseDurationSec`.

Хранилище и память, назначенные подготовленному компьютеру путем резервирования, освобождаются, когда компьютер, которому они назначены, удаляется в vRealize Automation. Хранилище и память не освобождаются, если компьютер удален в vCenter Server.

Например, нельзя удалить резервирование, которое связано с компьютерами в существующем развертывании. При перемещении или удалении развернутых компьютеров в vCenter Server вручную vRealize Automation по-прежнему распознает развернутые компьютеры как существующие и не даст удалить связанные резервирования.

Настройка политик резервирования хранилищ

Вы можете создать политику резервирования хранилища для группирования хранилищ данных с аналогичными характеристиками, например похожей скоростью или ценой. Чтобы использовать такую политику в схеме элементов, после создания ее нужно заполнить хранилищами данных.

Процедура

1. Создание политики резервирования хранилища

Политику резервирования хранилища можно использовать для группировки хранилищ данных с аналогичными характеристиками, например с похожей скоростью или ценой.

2. Назначение политики резервирования хранилища хранилищу данных

Политику резервирования хранилища можно связать с вычислительным ресурсом. Создав политику резервирования хранилища, заполните ее хранилищами данных. Хранилище данных может принадлежать только к одной политике резервирования хранилища. Чтобы создать группу хранилищ данных для использования со схемой элементов, добавьте несколько хранилищ данных.

Создание политики резервирования хранилища

Политику резервирования хранилища можно использовать для группировки хранилищ данных с аналогичными характеристиками, например с похожей скоростью или ценой.

Политика создается как пустой контейнер.

Вы можете управлять отображением политик резервирования при добавлении, редактировании или удалении, используя параметр **«Фильтровать по типам»** на странице «Политики резервирования».

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Резервирования > Политики резервирования**.
2. Выберите значок **Создать (+)**.
3. В текстовом поле **Имя** введите имя.
4. Выберите пункт **Политика резервирования хранилища** в раскрывающемся меню **Тип**.
5. В текстовом поле **Описание** введите описание.
6. Нажмите кнопку **ОК**.

Назначение политики резервирования хранилища хранилищу данных

Политику резервирования хранилища можно связать с вычислительным ресурсом. Создав политику резервирования хранилища, заполните ее хранилищами данных. Хранилище данных может принадлежать только к одной политике резервирования хранилища. Чтобы создать группу хранилищ данных для использования со схемой элементов, добавьте несколько хранилищ данных.

Необходимые условия

[Создание политики резервирования хранилища.](#)

Процедура

1. Выберите **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**.
2. Наведите указатель на вычислительный ресурс и щелкните **Изменить**.
3. Перейдите на вкладку **Конфигурация**.
4. Найдите хранилище данных, которое нужно добавить в политику резервирования хранилища, в таблице «Хранилище».
5. Щелкните значок **Изменить** (✎) рядом с нужным объектом **Путь к хранилищу**.
6. Выберите политику резервирования хранилища в раскрывающемся меню **Политика резервирования хранилища**.

После подготовки компьютера его политику резервирования хранилища изменять нельзя, если это изменит профиль хранилища на диске.

7. Нажмите кнопку **ОК**.
8. (дополнительно) Назначьте дополнительные хранилища данных политике резервирования хранилища.
9. Нажмите кнопку **ОК**.

Размещение рабочей нагрузки

При развертывании схемы элементов собранные данные будут использоваться в размещении рабочей нагрузки для представления рекомендации относительно места развертывания схемы элементов на основе доступных ресурсов. vRealize Automation и vRealize Operations Manager работают вместе, обеспечивая рекомендации по размещению для рабочих нагрузок в развертывании новых схем элементов.

Одновременно с управлением политиками организации, такими как бизнес-группы, резервирования и квоты, vRealize Automation также интегрируется с аналитикой производительности vRealize Operations Manager для размещения компьютеров. Размещение рабочей нагрузки доступно только для конечных точек vSphere.

Используемые термины, касающиеся размещения рабочей нагрузки

К размещению рабочей нагрузки применяется ряд терминов.

- Кластеры в vSphere сопоставляются с вычислительными ресурсами в vRealize Automation.
- Резервирования состоят из вычисления и хранилища, при этом хранилище может включать в себя отдельные хранилища данных или кластеры хранилищ данных. Резервирование может включать в себя несколько хранилищ данных и/или кластеров хранилищ данных.
- Несколько резервирований могут ссылаться на один и тот же кластер.
- Виртуальные машины могут перемещаться в несколько кластеров.
- При включенном размещении рабочей нагрузки в рабочем процессе подготовки будет использоваться политика размещения для представления рекомендации относительно места развертывания схемы элементов.

Подготовка схем элементов с использованием размещения рабочей нагрузки

Если для подготовки схем элементов используется размещение рабочей нагрузки, в рабочем процессе подготовки будут использоваться резервирования в vRealize Automation и оптимизация размещений из vRealize Operations Manager.

1. vRealize Automation предоставляет правила управления, чтобы разрешать назначения размещений.
2. vRealize Operations Manager предоставляет рекомендации по оптимизации размещений в соответствии с данными аналитики.
3. vRealize Automation продолжает процесс подготовки в соответствии с рекомендациями по размещению из vRealize Operations Manager.

Если решением vRealize Operations Manager не может быть предоставлена рекомендация (или рекомендация не может быть использована), vRealize Automation возвращается к логике размещений по умолчанию.

Когда разработчик выбирает элемент каталога и заполняет форму его запроса, в vRealize Automation для подготовки виртуальных машин учитываются следующие факторы.

Таблица 2-16. Факторы для подготовки виртуальных машин

Фактор	Эффект
Политики	Политика резервирования vRealize Automation может указывать на несколько резервирований.
Резервирования	<p>vRealize Automation оценивает запрос и определяет, какие резервирования удовлетворяют ограничениям, заданным в запросе.</p> <ul style="list-style-type: none"> ■ Если размещение включено и основано на аналитике vRealize Operations Manager, из vRealize Automation в vRealize Operations Manager передается список резервирований для определения того, какое из них лучше всего подходит к размещению с учетом показателей эксплуатации. ■ Если размещение не основано на vRealize Operations Manager, vRealize Automation выбирает размещение в зависимости от приоритетов и доступности. <p>Резервирования обновляются для отслеживания использованных ресурсов.</p> <p>Если vRealize Operations Manager рекомендует кластер или хранилище данных, а vRealize Automation сообщает, что в них недостаточно емкости или они больше не используются, vRealize Automation регистрирует исключение. vRealize Automation позволяет продолжить подготовку в соответствии с механизмами размещения, используемыми по умолчанию.</p>

Чтобы определить ресурсы для виртуальной машины, в vRealize Automation предоставляется список вариантов резервирований. Каждый вариант состоит из кластера и одного или нескольких хранилищ данных либо кластеров хранилищ данных. В vRealize Operations Manager варианты резервирования используются для создания списка вариантов целевых точек и обнаружения лучшей цели.

Политика в vRealize Operations Manager устанавливает уровень баланса, использования и объем буфера для кластера. В случае одиночного резервирования, представляющего собой кластер или кластер хранилища данных, в vRealize Automation проверяется, является ли рекомендация подходящей целевой точкой размещения.

- Если целевая точка подходит, vRealize Automation разворачивает схему элементов в соответствии с рекомендацией.

- Если целевая точка не подходит, в vRealize Automation для размещения виртуальных машин используется стандартный порядок размещения.

Факторы, касающиеся размещения, также должны охватывать проблемы работоспособности и использования. В то время как администратор облачного хранилища и администратор виртуальной инфраструктуры управляют инфраструктурой, разработчики заботятся о работоспособности своих приложений. Для поддержки разработчиков стратегия размещения рабочей нагрузки должна также учитывать проблемы работоспособности и использования.

Таблица 2-17. Факторы, касающиеся проблем работоспособности и использования

Проблема рабочей нагрузки	Решение размещения
Разработчик обозначает проблему работоспособности в среде.	vRealize Automation подготавливает схемы элементов в кластерах, в которых возникли проблемы, или кластерах, перегруженных из-за больших рабочих нагрузок. vRealize Automation должен интегрироваться с аналитикой производительности в vRealize Operations Manager, чтобы обеспечить подготовку схем элементов в кластерах, имеющих достаточную емкость.
Разработчик обозначает проблему использования.	Кластеры в среде недогружены. Решение vRealize Automation должно интегрироваться с предоставляемой диспетчером vRealize Operations Manager аналитикой производительности, чтобы схемы элементы могли подготавливаться в кластере с максимальным показателем использования.

Пользователи, подготавливающие схемы элементов

Следующие пользователи выполняют действия для подготовки схем элементов.

Таблица 2-18. Пользователи и роли для подготовки схем элементов

Шаг	Пользователь	Действие	Требуемая роль
1	Администратор облачного хранилища или администратор виртуальной инфраструктуры (VI)	Обеспечивает начальное размещение виртуальных машин в соответствии с политиками организации и их оптимизацию согласно данным эксплуатационной аналитики.	Роль «Администратор инфраструктуры как услуги»
1	Администратор структуры	Определяет резервирования, политики резервирования и политику размещения в vRealize Automation.	Роль «Администратор структуры», архитектор инфраструктуры
1	Администратор инфраструктуры как услуги	Определяет конечные точки для vSphere и vRealize Operations Manager, необходимые для размещения рабочих нагрузок.	Роль «Администратор инфраструктуры как услуги»
2	Архитектор инфраструктуры	Архитектор схемы элементов, который работает непосредственно с типами компонентов виртуальных машин, назначает виртуальным машинам политики резервирования во время разработки схемы элементов. Политика резервирования указывается как свойство компонента компьютера в схеме элементов.	Архитектор инфраструктуры

Таблица 2-18. Пользователи и роли для подготовки схем элементов (продолжение)

Шаг	Пользователь	Действие	Требуемая роль
3	Архитектор инфраструктуры, архитектор приложений, архитектор программного обеспечения и архитектор решений «все как услуга»	<p>Создает и публикует схему элементов для подготовки виртуальных машин. Непосредственно с компонентами компьютеров работает только архитектор инфраструктуры. Архитекторы других ролей могут использовать схемы элементов инфраструктуры в качестве вложенных структур, но не могут изменять параметры компонента компьютера.</p> <p>Схема элементов может включать в себя один компонент или вложенные схемы элементов, компоненты службы «Все как услуга», несколько виртуальных машин в многоуровневом приложении и так далее.</p> <p>vRealize Automation размещает виртуальные машины в соответствии с конфигурацией резервирования и при необходимости включает политику резервирования на уровне компонентов компьютеров в схеме элементов. Например, схема элементов может включать в себя два компьютера, к каждому из которых применена своя политика.</p> <p>vRealize Automation также оптимизирует виртуальные машины в соответствии с данными эксплуатационной аналитики, предоставляемыми решением vRealize Operations Manager.</p>	Архитектор инфраструктуры
4	Администратор облачного хранилища или администратор виртуальной инфраструктуры	<p>Выбирает политики, управляющие первоначальным размещением виртуальных машин, которые подготавливает vRealize Automation.</p> <p>Администратор может выполнять следующие действия.</p> <ul style="list-style-type: none"> ■ Выбирать политики, используя API. ■ Использовать политику размещения, попеременно использующую каждый сервер в vRealize Automation для балансировки рабочих нагрузок. Этот подход не требует ввода данных из vRealize Operations Manager. 	Роль «Администратор инфраструктуры как услуги», архитектор инфраструктуры
5	Администратор виртуальной инфраструктуры	<p>Собирает настраиваемый центр обработки данных и настраиваемые группы в vRealize Operations Manager. Затем администратор виртуальной инфраструктуры применяет к настраиваемым центрам обработки данных политики для сбора и балансировки рабочей нагрузки.</p>	Роль «Администратор инфраструктуры как услуги», архитектор инфраструктуры
6	Администратор структуры	<p>Выбирает политику размещения в vRealize Automation.</p> <p>Использовать политику размещения рабочих нагрузок при развертывании новых схем элементов, чтобы ПО vRealize Automation определило, где следует разместить компьютеры. Для политики размещения требуется ввод данных из vRealize Operations Manager</p>	Роль администратора структуры

Таблица 2-18. Пользователи и роли для подготовки схем элементов (продолжение)

Шаг	Пользователь	Действие	Требуемая роль
7	Разработчик	Запрашивает схему элементов для подготовки виртуальных машин. Схема элементов может состоять из нескольких компьютеров для запуска приложения с трехуровневой архитектурой.	
8	Разработчик	Когда разработчик развертывает схему элементов, vRealize Operations Manager ищет политику размещения, подбирающую кластеры, соответствующие запросу.	

Дополнительные сведения о политике размещения см. в разделе [Политика размещения](#).

Для настройки размещения рабочей нагрузки см. [Настройка размещения рабочей нагрузки](#).

Для размещения виртуальных машин требуется Distributed Resource Scheduler (DRS)

vSphere DRS — это модуль размещения, который используется в vRealize Automation и vRealize Operations Manager для подготовки и размещения виртуальных машин.

Чтобы в vRealize Automation мог быть предложен оптимальный вариант размещения виртуальных машин, в кластере необходимо включить модуль DRS и задать для него полностью автоматизированный режим работы. После этого в vRealize Automation интерфейсы API vSphere DRS будут использоваться, чтобы определять правильное размещение виртуальных машин.

В vRealize Automation предусмотрена интеграция со службой размещения vRealize Operations Manager. В vRealize Operations Manager рекомендации по размещению предоставляются только для кластеров, в которых модуль DRS включен и полностью автоматизирован.

Влияние политик резервирования хранилища vRealize Automation

Наличие политик резервирования хранилища vRealize Automation влияет на размещение рабочей нагрузки с помощью vRealize Operations Manager.

Если функция размещения рабочей нагрузки с помощью vRealize Operations Manager включена, vRealize Automation передает список доступных резервирований в vRealize Operations Manager и vRealize Operations Manager оценивает их для размещения в хранилище с учетом эксплуатационной аналитики.

Примечание При размещении рабочей нагрузки с помощью vRealize Operations Manager поддерживаются только виртуальные машины с одним или несколькими дисками и лишь одной политикой резервирования хранилища. Для размещения дисков не поддерживается несколько комбинаций политик, поскольку не поддерживается размещение отдельного диска.

Если схема элементов содержит политики резервирования хранилища, рекомендации по размещению рабочих нагрузок от vRealize Operations Manager изменяются следующим образом.

Конфигурация	Размещение
Виртуальные машины с одним или несколькими дисками, в которых не указана политика резервирования хранилища.	Размещение происходит в обычном режиме. vRealize Operations Manager оценивает полный, неотфильтрованный список вариантов резервирования.
Виртуальные машины с одним или несколькими дисками, в которых указана одинаковая политика резервирования хранилища.	Варианты резервирования фильтруются на уровне хранилища, чтобы в vRealize Operations Manager выполнялась оценка только хранилищ данных, которые соответствуют этой политике резервирования хранилища.
Виртуальные машины с несколькими дисками, в некоторых из которых указана одинаковая политика резервирования хранилища, а в других не указана никакая политика резервирования хранилища.	<ul style="list-style-type: none"> ■ Если установлен тип СОБРАННОЕ для выделения хранилища, по умолчанию все диски обрабатываются, как если бы в них всех использовалась одна и та же политика. vRealize Operations Manager оценивает хранилища данных, которые соответствуют этой политике резервирования хранилища. ■ Если установлен тип РАСПРЕДЕЛЕННОЕ для выделения хранилища, невозможно разместить виртуальные машины в соответствии с рекомендациями vRealize Operations Manager, поскольку размещение отдельного диска не поддерживается. Вместо этого в размещении по умолчанию используются алгоритмы размещения vRealize Automation. <p>Можно задать тип выделения хранилища с помощью настраиваемого свойства.</p>
Виртуальные машины с несколькими дисками, для которых указаны разные политики резервирования хранилища.	Поскольку есть конфликтные требования политики резервирования хранилища, эти виртуальные машины невозможно разместить в соответствии с рекомендациями vRealize Operations Manager. Вместо этого в размещении по умолчанию используются алгоритмы размещения vRealize Automation.
Виртуальные машины, для которых требуется определенный путь к хранилищу.	<p>Эти виртуальные машины не размещаются в соответствии с рекомендациями vRealize Operations Manager, поскольку для них уже задан путь к хранилищу. Размещение необязательно должно совпадать с рекомендациями vRealize Operations Manager.</p> <p>Путь к хранилищу можно задать с помощью настраиваемого свойства.</p>

Ошибки размещения. Если невозможно выполнить размещение на основе рекомендаций vRealize Operations Manager, в сообщении об ошибке указывается причина. Среди причин могут быть неподдерживаемые условия, описанные в предыдущем списке, или такие факторы среды, как сбой связи между vRealize Operations Manager и vRealize Automation.

Чтобы просмотреть ошибки, перейдите в раздел **Запросы > Выполнение**. В правом верхнем углу щелкните **Просмотреть ошибки размещения**.

Ограничения на размещение рабочей нагрузки

Когда при развертывании новых схем элементов для размещения компьютеров используется политика размещения, предназначенная для размещения рабочих нагрузок, имейте в виду ограничения.

- В vRealize Operations Manager решение vRealize Automation определяет кластеры и виртуальные машины, которыми управляет vRealize Automation.
- Когда vRealize Automation управляет дочерними объектами контейнера стандартного или настраиваемого центра обработки данных в vRealize Operations Manager, возможность перебалансировать или переместить эти объекты отсутствует. Вы не сможете активировать или деактивировать исключение действий на объектах, управляемых службой vRealize Automation.

- Для объектов, которыми управляет vRealize Automation, размещение рабочей нагрузки выглядит следующим образом:
 - Если центр обработки данных (или пользовательский центр обработки данных) содержит кластер, которым управляет vRealize Automation, в процессе размещения рабочей нагрузки нельзя будет перебалансировать этот кластер.
 - Если кластер содержит виртуальные машины, которыми управляет vRealize Automation, в процессе размещения рабочих нагрузок нельзя будет переместить эти виртуальные машины.
- vRealize Operations Manager не поддерживает размещение рабочих нагрузок в пулах ресурсов в vCenter Server.
- vRealize Operations Manager 7.5 и более поздних версий поддерживает хранилища данных vSAN для размещения обходного пути. Дополнительные сведения см. в [информации о версии](#) для vRealize Operations Manager 7.5.

Разрешения на настройку размещения рабочих нагрузок

Чтобы настраивать размещение рабочих нагрузок и его политику, требуются разрешения в vRealize Automation и vRealize Operations Manager.

Чтобы настроить размещение рабочих нагрузок в vRealize Automation, требуется роль администратора структуры. См. раздел «Описание ролей» в vRealize Automation Информационном центре.

В vRealize Operations Manager необходимо создать роль пользователя для размещения рабочей нагрузки и назначить ей разрешения.

- В учетной записи пользователя в иерархии объектов назначьте разрешение на доступ к узлам и кластерам vSphere и к хранилищу vSphere только для чтения.
- Чтобы дать роли пользователя возможность использовать вызовы API при размещении рабочих нагрузок, назначьте для API разрешения на чтение и запись. Выберите **Администрирование > Контроль доступа > Разрешения** и затем **REST API > Все прочие API** для чтения, записи.

В vRealize Automation при регистрации конечной точки, а также для запроса рекомендаций по размещению во время подготовки от имени пользователей, запрашивающих элементы каталога, используется роль vRealize Operations Manager.

Дополнительные сведения см. в статье «Контроль доступа» в Информационном центре vRealize Operations Manager.

Политика размещения

При развертывании новых схем элементов можно использовать политику размещения, чтобы ПО vRealize Automation определило, где следует разместить компьютеры. Политика размещения работает с использованием аналитики vRealize Operations Manager для определения нагрузок в ваших кластерах, что позволяет ей предлагать точки размещения.

Прежде чем приступить к использованию политики размещения, необходимо выполнить несколько действий. Создайте в vRealize Automation конечные точки для экземпляров vRealize Operations Manager и vCenter Server. Затем нужно создать группу структур и добавить резервирования к конечной точке vCenter Server.

Чтобы диспетчер vRealize Operations Manager предоставлял vRealize Automation аналитику размещения рабочей нагрузки, выполните следующие действия.

- Установите решение vRealize Automation в экземпляре vRealize Operations Manager, используемом для размещения рабочей нагрузки.
- Настройте vRealize Operations Manager для мониторинга сервера vCenter Server.

Порядок настройки vRealize Automation и vRealize Operations Manager для размещения рабочей нагрузки см. в разделе [Настройка размещения рабочей нагрузки](#).

Расположение политики размещения

В экземпляре vRealize Automation выберите **Инфраструктура > Резервирования > Политика размещения**.

Чтобы использовать аналитические данные по размещению рабочих нагрузок, получаемые от vRealize Operations Manager, выберите элемент **Использовать vRealize Operations Manager для получения рекомендаций по размещению**

Если политика размещения рабочих нагрузок не используется, в vRealize Automation применяется стандартный метод размещения.

Настройка размещения рабочей нагрузки

Чтобы использовать политику размещения для размещения компьютеров при развертывании новых схем элементов, необходимо настроить vRealize Automation для использования аналитических данных, которые предоставляются vRealize Operations Manager. Необходимо также настроить vRealize Operations Manager для применения политики при консолидации и балансировке нагрузки в вычислительных ресурсах кластера.

В vRealize Automation необходимо настроить конечные точки, создать группу структуры и добавить резервирования. В vRealize Operations Manager необходимо настроить политику поддержки балансировки нагрузки и применить ее к настраиваемой группе, которая содержит настраиваемые вычислительные ресурсы.

Необходимые условия

Чтобы политика размещения могла предлагать для схем элементов варианты мест назначения для размещений в схемах элементов, необходимо выполнить ряд действий.

- Изучить политику размещения. См. раздел [Политика размещения](#).
- Проверить наличие конечной точки в vRealize Automation для экземпляра vRealize Operations Manager, который используется для размещения рабочей нагрузки. См. раздел [Создание конечной точки vRealize Operations Manager](#).

- Проверить наличие конечной точки в vRealize Automation для экземпляра vCenter Server. См. раздел [Создание конечной точки vSphere в vRealize Automation и ее связывание с NSX](#).
- Добавить резервирования в конечную точку vCenter Server. См. раздел [Резервирования](#).
- Добавить группу структуры и убедиться в том, что ваша учетная запись назначена администратором группы структуры. См. раздел [Создание групп структур](#).
- Убедиться в том, что vRealize Operations Manager осуществляет мониторинг той же инфраструктуры, что и vRealize Automation, чтобы подтвердить, что они содержат одинаковые экземпляры vCenter Server. См. раздел [Решение VMware vSphere в vRealize Operations Manager](#) в Информационном центре по vRealize Operations Manager.
- Изучить резервирования, резервирование хранилища, схемы элементов и делегировать поставщиков. См. разделы в vRealize Automation Информационном центре.
- Изучите и определите настройки заполнения и балансировки в политике vRealize Operations Manager, которая используется для размещения рабочей нагрузки. См. раздел [Сведения об автоматизации рабочих нагрузок](#) в Информационном центре по vRealize Operations Manager.

Процедура

1. Настройка vRealize Automation для размещения рабочей нагрузки

Чтобы использовать аналитические данные по размещению рабочей нагрузки для размещения компьютеров во время развертывания новых схем элементов, необходимо подготовить экземпляр vRealize Automation.

2. Настройка vRealize Operations Manager для размещения рабочей нагрузки в vRealize Automation

Чтобы предоставить vRealize Automation аналитические данные по размещению рабочей нагрузки для размещения компьютеров во время развертывания новых схем элементов, необходимо подготовить экземпляр vRealize Operations Manager.

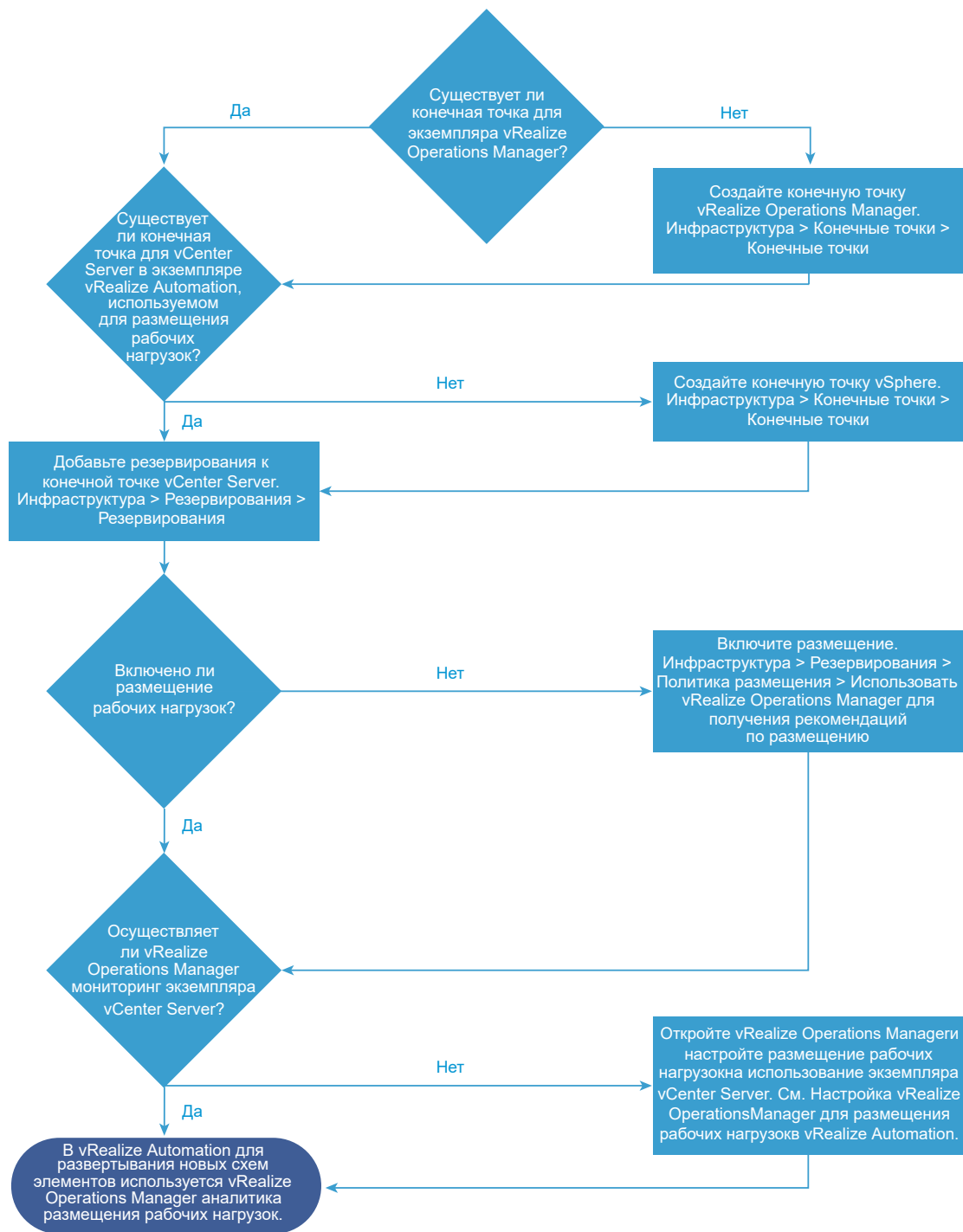
Результаты

vRealize Automation и vRealize Operations Manager настроены для использования аналитических данных о размещении рабочей нагрузки, чтобы предлагать для новых схем элементов варианты мест назначения для размещения.

Настройка vRealize Automation для размещения рабочей нагрузки

Чтобы использовать аналитические данные по размещению рабочей нагрузки для размещения компьютеров во время развертывания новых схем элементов, необходимо подготовить экземпляр vRealize Automation.

Чтобы подготовить экземпляр vRealize Automation для использования политики размещения, необходимо настроить конечные точки, создать группу структуры и добавить резервирования.



Необходимые условия

- Чтобы использовать размещение рабочей нагрузки, необходимо изучить соответствующие требования. См. раздел [Настройка размещения рабочей нагрузки](#).
- В vRealize Automation добавьте отдельную роль и разрешения пользователя для проверки учетных данных в vRealize Operations Manager. См. раздел «Описание ролей» в vRealize Automation Информационном центре.

Процедура

1. В экземпляре vRealize Automation добавьте конечную точку для экземпляра vRealize Operations Manager и нажмите **ОК**.

- а) Выберите **Инфраструктура > Конечная точка > Конечные точки**.
- б) Выберите **Создать > Управление > vRealize Operations Manager**.
- в) Укажите общие сведения для конечной точки **vRealize Operations Manager**.

Задавать свойства для конечной точки не требуется.

2. В экземпляре vRealize Automation добавьте конечную точку для экземпляра vCenter Server и нажмите **ОК**.

- а) Выберите **Инфраструктура > Конечная точка > Конечные точки**.
- б) Выберите элементы **Создать > Виртуальный > vSphere (vCenter)**.
- в) Укажите общие сведения, свойства и связи для конечной точки vCenter Server.

После того как пользователь добавит конечные точки и vRealize Automation выполнит сбор данных, для этих конечных точек станут доступны вычислительные ресурсы. Затем можно добавить эти вычислительные ресурсы в созданную группу структуры.

3. Создайте группу структуры, чтобы остальные пользователи могли создать резервирования, и включите политику размещения.

- а) Выберите **Инфраструктура > Конечная точка > Группы структур**.
- б) Нажмите **Создать** и укажите сведения о группе структуры.

Параметр	Описание
Имя	Укажите значимое имя для группы структуры.
Описание	Укажите подробное описание.
Администраторы структуры	Укажите адрес электронной почты всех пользователей, которых необходимо назначить администраторами структуры.
Вычислительные ресурсы	Выберите кластеры вычислительных ресурсов, которыми может управлять администратор.

После добавления вычислительных ресурсов в группу структуры, когда vRealize Automation выполнит сбор данных, администраторы структуры смогут создать резервирования вычислительных ресурсов.

4. Создайте резервирования вычислительных ресурсов в экземпляре vCenter Server.

- а) Выберите **Инфраструктура > Резервирования > Резервирования**.
- б) Выберите **Создать > vSphere (vCenter)**.
- в) На каждой вкладке укажите сведения о резервировании.

Параметр	Действие
Общие	Выберите политику резервирования, установите приоритет для политики и нажмите Включить это резервирование .
Ресурсы	Выберите квоту на компьютеры, память и хранилище. Выбирать пул ресурсов не требуется.
Сеть	Выберите сетевой адаптер. Выбирать профиль сети не требуется.
Свойства	При необходимости добавьте настраиваемые свойства для резервирования.
Оповещение	При необходимости выберите Оповещение о емкости , чтобы уведомлять получателей о превышении порогового значения емкости для резервирования.

5. Включите политику размещения.

- а) Выберите **Инфраструктура > Резервирования > Политика размещения**.
- б) Установите флажок **Использовать vRealize Operations Manager для рекомендаций по размещению**.

Результаты

vRealize Automation настроен для использования аналитических данных из vRealize Operations Manager для размещения компьютеров при развертывании пользователями схем элементов.

Следующие шаги

Настройте vRealize Operations Manager для мониторинга экземпляра vCenter Server и примените политику размещения рабочей нагрузки для вычислительных ресурсов кластера. См. раздел [Настройка vRealize Operations Manager для размещения рабочей нагрузки в vRealize Automation](#).

Настройка vRealize Operations Manager для размещения рабочей нагрузки в vRealize Automation

Чтобы предоставить vRealize Automation аналитические данные по размещению рабочей нагрузки для размещения компьютеров во время развертывания новых схем элементов, необходимо подготовить экземпляр vRealize Operations Manager.

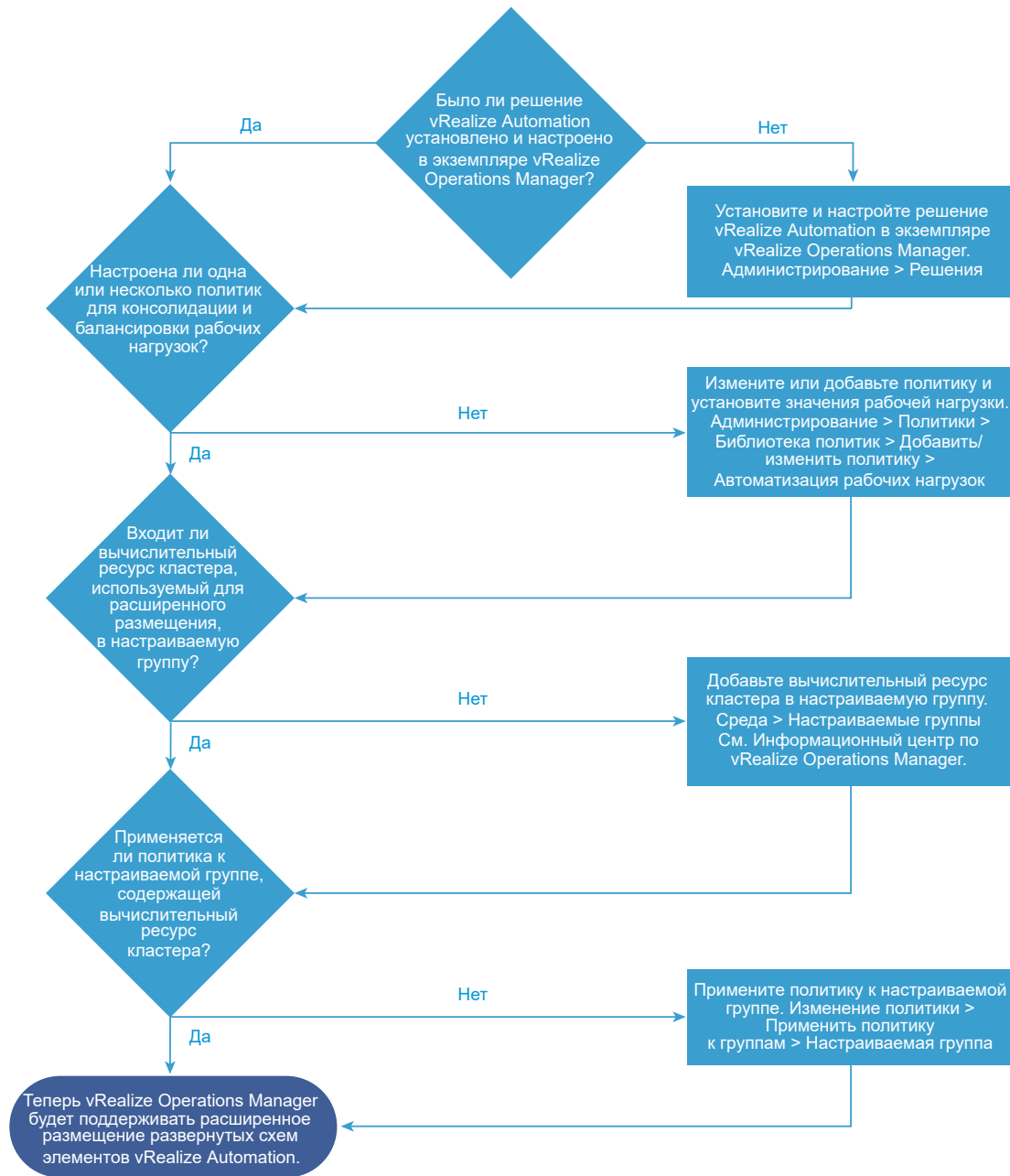
Осторожно! Решение vRealize Automation, которое включает пакет управления, необходимо установить только в одном экземпляре vRealize Operations Manager.

Чтобы подготовить экземпляр vRealize Operations Manager для предоставления аналитических данных vRealize Automation, необходимо установить и настроить решение vRealize Automation. Необходимо также настроить политику и применить ее для вычислительных ресурсов кластера.

После настройки решения vRealize Automation невозможно будет переместить или перебалансировать виртуальные машины, которыми управляет vRealize Automation.

Если в экземпляре vRealize Operations Manager не установлено решение vRealize Automation, можно с помощью размещения рабочей нагрузки переместить или перебалансировать виртуальные машины, которыми управляет vRealize Automation.

Виртуальные машины, перемещаемые с помощью размещения рабочей нагрузки, должны находиться в центре обработки данных или настраиваемом центре обработки данных.



Необходимые условия

- Настройка vRealize Automation для использования аналитических данных по размещению рабочей нагрузки. См. раздел [Настройка vRealize Automation для размещения рабочей нагрузки](#).

- Убедитесь в том, что решение vRealize Automation установлено и настроено в экземпляре vRealize Operations Manager, который используется для размещения рабочей нагрузки. Сведения о решении см. в разделе [Management Pack для vRealize Automation в Solution Exchange](#). Сведения о размещении рабочей нагрузки в vRealize Operations Manager см. в разделе [Сведения об автоматизации нагрузки](#) и соответствующих темах в документации по vRealize Operations Manager.

Процедура

1. В экземпляре vRealize Operations Manager, который управляет размещением рабочей нагрузки, необходимо установить и настроить решение vRealize Automation.

Решение может быть уже установлено.

- а) Для просмотра уже установленных в vRealize Operations Manager решений выберите **Администрирование > Решения**.

- б) Убедитесь в том, что решение vRealize Automation уже установлено.

Если решение vRealize Automation отсутствует в списке, загрузите и установите его. См. раздел [Management Pack для vRealize Automation в Solution Exchange](#).

- в) Если решение представлено в списке, выберите **Решение VMware vRealize Automation** и нажмите **Настроить**.

- г) Настройте решение vRealize Automation и сохраните настройки.

Дополнительные сведения о настройке решения см. в разделе [Решения в vRealize Operations Manager](#) в Информационном центре vRealize Operations Manager.

2. Если не используется политика по умолчанию для vRealize Operations Manager, необходимо создать настраиваемую группу. Затем следует добавить в настраиваемую группу вычислительные ресурсы кластера.

Чтобы применить для кластеров политику, отличную от политики по умолчанию, необходимо добавить настраиваемую группу. После этого можно применить политику к настраиваемой группе. Если используется политика по умолчанию, создавать настраиваемую группу не требуется, так как политика по умолчанию будет применяться для всех объектов.

- а) Нажмите **Среда > Настраиваемые группы**.

- б) Если настраиваемая группа для кластеров не существует, необходимо ее создать.

Дополнительные сведения см. в разделе [Пользовательский сценарий: создание настраиваемых групп объектов](#) в Информационном центре vRealize Operations Manager.

- в) Добавьте кластеры в настраиваемую группу и сохраните группу.

3. Настройте политику для консолидации и балансировки нагрузки в кластерах и примените ее для настраиваемой группы.

Политика в vRealize Operations Manager настраивается для задания параметров консолидации, балансировки, заполнения, а также параметров управления ресурсами ЦП, памятью и пространством на диске. Например, можно изменить параметр с именем «Объединение рабочих нагрузок», чтобы

определить оптимальное размещение для новых управляемых нагрузок с учетом статуса кластера и его емкости. Можно также изменить пороговое значение для балансировки нагрузок, установив уровень агрессивности, требуемый для размещения нагрузок. Можно настроить одну или несколько политик и применить их для вычислительных ресурсов кластера.

- а) Чтобы найти нужную политику, выберите **Администрирование > Политики > Библиотека политик**.
- б) Для задания значения нагрузки выберите **Добавить/редактировать политику** и нажмите **Автоматизация нагрузки**.

Параметры с именем «Объединение рабочих нагрузок» и «Высота кластера» применяются к изначальному размещению виртуальных машин.

- Когда для параметра «Объединение рабочих нагрузок» установлено значение **нет**, функция размещения рабочей нагрузки распределяет нагрузку среди всех кластеров, к которым применяется политика. Когда для параметра «Объединение рабочих нагрузок» установлено какое-либо другое значение, функция размещения рабочей нагрузки первым загружает наиболее занятый кластер.
- «Высота кластера» — это зарезервированный в кластере объем буфера, выраженный в процентах от общего объема. Например, если задать высоту кластера 20%, то такой буфер может помешать функции размещения рабочей нагрузки разместить виртуальные машины в данном кластере. Это связано с тем, что в кластере остается меньше 20% свободной емкости для ЦП, памяти или дискового пространства.

- в) В рабочем пространстве политики выберите **Применить политику для групп**.
- г) Выберите настраиваемую группу.
- д) Сохраните политику.

Результаты

Настройки vRealize Operations Manager предполагают, что vRealize Automation будет использовать аналитические данные о размещении рабочей нагрузки, чтобы предлагать путь назначения для размещения на компьютерах, где пользователи разворачивают схемы элементов.

Следующие шаги

Дождитесь, когда vRealize Automation и vRealize Operations Manager завершат сбор данных с конечных точек и объектов в среде. Затем после развертывания новых схем элементов vRealize Automation отобразит рекомендации относительно размещения рабочей нагрузки, возможные пути назначения и отдельные размещения, которые требуется подтвердить.

Устранение неполадок при размещении рабочей нагрузки

При возникновении проблем с размещением рабочей нагрузки используйте информацию об устранении неполадок.

Для правильного размещения рабочих нагрузок требуется решение vRealize Automation

Размещение рабочей нагрузки основывается на отдельных компьютерах, при этом оно осуществляется на уровне компьютера. Если vRealize Automation и vRealize Operations Manager установлены вместе, также должно быть установлено решение vRealize Automation.

Это решение включает в себя пакет управления и адаптер. Оно позволяет определить кластеры, где деактивированы действия повторная балансировка контейнера или перемещение виртуальной машины. Действие повторной балансировки деактивировано в пользовательском центре обработки данных, к которому относится этот кластер.

- Для неуправляемых кластеров vRealize Automation, относящихся к пользовательскому центру обработки данных, у которого нет управляемых кластеров vRealize Automation, операции перемещение виртуальной машины и повторная балансировка контейнера включены. Эти действия деактивированы для управляемых кластеров vRealize Automation.
- В случае с vRealize Operations Manager адаптер vRealize Automation является причиной того, что виртуальные машины в кластерах, сопоставляющих резервирования, не будут доступны для перемещения или повторной балансировки.

Осторожно! Решение vRealize Automation должно быть установлено только на одном экземпляре vRealize Operations Manager.

Включен режим высокой доступности, хотя он должен быть деактивирован

Когда включен режим высокой доступности, а vRealize Operations Manager не работает, время ожидания вызова vRealize Operations Manager для размещения рабочих нагрузок может завершиться сбоем.

vRealize Automation заносит ошибки размещения рабочей нагрузки в файл журнала `catalina.out`.

Мониторинг конечных точек vSphere в vRealize Automation не выполняется

В vRealize Operations Manager не отслеживается экземпляр vSphere vCenter Server, который содержит кластеры резервирования.

Если при попытке размещения vRealize Operations Manager не распознает потенциальные резервирования vRealize Automation для кластера, хранилища данных или кластера хранилища данных, эти резервирования игнорируются. vRealize Operations Manager передает vRealize Automation ответное сообщение о том, что резервирования не найдены.

В результате в сведениях о размещении после выполнения запроса vRealize Automation рядом с потенциальным резервированием отображает значок предупреждения, который показывает, что данное резервирование не распознано.

При возникновении расхождения vRealize Automation появляется в верхней части списка

vRealize Automation и vRealize Operations Manager управляют различными представлениями инфраструктуры. Но они оба должны управлять одними и теми же экземплярами vCenter Server в одной инфраструктуре.

Требуется выявление отключений и расхождений, а также отображение подробных сведений.

Что делать, если адаптер vRealize Automation не работает

Первоначальное размещение всегда учитывает список вариантов целевых точек, полученный от vRealize Operations Manager, например когда пользователь добавляет кластер сразу же после установки.

В случае отсутствия в vRealize Operations Manager решения vRealize Automation, включающего пакет управления и адаптер, доступны действия перемещение виртуальной машины и повторная балансировка контейнера.

Непрерывная оптимизация с помощью vRealize Operations Manager

Непрерывная оптимизация обеспечивает постоянное автономное управление рабочими нагрузками vRealize Automation с помощью vRealize Operations Manager.

Непрерывная оптимизация обеспечивает перераспределение и перемещение рабочей нагрузки и использование vRealize Automation при помощи vRealize Operations Manager после исходного размещения рабочей нагрузки. Если ресурсы виртуализации перемещаются или изменяется нагрузка на них, то подготовленные рабочие нагрузки vRealize Automation можно перемещать по мере необходимости.

- Служба непрерывной оптимизации автоматически создает в vRealize Operations Manager новый центр обработки данных.

Для каждой конечной точки vCenter vRealize Automation создается новый центр обработки данных.

- Созданный центр обработки данных содержит каждый управляемый кластер vRealize Automation, связанный с данной конечной точкой.

Примечание Не нужно вручную создавать смешанный центр обработки данных для кластеров vRealize Automation и кластеров не на базе vRealize Automation.

- Непрерывную оптимизацию можно запустить только из такого созданного центра обработки данных на основе vRealize Automation.
- Оптимизация не поддерживает разные требования резервирования для разных кластеров в vCenter, которые могут возникнуть при наличии разных бизнес-групп.

Оптимизация выполняется на уровне центра обработки данных на основе vRealize Automation, и разные требования резервирования для разных кластеров могут помешать успеху этой операции. В этом случае выдается сообщение об ошибке с разъяснением, что некоторые целевые кластеры или хранилища не отвечают требованиям, и это не позволяет выполнить некоторые действия оптимизации.

- Оптимизация никогда не создает нарушений политик vRealize Automation или vRealize Operations Manager.
 - Если в данный момент существуют нарушения политики, служба оптимизации может исправить проблемы, связанные с эксплуатационной задачей vRealize Operations Manager.
 - Если в данный момент существуют нарушения политики, служба оптимизации не может исправить проблемы, связанные с бизнес-задачей vRealize Operations Manager.

Например, если виртуальная машина вручную перемещена в какой-либо кластер, который не был частью ее политики резервирования, vRealize Operations Manager не определяет такое нарушение и не будет пытаться устранить его. Чтобы устранить проблемы, связанные с бизнес-задачами, необходимо переместить эту рабочую нагрузку при помощи vRealize Automation.

- Данный выпуск подчиняется эксплуатационной задаче на уровне центра обработки данных. Все кластеры — участники vRealize Automation оптимизируются в соответствии с аналогичными параметрами.

Чтобы задать различные эксплуатационные задачи для кластеров, необходимо настроить их в отдельных центрах обработки данных vRealize Automation, связанных с отдельными конечными точками vCenter. Одним из примеров такой ситуации может быть разделение кластера тестирования и производственного кластера.

- vRealize Operations Manager запрашивает у vRealize Automation возможность размещения с учетом политик и резервирований vRealize Automation.
- Теги размещения vRealize Operations Manager не могут применяться к рабочим нагрузкам, подготовленным с помощью vRealize Automation.

Кроме того, поддерживается запланированная оптимизация с участием нескольких компьютеров. Регулярные запланированные сеансы оптимизации не предполагают обязательного выполнения всех предусмотренных задач. Если возникают условия, прерывающие перемещение компьютеров, успешно перемещенные компьютеры остаются в новой среде, а в ходе следующего цикла vRealize Operations Manager пытается переместить оставшиеся компьютеры в режиме, обычном для vRealize Operations Manager. Такая частично выполненная оптимизация не приводит к отрицательным последствиям для vRealize Automation.

Поиск несбалансированных рабочих нагрузок в vRealize Automation

vRealize Automation может обнаружить ситуацию, когда много рабочих нагрузок подготавливаются в одном кластере.

Процедура

1. Чтобы увидеть, где подготавливаются рабочие нагрузки, выберите **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**.
Обратите внимание на неравномерное размещение компьютеров.
2. Резервирование может привести к большому числу подготавливаемых компьютеров в одном кластере. Чтобы просмотреть резервирования, нажмите **Инфраструктура > Резервирования > Резервирования**.

Обратите внимание на приоритеты и на то, как они могут повлиять на размещение компьютеров.

Включение непрерывной оптимизации

При добавлении адаптера vRealize Automation в vRealize Operations Manager vRealize Operations Manager автоматически создает новый выделенный центр обработки данных для рабочих нагрузок на основе vRealize Automation.

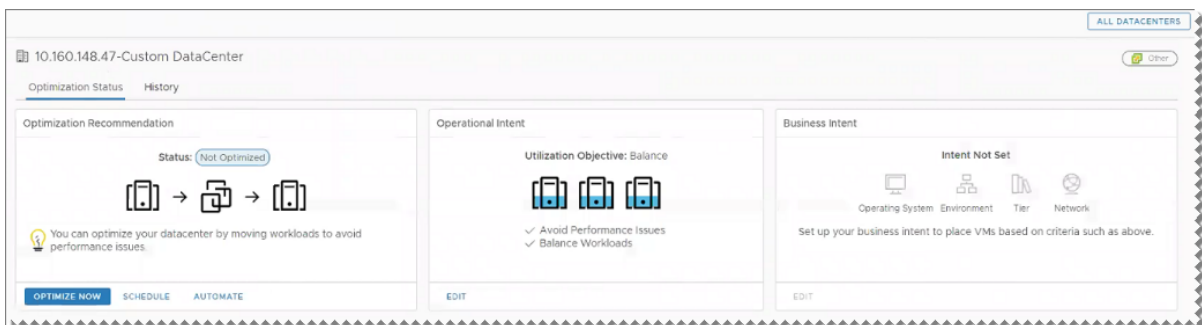
Другие действия по установке для организации непрерывной оптимизации, помимо добавления адаптера, не требуются. В созданном центре обработки данных можно настраивать и использовать vRealize Operations Manager для перемещения рабочих нагрузок. См. раздел [Пример непрерывной оптимизации](#).

Пример непрерывной оптимизации

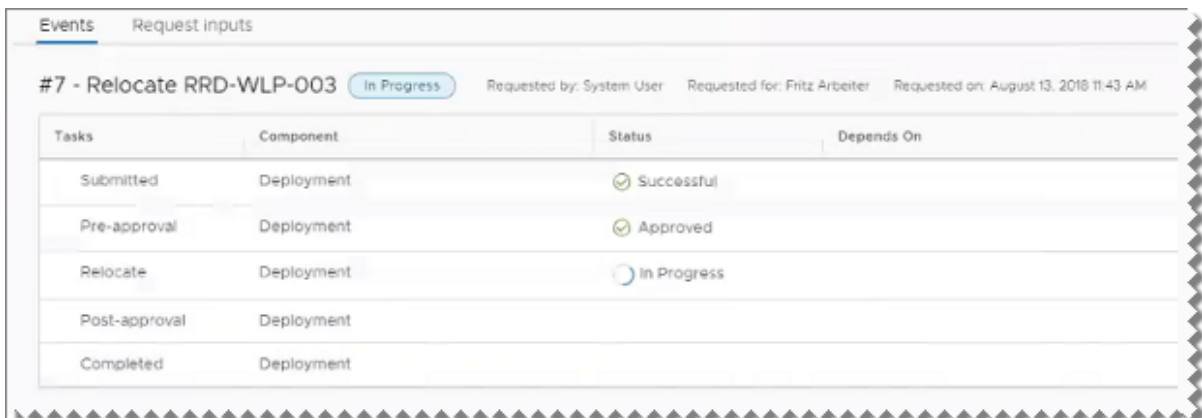
В следующем примере показан рабочий процесс изменения балансировки для непрерывной оптимизации vRealize Automation при помощи vRealize Operations Manager.

1. На главной странице vRealize Operations Manager выберите **Оптимизация рабочей нагрузки**.
2. Выберите автоматически созданный центр обработки данных vRealize Automation.
3. В разделе **Эксплуатационная задача** нажмите **Изменить** и выберите **Балансировка**.

Нельзя выбрать или изменить бизнес-задачу, которая деактивирована, если центр обработки данных используется для оптимизации vRealize Automation.

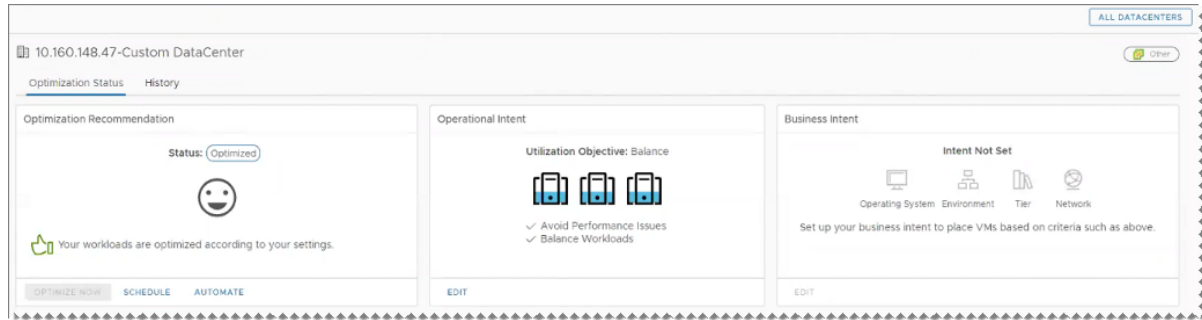


4. В разделе **Рекомендации по оптимизации** нажмите **Оптимизировать сейчас**.
vRealize Operations Manager отобразит схему состояния до и после предлагаемой операции.
5. Нажмите кнопку **Далее**.
6. Нажмите **Начать действие**.
7. В vRealize Automation можно отслеживать выполнение данной операции, если нажать **Развертывания** и следить за состоянием события.



Когда перераспределения завершается, окно vRealize Automation обновляется. На странице вычислительных ресурсов будет указано, что компьютеры перемещены.

В vRealize Operations Manager результаты следующего сбора данных изменятся с учетом завершения данной оптимизации.



В vRealize Operations Manager можно просмотреть данную операцию, перейдя в меню:

Администрирование > Журнал > Последние задачи.

Поиск центров обработки данных vRealize Automation в vRealize Operations Manager

vRealize Operations Manager можно использовать для отображения только тех центров обработки данных, которые управляются vRealize Automation.

Процедура

1. На главной странице vRealize Operations Manager выберите **Оптимизация рабочей нагрузки**.
2. В правом верхнем углу нажмите раскрывающееся меню **Просмотр**.
3. Выберите только центры обработки данных, управляемые vRealize Automation.



Управление парами ключей

Пары ключей используются для подготовки экземпляра облака и подключения к нему. Пара ключей используется для расшифровки паролей Windows или выполнения входа в компьютер Linux.

Пары ключей требуются для подготовки с использованием Amazon Web Services. Для Red Hat OpenStack пары ключей необязательны.

Существующие пары ключей импортируются в ходе сбора данных при добавлении конечной точки облака. Администратор структуры может также создавать пары ключей и управлять ими с помощью консоли vRealize Automation. При удалении пары ключей из консоли vRealize Automation она также удаляется из учетной записи для облачных служб.

Кроме управления парами ключей вручную, можно настроить vRealize Automation для автоматического создания пар ключей для компьютера или бизнес-группы.

- Администратор структуры может настроить автоматическое создание пар ключей на уровне резервирования.
- Если управление парой ключей будет осуществляться на уровне схемы элементов, администратору следует выбрать в резервировании **Не указано**.
- Администратор арендатора или диспетчер бизнес-групп может настроить автоматическое создание пар ключей на уровне схемы элементов.
- Если создание пар ключей настроено на уровне резервирования и схемы элементов, уровень резервирования является более приоритетным.

Создание пары ключей

Пары ключей, которые будут использоваться с конечными точками, можно создать с помощью vRealize Automation.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Создайте конечную точку в облаке и добавьте свои облачные вычислительные ресурсы в группу структур. См. [Выбор сценария конечной точки](#) и [Создание групп структур](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Пары ключей**.
2. Нажмите кнопку **Создать**.
3. В текстовом поле **Имя** введите имя.
4. Выберите регион облака в раскрывающемся списке **Вычислительный ресурс**.
5. Нажмите кнопку **ОК**.

Результаты

Пара ключей готова к использованию, когда столбец «Секретный ключ» содержит значение *****.

Отправка закрытого ключа для пары ключей

Закрытый ключ можно отправить для пары ключей в формате PEM.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Наличие пары ключей. См. [Создание пары ключей](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Пары ключей**.

2. Найдите пару ключей, для которой нужно отправить закрытый ключ.
3. Щелкните значок **Изменить** (✎).
4. Отправьте ключ одним из следующих способов.
 - Найдите файл в кодировке PEM и щелкните элемент **Передать**.
 - Вставьте в закрытый ключ текст, который начинается с ----- BEGIN RSA PRIVATE KEY----- и заканчивается на ----- END RSA PRIVATE KEY-----.
5. Щелкните значок **Сохранить** (✓).

Экспорт закрытого ключа из пары ключей

Можно экспортировать закрытый ключ из пары ключей в файл в кодировке PEM.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Требуется пара ключей с закрытым ключом. См. [Отправка закрытого ключа для пары ключей](#).

Процедура

1. Выберите **Инфраструктура > Резервирования > Пары ключей**.
2. Найдите пару ключей, из которой нужно экспортировать закрытый ключ.
3. Щелкните значок **Экспорт** (📄).
4. Укажите место для сохранения файла и нажмите кнопку **Сохранить**.

Сценарий: применение размещения к вычислительному ресурсу при развертываниях в нескольких регионах

Администратор структуры может назначать метки вычислительным ресурсам в зависимости от их принадлежности к тому или иному центру обработки данных, чтобы обеспечить поддержку развертывания в нескольких регионах. Если архитекторы включают функцию определения расположения для схем элементов, пользователи смогут выбрать, какой центр обработки данных следует использовать для подготовки компьютеров — в Бостоне или Лондоне.



При наличии центра обработки данных в Лондоне и Бостоне нельзя, чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Лондона и наоборот. Чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Бостона, а пользователи Лондона — в инфраструктуре Лондона, необходимо разрешить пользователям выбирать соответствующее расположение для подготовки при запросе компьютеров.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора структуры**.
- Определите расположение центров обработки данных, используя права системного администратора. См. [Сценарий: добавление данных о расположении центра обработки данных при развертываниях в нескольких регионах](#).

Процедура

1. Выберите **Инфраструктура > Вычислительные ресурсы > Вычислительные ресурсы**.
2. Укажите вычислительный ресурс, расположенный в центре обработки данных в Бостоне, и нажмите кнопку **Изменить**.
3. В раскрывающемся меню **Расположения** выберите Бостон.
4. Нажмите кнопку **ОК**.
5. Повторите эту процедуру, если необходимо связать вычислительные ресурсы с центром в Бостоне и Лондоне.

Результаты

Архитекторы инфраструктуры как услуги могут включать функцию выбора расположения, чтобы пользователи могли выбирать расположение для подготовки компьютера (Лондон или Бостон) во время заполнения формы элемента каталога. См. [Предоставление пользователям возможности выбирать расположение центра обработки данных при развертываниях в нескольких регионах](#).

Подготовка развертывания vRealize Automation с использованием решений для управления IP-адресами стороннего поставщика

IP-адреса и диапазоны IP-адресов для использования в профиле сети vRealize Automation можно получить у поддерживаемого стороннего поставщика решений для управления IP-адресами, такого как Infoblox.

Диапазоны IP-адресов в профиле сети используются в связанной резервации, указываемой в схеме элементов. Когда уполномоченный пользователь запрашивает подготовку компьютера с помощью элемента каталога схемы элементов, IP-адрес получают из назначенного сторонним поставщиком диапазона IP-адресов. После развертывания компьютера использованный IP-адрес можно увидеть, запросив страницу сведений об элементе vRealize Automation.

Таблица 2-19. Подготовка к процессу подготовки развертывания vRealize Automation с помощью контрольного списка службы управления IP-адресами Infoblox

Задача	Описание	Сведения
Получение, импорт и настройка подключаемого модуля или пакета стороннего поставщика решений для управления IP-адресами.	Получите и импортируйте подключаемый модуль vRealize Orchestrator, запустите рабочие процессы конфигурации vRealize Orchestrator и зарегистрируйте тип конечной точки поставщика управления IP-адресами в vRealize Orchestrator. Если на портале VMware Solution Exchange по адресу https://marketplace.vmware.com/vsx отсутствует необходимый пакет поставщика управления IP-адресами, можно создать собственный пакет с помощью комплекта SDK поставщика управления IP-адресами и сопроводительной документации. См. страницу vRealize Automation Example Third-Party IPAM Package («Пример интеграции стороннего решения для управления IP-адресами с vRealize Automation») по адресу code.vmware.com/web/sdk .	См. раздел Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами .
Создание конечной точки стороннего поставщика решений для управления IP-адресами.	Создайте новую конечную точку управления IP-адресами в vRealize Automation.	См. раздел Создание конечной точки стороннего поставщика управления IP-адресами .
Задание параметров конечной точки стороннего поставщика решений для управления IP-адресами в профиле внешней сети.	Создайте профиль внешней сети и укажите заданную конечную точку управления IP-адресами в vRealize Automation.	См. раздел Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами .
При необходимости: задание параметров конечной точки стороннего поставщика решений для управления IP-адресами в профиле маршрутизируемой сети.	Создайте профиль сети по требованию и укажите заданную конечную точку управления IP-адресами в vRealize Automation.	См. раздел Создание профиля маршрутизируемой сети с помощью сторонней конечной точки управления IP-адресами или Создание профиля сети NAT в vRealize Automation с помощью сторонней конечной точки управления IP-адресами .
Определение резервирования для использования профиля сети.	Создайте резервирование, которое вызывает профиль сети в vRealize Automation	См. раздел Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer .
Определение схемы элементов, в которой будет использоваться профиль сети.	Создайте схему элементов, в которой используется резервирование в vRealize Automation.	См. раздел Глава 3 Предоставление пользователям схем элементов служб .
Публикация схемы элементов в каталоге, чтобы она стала доступна для использования.	Опубликуйте схему элементов в каталоге в vRealize Automation. Добавьте необходимые права.	См. раздел Публикация схемы элементов .
Запрос подготовки компьютера с помощью элемента каталога, который является схемой элементов.	С помощью элемента каталога, который является схемой элементов, запросите подготовку компьютера в vRealize Automation	См. раздел Управление каталогом служб .

Настройка ресурсов Все как услуга

С помощью настройки конечных точек Все как услуга можно подключить vRealize Automation к среде. При настройке подключаемых модулей vRealize Orchestrator в качестве конечных точек используется интерфейс пользователя vRealize Automation, а не интерфейс конфигурации vRealize Orchestrator.

Чтобы использовать возможности vRealize Orchestrator и подключаемые модули vRealize Orchestrator, позволяющие применять технологии компании VMware и сторонних поставщиков в vRealize Automation, можно настроить подключаемые модули vRealize Orchestrator, добавив их в качестве конечных точек. Таким образом можно создать подключения к различным узлам и серверам, например к экземплярам vCenter Server, узлу Microsoft Active Directory и т. д.

При добавлении подключаемого модуля vRealize Orchestrator в качестве конечной точки в интерфейсе пользователя vRealize Automation на сервере vRealize Orchestrator по умолчанию выполняется рабочий процесс конфигурации. Такие рабочие процессы находятся в папке рабочих процессов, которую можно открыть, последовательно выбрав **vRealize Automation > Все как услуга > Конфигурация конечной точки**.

Важно! Настройка одного подключаемого модуля в vRealize Orchestrator и консоли vRealize Automation не поддерживается. Попытка сделать это приведет к возникновению ошибок.

Настройка подключаемого модуля Active Directory в качестве конечной точки

Для подключения к выполняющемуся экземпляру Active Directory, а также для управления пользователями и группами пользователей, компьютерами Active Directory, организационными единицами и так далее можно добавить конечную точку и настроить подключаемый модуль Active Directory.

После добавления конечной точки Active Directory ее можно обновить в любое время.

Необходимые условия

- Убедитесь, что у вас есть доступ к экземпляру Microsoft Active Directory. См. документацию по Microsoft Active Directory.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.
3. В раскрывающемся меню **Подключаемый модуль** выберите **Active Directory**.
4. Нажмите кнопку **Далее**.
5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.

7. Настройте сведения о сервере Active Directory.

- а) В текстовом поле **IP/URL узла Active Directory** введите IP-адрес или имя DNS для узла, в котором выполняется Active Directory.

- б) В текстовом поле **Порт** введите порт поиска своего сервера Active Directory.

vRealize Orchestrator поддерживает иерархическую структуру доменов Active Directory. Если контроллер домена настроен на использование глобального каталога, необходимо использовать порт 3268. Для подключения к серверу глобального каталога порт по умолчанию 389 использовать нельзя. Помимо портов 389 и 3268, можно использовать порт 636 для LDAPS.

- в) Введите корневой элемент службы Active Directory в текстовом поле **Корневой**.

Например, если имя домена — *mycompany.com*, корневой Active Directory — **dc=mycompany,dc=com**.

Этот узел используется для поиска в каталоге служб после ввода соответствующих учетных данных. Для крупных каталогов служб указание узла в дереве позволяет сузить операцию поиска и повышает производительность. Например, вместо поиска по всему каталогу, можно указать **ou=employees,dc=mycompany,dc=com**. Этот корневой элемент отображает всех пользователей в группе «Сотрудники».

- г) (дополнительно) Для активации шифрованной сертификации для соединения между vRealize Orchestrator и Active Directory нажмите **Да** в раскрывающемся меню **Использовать SSL**.

Сертификат SSL импортируется автоматически. Подтверждение не запрашивается даже в том случае, если сертификат является самозаверяющим.

- д) (дополнительно) Введите домен в текстовом поле **Домен по умолчанию**.

Например, если ваше имя домена — *mycompany.com*, наберите **@mycompany.com**.

8. Настройте параметры общего сеанса.

Эти учетные данные используются vRealize Orchestrator, чтобы выполнять все рабочие процессы и действия Active Directory.

- а) Введите имя пользователя для общего сеанса в текстовом поле **Имя пользователя для общего сеанса**.

- а) Введите пароль для общего сеанса в текстовом поле **Пароль для общего сеанса**.

9. Щелкните элемент **Готово**.

Результаты

Вы добавили экземпляр Active Directory как конечную точку. Разработчики архитектуры Все как услуга могут использовать Все как услуга для публикации рабочих процессов подключаемого модуля Active Directory в качестве элементов каталога и действий ресурса.

Следующие шаги

- Чтобы использовать схемы элементов vRealize Automation для управления пользователями Active Directory в своей среде, создайте схему элементов Все как услуга на основе Active Directory. Пример см. в разделе [Создание схемы элементов Все как услуга и действия для создания и изменения пользователя](#).
- Чтобы использовать vRealize Automation для создания записей Active Directory при развертывании компьютера, можно создать разные политики Active Directory и применить их к различным бизнес-группам и схемам элементов. См. раздел [Создание и применение политик Active Directory](#).

Настройка подключаемого модуля HTTP-REST в качестве конечной точки

Можно добавить конечную точку и настроить подключаемый модуль HTTP-REST для подключения к узлу REST.

Необходимые условия

- Войдите в vRealize Automation в качестве администратора арендатора.
- Убедитесь, что у вас есть доступ к узлу REST.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать** (+).
3. В раскрывающемся меню **Подключаемый модуль** выберите **HTTP-REST**.
4. Нажмите кнопку **Далее**.
5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Укажите сведения об узле REST.
 - а) В текстовом поле **Имя** укажите имя узла.
 - б) В текстовом поле **URL-адрес** укажите адрес узла.

Примечание При использовании проверки подлинности доступа Kerberos необходимо указать адрес узла в формате полного доменного имени.

- в) (дополнительно) В текстовом поле **Время ожидания подключения (в секундах)** введите время ожидания подключения (в секундах).

Значение по умолчанию — 30 секунд.

- г) (дополнительно) В текстовом поле **Время ожидания операции (в секундах)** введите время ожидания выполнения операции (в секундах).

Значение по умолчанию — 60 секунд.

8. (дополнительно) Настройте параметры прокси-сервера.

- а) В раскрывающемся меню **Использовать прокси-сервер** выберите значение **Да**.
- б) В текстовом поле **Адрес прокси-сервера** укажите IP-адрес прокси-сервера.
- в) Укажите номер порта, который будет использоваться для обмена данными с прокси-сервером, в текстовом поле **Порт прокси-сервера**.

9. Нажмите кнопку **Далее**.**10.** Выберите тип проверки подлинности.

Параметр	Действие
Нет	Проверка подлинности не требуется.
OAuth 1.0	Используется протокол OAuth 1.0. В этом разделе необходимо указать обязательные параметры проверки подлинности в OAuth 1.0. <ul style="list-style-type: none"> а) В текстовом поле Ключ потребителя введите ключ, используемый для идентификации потребителя в качестве поставщика служб. б) В текстовом поле Секрет ключа потребителя введите секрет, чтобы установить владельца ключа потребителя. в) (дополнительно) В текстовом поле Маркер доступа введите маркер доступа, используемый потребителем для доступа к защищенным ресурсам. г) (дополнительно) В текстовом поле Секрет маркера доступа введите секрет, чтобы установить владельца маркера.
OAuth 2.0	Используется протокол OAuth 2.0. В текстовом поле Маркер введите маркер проверки подлинности.
Обычная	Выполняется базовая проверка подлинности доступа. Обмен данными с узлом осуществляется с помощью сеанса общего доступа. <ul style="list-style-type: none"> а) В текстовом поле Имя пользователя проверки подлинности введите имя пользователя общего сеанса. б) В текстовом поле Пароль для проверки подлинности введите пароль общего сеанса.
Дайджест	Выполняется дайджест-проверка подлинности доступа с использованием шифрования. Обмен данными с узлом осуществляется с помощью сеанса общего доступа. <ul style="list-style-type: none"> а) В текстовом поле Имя пользователя проверки подлинности введите имя пользователя общего сеанса. б) В текстовом поле Пароль для проверки подлинности введите пароль общего сеанса.

Параметр	Действие
NTLM	<p>Выполняется проверка подлинности доступа с использованием протокола NTLM в рамках инфраструктуры Windows SSP. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <p>а) Укажите учетные данные пользователя общего сеанса.</p> <ul style="list-style-type: none"> ■ В текстовом поле Имя пользователя проверки подлинности введите имя пользователя общего сеанса. ■ В текстовом поле Пароль для проверки подлинности введите пароль общего сеанса. <p>б) Укажите сведения об NTLM.</p> <ul style="list-style-type: none"> ■ (дополнительно) В текстовом поле Рабочая станция для проверки подлинности NTLM введите имя рабочей станции. ■ В текстовом поле Домен для проверки подлинности NTLM введите доменное имя.
Kerberos	<p>Выполняется проверка подлинности доступа Kerberos. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <p>а) В текстовом поле Имя пользователя проверки подлинности введите имя пользователя общего сеанса.</p> <p>б) В текстовом поле Пароль для проверки подлинности введите пароль общего сеанса.</p>

11. Щелкните элемент **Готово**.

Результаты

Теперь конечная точка настроена, а узел REST добавлен. Разработчики архитектуры Все как услуга могут использовать Все как услуга для публикации рабочих процессов подключаемого модуля HTTP-REST в качестве элементов каталога и действий ресурсов.

Настройка подключаемого модуля PowerShell в качестве конечной точки

Можно добавить конечную точку и настроить подключаемый модуль PowerShell для подключения к работающему узлу PowerShell, что позволит вызывать сценарии и командлеты PowerShell из действий и рабочих процессов vRealize Orchestrator.

Необходимые условия

- Убедитесь, что у вас есть доступ к узлу Windows PowerShell. Дополнительные сведения о Microsoft Windows PowerShell см. в документации к Windows PowerShell.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.
3. В раскрывающемся меню **Подключаемый модуль** выберите **PowerShell**.
4. Нажмите кнопку **Далее**.

5. Введите имя конечной точки PowerShell.
6. (дополнительно) Введите описание конечной точки PowerShell.
7. Нажмите кнопку **Далее**.
8. Укажите сведения об узле PowerShell.
 - а) В текстовом поле **Имя** укажите имя узла.
 - б) В текстовом поле **IP-адрес или узел** укажите IP-адрес или полное доменное имя узла.
9. Настройте параметры WinRM для узла PowerShell.
 - а) В разделе сведений об узле PowerShell в текстовом поле **Порт** введите номер порта, который будет использоваться для обмена данными с узлом.
 - б) Выберите транспортный протокол в раскрывающемся меню **Транспортный протокол**.

Примечание При использовании транспортного протокола HTTPS сертификат удаленного узла PowerShell импортируются в хранилище ключей vRealize Orchestrator.

- в) В раскрывающемся меню **Проверка подлинности** выберите тип проверки подлинности.

Примечание Чтобы использовать проверку подлинности Kerberos, включите соответствующий параметр в службе WinRM. Дополнительные сведения о настройке проверки подлинности Kerberos см. в разделе *Использование подключаемого модуля PowerShell*.

10. В текстовых полях **Имя пользователя** и **Пароль** введите соответствующие учетные данные для взаимодействия с узлом PowerShell с помощью общего сеанса.
11. Щелкните элемент **Готово**.

Результаты

Теперь узел Windows PowerShell добавлен в качестве конечной точки. Разработчики архитектуры Все как услуга могут использовать Все как услуга для публикации рабочих процессов подключаемого модуля PowerShell в качестве элементов каталога и действий ресурсов.

Настройка подключаемого модуля SOAP в качестве конечной точки

Можно добавить конечную точку и настроить подключаемый модуль SOAP для определения службы SOAP в качестве объекта иерархии и выполнения операций SOAP для определенных объектов.

Необходимые условия

- Убедитесь, что у вас есть доступ к узлу SOAP. Подключаемый модуль поддерживает SOAP версии 1.1 и 1.2 и WSDL версии 1.1 и 2.0.
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.

2. Выберите значок **Создать** (+).
3. В раскрывающемся меню **Подключаемый модуль** выберите **SOAP**.
4. Нажмите кнопку **Далее**.
5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Укажите сведения об узле SOAP.
 - а) В текстовом поле **Имя** укажите имя узла.
 - б) В раскрывающемся меню **Указать содержимое WSDL** выберите, следует ли указывать содержимое WSDL в виде текста.

Параметр	Действие
Да	В текстовом поле Содержимое WSDL введите текст WSDL.
Нет	В текстовом поле URL-адрес WSDL введите правильный путь.

- в) (дополнительно) В текстовом поле **Время ожидания подключения (в секундах)** введите время ожидания подключения (в секундах).
Значение по умолчанию — 30 секунд.
- г) (дополнительно) В текстовом поле **Время ожидания запроса (в секундах)** введите время ожидания запроса (в секундах).
Значение по умолчанию — 60 секунд.
8. (дополнительно) Задайте параметры прокси-сервера.
 - а) Чтобы использовать прокси-сервер, в раскрывающемся меню **Прокси-сервер** выберите значение **Да**.
 - б) В текстовом поле **Адрес** укажите IP-адрес прокси-сервера.
 - в) Укажите номер порта, который будет использоваться для обмена данными с прокси-сервером, в текстовом поле **Порт**.
9. Нажмите кнопку **Далее**.
10. Выберите тип проверки подлинности.

Параметр	Действие
Нет	Проверка подлинности не требуется.
Обычная	<p>Выполняется базовая проверка подлинности доступа. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <ol style="list-style-type: none"> а) В текстовом поле Имя пользователя введите имя пользователя общего сеанса. б) В текстовом поле Пароль введите пароль общего сеанса.

Параметр	Действие
Дайджест	<p>Выполняется дайджест-проверка подлинности доступа с использованием шифрования. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <p>а) В текстовом поле Имя пользователя введите имя пользователя общего сеанса.</p> <p>б) В текстовом поле Пароль введите пароль общего сеанса.</p>
NTLM	<p>Выполняется проверка подлинности доступа с использованием протокола NTLM в рамках инфраструктуры Windows SSP. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <p>а) Укажите учетные данные пользователя.</p> <ul style="list-style-type: none"> ■ В текстовом поле Имя пользователя введите имя пользователя общего сеанса. ■ В текстовом поле Пароль введите пароль общего сеанса. <p>б) Задайте параметры NTLM.</p> <ul style="list-style-type: none"> ■ В текстовом поле Домен NTLM введите доменное имя. ■ (дополнительно) В текстовом поле Рабочая станция NTLM введите имя рабочей станции.
Negotiate	<p>Выполняется проверка подлинности доступа Kerberos. Обмен данными с узлом осуществляется с помощью сеанса общего доступа.</p> <p>а) Укажите учетные данные пользователя.</p> <ol style="list-style-type: none"> 1. В текстовом поле Имя пользователя введите имя пользователя общего сеанса. 2. В текстовом поле Пароль введите пароль общего сеанса. <p>б) В текстовое поле SPN службы Kerberos введите SPN службы Kerberos.</p>

11. Щелкните элемент **Готово**.

Результаты

Теперь служба SOAP добавлена. Разработчики архитектуры Все как услуга могут использовать Все как услуга для публикации рабочих процессов подключаемого модуля SOAP в качестве элементов каталога и действий ресурсов.

Настройка подключаемого модуля vCenter Server в качестве конечной точки

Можно добавить конечную точку и настроить подключаемый модуль vCenter Server для подключения к работающему экземпляру vCenter Server, чтобы создать схемы элементов Все как услуга для управления объектами иерархии vSphere.

Необходимые условия

- Установите и настройте vCenter Server. См. раздел *Установка и настройка vSphere*.
- Войдите в vRealize Automation в качестве администратора арендатора.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.

3. Выберите **vCenter Server** в раскрывающемся меню **Подключаемый модуль**.

4. Нажмите кнопку **Далее**.

5. Введите имя и, при необходимости, описание.

6. Нажмите кнопку **Далее**.

7. Введите данные об экземпляре vCenter Server.

- а) Введите IP-адрес или имя DNS для компьютера в текстовом поле **IP-адрес или имя узла добавляемого экземпляра vCenter Server**.

Это — IP-адрес или имя DNS для компьютера, где установлен экземпляр vCenter Server, который требуется добавить.

- б) Введите порт для обмена данными с экземпляром vCenter Server в текстовом поле **Порт экземпляра vCenter Server**.

По умолчанию используется порт 443.

- в) Укажите расположение пакета SDK, который должен использоваться для подключения к экземпляру vCenter Server в текстовом поле **Расположение SDK, используемого для подключения к экземпляру vCenter Server**.

Например, `/sdk`.

8. Нажмите кнопку **Далее**.

9. Определите параметры подключения.

- а) Укажите HTTP-порт экземпляра vCenter Server в текстовом поле **HTTP-порт экземпляра vCenter Server — применимо для подключаемого модуля VC, версия 5.5.2 или ранее**.

- б) Введите учетные данные для vRealize Orchestrator, которые будут использоваться для установления соединения с экземпляром vCenter Server в текстовых полях **Имя пользователя, которого Orchestrator будет использовать для подключения к экземпляру vCenter Server** и **Пароль пользователя, которого Orchestrator будет использовать для подключения к экземпляру vCenter Server**.

Выбираемый пользователь должен быть допустимым пользователем, имеющим права на управление расширениями vCenter Server и набором специальных определяемых привилегий.

10. Щелкните элемент **Готово**.

Результаты

Вы добавили экземпляр vCenter Server в качестве конечной точки. Разработчики архитектуры Все как услуга могут использовать Все как услуга для публикации рабочих процессов подключаемого модуля vCenter Server в качестве элементов каталога и действий ресурса.

Создание конечной точки Microsoft Azure

Можно создать конечную точку Microsoft Azure, чтобы упростить подключение с использованием учетных данных между vRealize Automation и развертыванием Azure.

Конечная точка обеспечивает подключение к ресурсу, в данном случае — экземпляру Azure, который можно использовать для создания схем элементов виртуальной машины. У вас должна быть конечная точка Azure, которая будет использоваться как основа схемы элементов для подготовки виртуальных машин Azure. Если используется несколько подписок Azure, необходимы конечные точки для каждого идентификатора подписки.

Либо можно создать подключение Azure непосредственно из vRealize Orchestrator, используя команду «Добавить подключение Azure» в разделе **Библиотека > Azure > Конфигурация** в дереве рабочих процессов vRealize Orchestrator. Для большинства сценариев рекомендуется использовать подключение через конечную точку (как описано здесь).

Конечные точки Azure поддерживаются vRealize Orchestrator и элементами «Все как услуга». Конечную точку Azure можно создать, удалить и изменить. Если изменить существующую конечную точку и не выполнять никакие обновления на портале Azure через новое подключение в течение нескольких часов, могут возникнуть проблемы. Необходимо перезапустить службу vRealize Orchestrator с помощью команды `service vco-service restart`. Если этого не сделать, могут возникнуть ошибки.

Необходимые условия

- Настройте экземпляр Microsoft Azure и получите действующую подписку Microsoft Azure, позволяющую использовать идентификатор подписки. Подробнее о настройке Azure и получении идентификатора подписки см. в разделе [Настройка конечной точки Microsoft Azure](#).
- Убедитесь, что в развертывании vRealize Automation есть по крайней мере один арендатор и одна бизнес-группа.
- Создайте приложение Active Directory, как описано в разделе <https://azure.microsoft.com/ru-ru/documentation/articles/resource-group-create-service-principal-portal>.
- Запишите указанную далее информацию, связанную с Azure, так как она понадобится во время настройки конечной точки и схемы элементов.
 - идентификатор подписки
 - идентификатор арендатора
 - имя учетной записи хранилища
 - имя группы ресурса
 - расположение
 - имя виртуальной сети
 - идентификатор клиентского приложения
 - секретный ключ клиентского приложения
 - URN образа виртуальной машины
- Развертывание vRealize Automation Azure поддерживается в некоторых регионах распространения Microsoft Azure. См. раздел [Регионы с поддержкой Azure](#).
- Войдите в vRealize Automation в качестве **администратора арендатора**.

Процедура

1. Выберите **Администрирование > Конфигурация vRO > Конечные точки**.
2. Выберите значок **Создать (+)**.
3. На вкладке «Подключаемый модуль» в раскрывающемся меню **Подключаемый модуль** выберите вариант **Azure**.
4. Нажмите кнопку **Далее**.
5. Введите имя и, при необходимости, описание.
6. Нажмите кнопку **Далее**.
7. Заполните текстовые поля на вкладке «Сведения» в соответствии с параметрами конечной точки.

Параметр	Описание
Параметры подключения	
Имя подключения	Уникальное имя для подключения к новой конечной точке. Это имя появится в интерфейсе vRealize Orchestrator, чтобы помочь определить конкретное подключение.
Идентификатор подписки Azure	Идентификатор подписки Azure. Идентификатор определяет учетные записи хранения, виртуальные машины и другие ресурсы Azure, к которым вы имеете доступ.
Среда Azure	Географический регион для развернутого ресурса Azure. vRealize Automation поддерживает все текущие регионы Azure, в зависимости от идентификатора подписки.
Параметры диспетчера ресурсов	
URI-адрес службы Azure	URI-адрес, который обеспечивает доступ к вашему экземпляру Azure. Значение по умолчанию <code>https://management.azure.com/</code> подходит для многих типичных реализаций. Это поле автоматически заполняется при выборе среды.
Идентификатор арендатора	Идентификатор арендатора Azure, который должен использоваться конечной точкой.
Идентификатор клиента	Идентификатор клиента Azure, который должен использоваться конечной точкой. Он назначается при создании приложения Active Directory.
Секретный ключ клиента	Ключ, который используется с идентификатором клиента Azure. Этот ключ назначается при создании приложения Active Directory.
URI-адрес хранилища Azure	URI-адрес, по которому вы получаете доступ к экземпляру хранилища Azure. Это поле автоматически заполняется при выборе среды.
Параметры прокси	

Параметр	Описание
Прокси-узел	Если в компании используется веб-сервер прокси, введите имя узла этого сервера.
Прокси-порт	Если в компании используется веб-сервер прокси, введите номер порта этого сервера.

8. (дополнительно) Выберите элемент «Свойства» и добавьте стандартные настраиваемые свойства, группы свойств или собственные определения настраиваемых свойств.

9. Щелкните элемент **Готово**.

Следующие шаги

Создайте соответствующие группы ресурсов, учетные записи хранения и группы безопасности сети в Azure. Нужно также создать подсистемы балансировки нагрузки, если это необходимо для реализации.

Действие	Параметры
Создание группы ресурсов Azure	<ul style="list-style-type: none"> ■ Создайте группу ресурсов с помощью портала Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Resource/Create resource group. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Вы можете запросить группу ресурсов после того, как свяжите ее со службой и правами. <p>Примечание Тип ресурса «Группа ресурсов» не поддерживается и недоступен для управления в решении vRealize Automation.</p>
Создание учетной записи хранения Azure	<ul style="list-style-type: none"> ■ Создайте учетную запись хранения с помощью Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Storage/Create storage account. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Вы можете запросить учетную запись хранения после того, как свяжите ее со службой и правами.
Создание группы безопасности сети Azure	<ul style="list-style-type: none"> ■ Создайте группу безопасности с помощью Azure. Точные инструкции см. в документации Azure. ■ Используйте соответствующий рабочий процесс vRealize Orchestrator, описанный в разделе Library/Azure/Network/Create Network security group. ■ Создайте и опубликуйте в vRealize Automation схему элементов «Все как услуга», содержащую рабочий процесс vRealize Orchestrator. Группу безопасности можно запросить после того, как она будет связана со службой и правами.

Регионы с поддержкой Azure

Развертывание vRealize Automation Azure поддерживается в некоторых регионах распространения Microsoft Azure.

Ниже перечислены регионы, в которых поддерживается развертывание Azure в рамках vRealize Automation.

- | | |
|---------------------------------|----------------------------------|
| ■ Восточная Азия | ■ Восточная Австралия |
| ■ Юго-восточная Азия | ■ Юго-восточная Австралия |
| ■ Центральные регион США | ■ Южная Индия |
| ■ Восточный регион США | ■ Центральная Индия |
| ■ Восточный регион США (2) | ■ Восточная Индия |
| ■ Западный регион США | ■ Центральная Канада |
| ■ Западный регион США (2) | ■ Восточная Канада |
| ■ Северо-центральный регион США | ■ Западно-центральный регион США |
| ■ Южно-центральный регион США | ■ Центральная Корея |
| ■ Северная Европа | ■ Южная Корея |
| ■ Западная Европа | ■ Западная Великобритания |
| ■ Западная Япония | ■ Южная Великобритания |
| ■ Восточная Япония | ■ Восточный Китай |
| ■ Южная Бразилия | ■ Северный Китай |

Создание и настройка контейнеров

С помощью вкладки Containers в vRealize Automation можно открывать интегрированное приложение Контейнеры для vRealize Automation, а также создавать и настраивать контейнеры и параметры сети контейнеров для предоставления к ним доступа разработчикам архитектуры схемы элементов vRealize Automation.

Контейнеры можно определить с помощью новых и существующих шаблонов и образов в интегрированном приложении Containers. После этого в схемы элементов vRealize Automation можно добавить компоненты контейнеров и соответствующие параметры сети.

Управление узлами контейнеров и кластерами

На вкладке «Кластеры» можно просматривать добавляемые узлы и выполнять с ними необходимые действия. В контексте компонента Containers узлом считается виртуальная машина или инфраструктура, с помощью которой вы работаете с контейнерами.

На странице «Кластеры», которая находится на вкладке «Инфраструктура», содержатся элементы управления, позволяющие добавлять новые кластеры и узлы. Чтобы добавить узел в среду «Контейнеры», необходимо добавить его в кластер. На любой странице на вкладках «Библиотека» и «Развертывания» можно отслеживать состояние запросов на подготовку существующих узлов и просматривать журналы событий по контейнерам. Панели «Запросы» и «Журнал событий» расположены в правой части страниц.

Создание кластера узлов контейнера

Для развертывания контейнеров необходимо добавить узел в кластер.

Необходимые условия

Выберите бизнес-группу в левом верхнем углу вкладки «Контейнеры».

Процедура

1. Войдите в консоль vRealize Automation в качестве **администратора контейнера**.
2. Откройте вкладку **Контейнеры**.

3. Нажмите в меню **Инфраструктура > Кластеры узлов контейнера**.
4. Щелкните **Кластер**.
5. Введите имя и описание кластера.
6. В раскрывающемся меню **Тип** выберите виртуальный узел контейнеров Docker (VCH).
7. Введите IP-адрес или имя узла в формате URL **http(s)://<имя_узла>:<порт>**.
8. Выберите в списке свои учетные данные для входа.

В компоненте Containers поддерживается проверка подлинности учетных данных и проверка подлинности пары открытого и закрытого ключей. На странице **Управление учетными данными** можно указать учетные данные.

9. Нажмите кнопку **Сохранить**.

Результаты

Кластер узлов контейнера успешно создан.

Использование политик развертывания контейнеров

Политики развертывания можно привязать к узлам и определениям контейнеров. В Контейнеры для vRealize Automation политики развертывания используются для установления конкретного узла и квот, которые в предпочтительном порядке применяются при развертывании контейнера.

Политики развертывания, применяемые к контейнеру, обладают более высоким приоритетом, чем размещения, которые применяются к узлам контейнера.

Примечание Политики развертывания не рекомендуются к использованию и будут удалены в последующем выпуске vRealize Automation.

Задание политики развертывания на узле

Задайте конкретный узел и квоты, которые будут в предпочтительном порядке использоваться при развертывании контейнера.

Примечание Политики развертывания не рекомендуются к использованию и будут удалены в последующем выпуске vRealize Automation.

Необходимые условия

Добавьте узел в кластер.

Процедура

1. Войдите в консоль vRealize Automation в качестве **администратора контейнера**.
2. Откройте вкладку **Контейнеры**.
3. Выберите **Инфраструктура > Кластеры узла контейнера**.
4. Щелкните кластер, содержащий узел, который вы хотите изменить.

5. Щелкните **Ресурсы**.

6. Щелкните значок параметров на узле, который вы хотите настроить, и нажмите кнопку **Изменить**.

7. Выберите политику развертывания и нажмите **Обновить**.

Задание политики развертывания для определения контейнера

Задайте политику развертывания для определения контейнера.

Примечание Политики развертывания не рекомендуются к использованию и будут удалены в последующем выпуске vRealize Automation.

Процедура

1. Откройте вкладку **Контейнеры**.
2. Нажмите кнопку **Горячие кластеры контейнера**, чтобы начать предоставление контейнера.
3. Выберите из данного списка существующий контейнер.
4. В разделе параметров предоставления щелкните **Политика**.
5. В раскрывающемся списке **Политика развертывания** выберите существующую политику.
6. Выполните предоставление контейнера или сохраните его в качестве шаблона.

Настройка параметров контейнера

Можно задать приложение с одним или несколькими контейнерами. Используйте для этого новые и существующие свойства и параметры конфигурации контейнера.

В дополнение к основным параметрам Контейнеры для vRealize Automation для развертываний, в которых используются компоненты контейнера, доступны следующие параметры vRealize Automation:

- Конфигурация работоспособности
- Ссылки
- Представляемые службы
- Размер кластера, а также параметры уменьшения и увеличения масштаба

Настройка проверок работоспособности в компоненте Containers

Можно настроить способ проверки работоспособности, чтобы обновлять состояние контейнера на основе настраиваемых критериев.

При выполнении команды в отношении контейнера можно использовать протокол HTTP или TCP. Можно также указать способ проверки работоспособности.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Убедитесь в наличии прав роли **администратор контейнера** или **архитектор контейнера**.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.
4. Измените шаблон или образ.

Параметр	Описание
Изменение шаблона	а) Щелкните Изменить в правом верхнем разделе шаблона, который нужно открыть. б) Щелкните Изменить в правом верхнем разделе контейнера, который нужно открыть.
Изменение образа.	Щелкните стрелку возле кнопки Подготовить образа и выберите Ввести дополнительные сведения .

5. Откройте вкладку **Настройка проверки работоспособности**.
6. Выберите режим работоспособности.

Таблица 2-20. Настройка проверки работоспособности: режимы

Режим	Описание
Нет	По умолчанию. Проверки работоспособности не настроены.
HTTP	Если выбран параметр HTTP , необходимо указать API-интерфейс для доступа, а также используемые метод и версию HTTP. Интерфейс API относителен, поэтому не нужно вводить адрес контейнера. Кроме того, можно задать период времени ожидания для операции и установить пороговые значения работоспособности. Например, пороговое значение работоспособности 2 означает, что для того, чтобы контейнер считался работоспособным и имел состояние ЗАПУЩЕН, должно быть два последовательных успешных вызова. Пороговое значение неработоспособности 2 означает, что для того, чтобы контейнер считался неработоспособным и имел состояние ОШИБКА, должно быть два неуспешных вызова. В случае всех условий между пороговыми значениями работоспособности и неработоспособности контейнер имеет состояние СНИЖЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ.
TCP-соединение	Если выбран параметр TCP-соединение , необходимо ввести только порт для контейнера. При проверке работоспособности будет предпринята попытка установить TCP-соединение с контейнером в указанном порту. Кроме того, можно задать значение времени ожидания для операции и установить пороговые значения работоспособности и неработоспособности, как в случае с HTTP.

Таблица 2-20. Настройка проверки работоспособности: режимы (продолжение)

Режим	Описание
Команда	Если выбран параметр Команда , необходимо ввести команду, которая будет выполняться в контейнере. Успех проверки работоспособности определяется состоянием выхода команды.
Пропускать проверку работоспособности при подготовке	Снимите этот флажок, чтобы выполнять принудительную проверку работоспособности при подготовке. Если включена эта функция, контейнер не считается подготовленным до тех пор, пока он не пройдет хотя бы одну проверку работоспособности.
Автоматическое развертывание	Автоматическое повторное развертывание контейнеров, находящихся в состоянии ОШИБКИ.

7. Нажмите кнопку **Сохранить**.

Настройка ссылок в компоненте Containers

Ссылки и доступ к службам используются для передачи данных между службами контейнеров и балансировки нагрузки между узлами. Настроить параметры ссылок для контейнеров можно в компоненте Containers

Ссылки можно использовать для передачи данных между несколькими службами в приложении. Ссылки в компоненте Containers похожи на ссылки Docker, но они связывают контейнеры на разных узлах.

Ссылка состоит из двух частей: имени службы и псевдонима. Имя службы — имя вызываемой службы или шаблона. Псевдоним — имя узла, используемое для связи с этой службой.

Например, если приложение содержит веб-службу и службу базы данных и вы задали в веб-службе ссылку на службу базы данных с использованием псевдонима **my-db**, приложение веб-службы установит TCP-соединение с `my-db:{PORT_OF_DB}`. `PORT_OF_DB` — это порт, который прослушивает база данных, независимо от того, какой общедоступный порт задан для узла в параметрах контейнера. Если программа MySQL проверяет наличие обновлений через используемый по умолчанию порт 3306, а опубликованный порт для узла контейнера — 32799, то веб-приложение связывается с базой данных с помощью `my-db:3306`.

Примечание Рекомендуется использовать сети вместо ссылок. Ссылки — это устаревшая функция Docker. При их использовании для связывания кластеров контейнеров возникают существенные ограничения, например следующие.

- Docker не поддерживает использование нескольких ссылок с одним и тем же псевдонимом. Рекомендуем разрешить Контейнеры для vRealize Automation создавать для вас псевдонимы ссылок.
- Невозможно обновлять ссылки среды выполнения контейнера. При масштабировании связанного кластера ссылки зависимого контейнера не обновляются.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.

- Убедитесь в наличии прав роли **администратор контейнера** или **архитектор контейнера**.
- Связывающиеся службы должны иметь доступ к мостовой сети.
- Должен быть опубликован внутренний порт целевой службы. Для перекрестной передачи данных службу можно привязать к любому другому порту, но при этом она должна быть доступна для объектов за пределами узла.
- Необходимо убедиться в том, что узлы службы могут связаться друг с другом.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку «Контейнеры».
3. В левой панели выберите **Библиотека > Шаблоны**.
4. Измените шаблон или образ.

Параметр	Описание
Изменение шаблона	а) Щелкните Изменить в правом верхнем разделе шаблона, который нужно открыть. б) Щелкните Изменить в правом верхнем разделе контейнера, который нужно открыть.
Изменение образа.	Щелкните стрелку возле кнопки Подготовить образа и выберите Ввести дополнительные сведения .

5. Откройте вкладку **Основное**.
6. В текстовом поле **Службы** укажите через запятую службы, от которых зависит данный контейнер.
7. В текстовом поле **Псевдоним** укажите описательное имя службы или список служб через запятую.
8. Нажмите кнопку **Сохранить**.

Настройка доступных служб в компоненте Containers

Для средства балансировки нагрузки можно использовать уникальное имя узла, указав адрес и заполнитель в настройках контейнера.

Заполнитель определяет расположение автоматически создаваемой части URL-адреса. Это значение уникально для каждого имени узла. В адресе используются символы в формате %s, с помощью которых указывается расположение заполнителя.

Примечание Если заполнитель не используется, он размещается как префикс или суффикс в имени узла, в зависимости от конфигурации системы.

Рекомендуется использовать средство балансировки нагрузки, способное нацеливать запросы на каждый узел, если в собираемом приложении есть служба, которая должна быть общедоступной и поддерживать уменьшение и увеличение масштаба. После подготовки приложения конфигурация средства балансировки нагрузки обновляется каждый раз при уменьшении или увеличении масштаба службы в vRealize Automation.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Убедитесь в наличии прав роли **администратор контейнера** или **архитектор контейнера**.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.
4. Измените шаблон или образ.

Параметр	Описание
Изменение шаблона	а) Щелкните Изменить в правом верхнем разделе шаблона, который нужно открыть. б) Щелкните Изменить в правом верхнем разделе контейнера, который нужно открыть.
Изменение образа.	Щелкните стрелку возле кнопки Подготовить образа и выберите Ввести дополнительные сведения .

5. Перейдите на вкладку **Сеть**.
6. В текстовом поле **Адрес** укажите расположение заполнителя.
 Узел, к которому относится адрес, используется как виртуальный узел. Чтобы получать доступ к узлу, к которому относится адрес, можно добавить сведения о сопоставлении в файле `etc/hosts` или использовать службу DNS, которая сопоставляет адрес контейнера с именем узла.
7. В текстовом поле **Порт контейнера** введите номер порта, через который осуществляется доступ к службе.
 Используйте в качестве примера формат, указанный в форме. Если приложение контейнера предоставляет доступ более чем к одному порту, укажите через какой именно внутренний порт (или порты) можно получать доступ к службе.
8. Нажмите кнопку **Сохранить**.

Настройка размера и масштаба кластера в компоненте Containers

Можно создавать кластеры контейнеров и с помощью настроек размещения в компоненте Containers задавать для них размеры.

При настройке кластера в компоненте Containers автоматически подготавливается указанное число контейнеров. Запросы равномерно распределяются между всеми контейнерами в кластере.

Можно изменить размер кластера так, чтобы добавить или удалить какой-либо из подготовленных контейнеров или приложений в этом кластере. При изменении размера кластера в среде выполнения учитываются все связанные фильтры и правила размещения.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Убедитесь в наличии прав роли **администратор контейнера** или **архитектор контейнера**.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.
4. Измените шаблон или образ.

Параметр	Описание
Изменение шаблона	а) Щелкните Изменить в правом верхнем разделе шаблона, который нужно открыть. б) Щелкните Изменить в правом верхнем разделе контейнера, который нужно открыть.
Изменение образа.	Щелкните стрелку возле кнопки Подготовить образа и выберите Ввести дополнительные сведения .

5. Перейдите на вкладку **Политика**.
6. Задайте размер кластера контейнеров.
7. Нажмите кнопку **Сохранить**.

Настройка и использование шаблонов и образов в компоненте Containers

В компоненте Containers используются шаблоны для подготовки контейнеров.

Шаблон — это многократно используемая конфигурация для подготовки контейнера или набора контейнеров. В шаблоне можно определить многоуровневое приложение, которое состоит из связанных служб.

Служба определяется как один или несколько контейнеров одного типа или образа.

Для настройки шаблона контейнера можно использовать существующий шаблон на странице **Шаблоны** или импортировать правильно отформатированный YAML-файл. Можно также подготовить шаблон или образ контейнера.

Создание настраиваемого шаблона контейнера

Можно создать настраиваемый шаблон и использовать его для определения контейнера.

Шаблон — это многоразовая конфигурация, которую можно использовать для подготовки контейнера или набора контейнеров.

На странице «Шаблоны» отображаются образы шаблонов, которые доступны на основе определяемых вами реестров. Можно создать настраиваемый шаблон на основе существующего образа шаблона либо импортировать шаблон или файл Docker Compose. См. раздел [Импорт шаблона контейнера или файла Docker Compose](#).

Настраиваемый шаблон или образ также можно создать, используя параметр **Подготовить > Ввести дополнительные сведения**, описанный в разделе [Подготовка контейнера на основе шаблона или образа](#).

Необходимые условия

- Убедитесь в наличии прав роли **администратор контейнера**.

Процедура

1. Войдите в консоль vRealize Automation в качестве **администратора контейнера**.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.

В списке отобразятся шаблоны и образы, которые доступны для подготовки.

- Настроенные шаблоны в представлении «Образы».
- Существующие или настраиваемые шаблоны в представлении **Шаблон**.
- Все доступные шаблоны и образы на основе указанных реестров в представлении **Все**.

Также доступны параметры **Импорт** и **Экспорт**, позволяющие импортировать и экспортировать шаблоны и образы.

4. Щелкните стрелку возле кнопки **Подготовить** образа, который необходимо включить в шаблон.
5. Щелкните **Ввод дополнительных сведений**.
6. Щелкните **Сохранить как шаблон**, чтобы сохранить свои изменения в виде нового шаблона контейнеров в Containers для vRealize Automation.

Следующие шаги

Шаблон можно изменить для подготовки в будущем. Изменения, которые вносятся в шаблон после подготовки, не влияют на существующие приложения, подготовленные из шаблона.

Импорт шаблона контейнера или файла Docker Compose

Импортированный шаблон Docker Container или YAML-файл Docker Compose можно использовать в качестве настраиваемого шаблона в Контейнеры для vRealize Automation.

В случае использования YAML-файла введите содержимое этого файла в виде текста либо перейдите к YAML-файлу и передайте его. YAML-файл представляет шаблон, конфигурацию для различных контейнеров и их связи. Поддерживаются такие типы форматов, как YAML Docker Compose и YAML Контейнеры для vRealize Automation.

Формат YAML Контейнеры для vRealize Automation аналогичен Docker Compose, однако он предполагает применение формата YAML схемы элементов vRealize Automation, отображаемого в REST API vRealize Automation или в vRealize CloudClient. Формат YAML Контейнеры для vRealize Automation позволяет импортировать существующие приложения Docker Compose, а также изменять, подготавливать их и управлять ими с помощью Containers.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Войдите в vRealize Automation в качестве **администратора контейнера**.

Дополнительные сведения о формате YAML, используемом интерфейсами REST API службы vRealize Automation, см. в разделе *Справочник по интерфейсу API vRealize Automation*.

Процедура

1. Откройте вкладку **Контейнеры**.
2. В левой панели выберите **Библиотека > Шаблоны**.

В списке отобразятся шаблоны и образы, которые доступны для подготовки.

- Настроенные шаблоны в представлении «Образы».
- Существующие или настраиваемые шаблоны в представлении **Шаблон**.
- Все доступные шаблоны и образы на основе указанных реестров в представлении **Все**.

Также доступны параметры **Импорт** и **Экспорт**, позволяющие импортировать и экспортировать шаблоны и образы.

3. Щелкните значок **Импортировать шаблон или Docker Compose**.

Откроется страница «Импорт шаблона».

4. Укажите содержимое файла YAML.

Параметр	Описание
Загрузить из файла	Щелкните Загрузить из файла , чтобы выбрать файл YAML из каталога.
Введите шаблон или Docker Compose	Вставьте содержимое правильно отформатированного файла YAML в текстовое поле Введите шаблон или Docker Compose .

5. Щелкните **Импортировать**.

Новый шаблон появится в представлении **Шаблоны**.

Подготовка контейнера на основе шаблона или образа

Контейнер можно подготовить на основе шаблона или образа в представлении «Шаблоны».

Процесс подготовки создает контейнер на основе параметров конфигурации, имеющихся в шаблоне или образе, с помощью которых выполняется подготовка.

Контейнер можно либо подготовить на основе шаблона или образа, используя существующие параметры конфигурации, либо вначале отредактировать параметры конфигурации, а затем выполнить подготовку.

Кроме того, можно отредактировать параметры конфигурации и сохранить их для создания нового пользовательского образа или шаблона контейнера.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Войдите в vRealize Automation в качестве **администратора контейнера**.

Процедура

1. Откройте вкладку **Контейнеры**.
2. В левой панели выберите **Библиотека > Шаблоны**.

В списке отобразятся шаблоны и образы, которые доступны для подготовки.

- Настроенные шаблоны в представлении «Образы».
- Существующие или настраиваемые шаблоны в представлении **Шаблон**.
- Все доступные шаблоны и образы на основе указанных реестров в представлении **Все**.

Также доступны параметры **Импорт** и **Экспорт**, позволяющие импортировать и экспортировать шаблоны и образы.

3. Просмотреть образ или шаблон для подготовки можно с помощью параметров представления **Все**, **Образы** или **Шаблоны**.
4. Подготовьте шаблон или образ.

Параметр	Описание
Подготовка с использованием существующих параметров.	<p>а) Щелкните Инициализировать.</p> <p>В представлении «Запросы на подготовку» отображаются сведения о состоянии подготовки.</p>
Подготовка с редактированием параметров.	<p>а) Щелкните стрелку возле кнопки Подготовить.</p> <p>б) Щелкните Ввод дополнительных сведений.</p> <p>в) Введите дополнительные сведения в отношении контейнера в форме Подготовить контейнер.</p> <p>г) После завершения заполнения формы щелкните Подготовить, чтобы выполнить подготовку на основе измененных параметров.</p> <p>д) Щелкните Сохранить как шаблон, чтобы сохранить свои изменения в виде нового шаблона контейнера в Контейнеры для vRealize Automation.</p> <p>В представлении «Запросы на подготовку» отображаются сведения о состоянии подготовки.</p>

Экспорт шаблона контейнера или файла Docker Compose

Шаблон контейнера можно экспортировать в виде YAML-файла Docker Compose или YAML-файла Контейнеры для vRealize Automation.

Можно импортировать шаблон, изменить его программными средствами с помощью REST API vRealize Automation или vRealize CloudClient либо графическими средствами в Containers. Измененный файл можно затем экспортировать. Например, можно выполнить импорт в формате Docker Compose, а затем экспортировать полученный файл в формате YAML схемы элементов, который используется в API службы построения vRealize Automation. Однако следует учитывать, что некоторые конфигурации, свойственные Containers, например конфигурация работоспособности и ограничения сходства, не включаются при экспорте шаблона в формате Docker Compose.

Необходимые условия

- Убедитесь, что Контейнеры для vRealize Automation включены в поддерживаемом развертывании vRealize Automation.
- Войдите в vRealize Automation в качестве **администратора контейнера**.

Дополнительные сведения о формате YAML, используемом интерфейсами REST API службы vRealize Automation, см. в разделе *Справочник по интерфейсу API vRealize Automation*.

Процедура

1. Откройте вкладку **Контейнеры**.
2. В левой панели выберите **Библиотека > Шаблоны**.
В списке отобразятся шаблоны и образы, которые доступны для подготовки.
 - Настроенные шаблоны в представлении «Образы».
 - Существующие или настраиваемые шаблоны в представлении **Шаблон**.
 - Все доступные шаблоны и образы на основе указанных реестров в представлении **Все**.
 Также доступны параметры **Импорт** и **Экспорт**, позволяющие импортировать и экспортировать шаблоны и образы.
3. Наведите указатель на шаблон и щелкните значок **Экспорт**.
4. По запросу выберите тип выходного формата:

- **Схема элементов YAML**

Этот формат соответствует формату схемы элементов YAML, который используется в API службы построения vRealize Automation.

- **Docker Compose**

Этот формат соответствует формату YAML, который используется в приложении Docker Compose.

5. Нажмите **Экспорт**.
6. По запросу сохраните файл или откройте его с помощью соответствующего приложения.

Использование реестра контейнера

Реестр Docker — это приложение на стороне сервера без отслеживания состояния. Реестры в Контейнеры для vRealize Automation можно использовать для хранения и распространения образов Docker.

Для настройки реестра необходимо указать его адрес, пользовательское имя реестра и учетные данные при необходимости. Адрес должен начинаться с HTTP или HTTPS, чтобы было видно, защищен реестр или нет. Если тип подключения не указывается, по умолчанию используется HTTPS.

Примечание Для HTTP необходимо объявить порт 80; для HTTPS необходимо объявить порт 443. Если порт не указан, ядро Docker ожидает порт 5000, что может привести к обрыву соединений.

Примечание Не рекомендуется использовать реестры с HTTP, поскольку подключение HTTP считается незащищенным. Если необходимо использовать HTTP, измените свойство DOCKER_OPTS на каждом узле следующим образом:

```
DOCKER_OPTS="--insecure-registry myregistrydomain.com:5000".
```

Дополнительные сведения см. в документации Docker по адресу <https://docs.docker.com/registry/insecure/>.

Containers может взаимодействовать с версиями 1 и 2 интерфейса API HTTP реестра Docker следующим образом.

Версия 1 через HTTP (незащищенный, простой реестр HTTP)

Можно свободно выполнять поиск по этому виду реестра, но необходимо вручную настроить каждый узел Docker с помощью флага `--insecure-registry`, чтобы подготовить контейнеры, основанные на образах из незащищенных реестров. После настройки данного свойства необходимо перезапустить управляющую программу Docker.

Версия 1 через HTTPS

Используется за обратным прокси-сервером, например NGINX. Стандартная реализация доступна через открытый код по адресу <https://github.com/docker/docker-registry>.

Версия 2 через HTTPS

Стандартная реализация выполняется через открытый код по адресу <https://github.com/docker/distribution>.

Версия 2 через HTTPS с обычной проверкой подлинности

Стандартная реализация выполняется через открытый код по адресу <https://github.com/docker/distribution>.

Версия 2 через HTTPS с проверкой подлинности через центральную службу

Можно запустить реестр Docker в автономном режиме, в котором отсутствуют проверки авторизации. Поддерживаемые реестры сторонних производителей — JFrog Artifactory и Harbor. Центр Docker

Hub включен по умолчанию для всех арендаторов и отсутствует в списке реестра, но его можно деактивировать с помощью системного свойства.

Примечание Docker обычно не взаимодействует с защищенными реестрами, настроенными с помощью сертификатов, подписанных неизвестным центром сертификации. Служба контейнеров обрабатывает такой случай, автоматически передавая недоверенные сертификаты всем узлам Docker и разрешая узлам подключаться к этим реестрам. Если сертификат не удастся загрузить на указанный узел, этот узел будет автоматически деактивирован.

Создание реестров контейнеров и управление ими

Можно настроить несколько реестров, чтобы получить доступ и к общедоступным, и к частным образам.

Реестры — это общедоступные или частные хранилища, в которые передаются и из которых загружаются образы. Созданные реестры можно деактивировать, изменять и удалять. Образы, показываемые на вкладке

Шаблоны, основаны на реестрах, которые определяет пользователь.

При создании реестров или управлении ими можно нажать кнопку **Учетные данные** либо **Сертификат**, чтобы добавить учетные данные и сертификаты или перейти к управлению ими.

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора контейнера**.
- Убедитесь, что хотя бы один узел настроен и доступен для конфигурации сети контейнера.

Процедура

1. Откройте вкладку **Контейнеры**.
2. Выберите **Библиотека > Глобальные реестры**.
3. Нажмите **Реестр**, чтобы создать новый реестр.
4. Введите адрес реестра.
5. Введите имя реестра.
6. В раскрывающемся списке выберите учетные данные для входа.
7. (дополнительно) Выберите элемент **Проверить**, чтобы подтвердить правильность заданных параметров.
8. Чтобы добавить реестр, нажмите кнопку **Сохранить**.

Добавить изображение в избранное

Для быстрого доступа к наиболее часто используемым и предпочитаемым образам их можно добавить в список избранных.

Когда образ добавляется в список избранных, он отображается на домашней странице репозитория, и его уже не нужно искать. Только администраторы контейнеров могут добавлять и удалять образы из списка избранных, а остальные пользователи могут только просматривать избранные образы в соответствующем репозитории. Рядом с именем образа, добавленного в избранное, отображается значок звездочки.

Процедура

1. На странице репозитория выберите нужный реестр из раскрывающегося меню и найдите нужный образ.
2. Щелкните стрелку рядом с полем **Подготовка** и выберите пункт **Добавить образ в Избранное**.

При этом отображается уведомление о том, что данный образ успешно добавлен в список избранных, и рядом с именем этого образа появляется значок звездочки.

Результаты

Данный образ будет отображаться на странице репозитория, и его не нужно будет специально искать.

Чтобы удалить образ из списка избранных, на странице репозитория нажмите стрелку возле поля

Подготовка и выберите команду **Удалить образ из Избранного**.

Настройка сетевых ресурсов для контейнеров

Создавать, изменять и присоединять сетевые конфигурации к контейнерам и шаблонам контейнеров можно в приложении Контейнеры для vRealize Automation.

При подготовке контейнера встроена и доступна конфигурация сети. Для компонентов контейнера, добавленных к схеме элементов vRealize Automation, можно настроить сетевые параметры.

Создание новой сети для контейнеров

Если подходящая конфигурация сети отсутствует, в vRealize Automation можно создать новую конфигурацию.

Необходимые условия

- Убедитесь в наличии прав роли **администратор контейнера, архитектор контейнера** или **администратор инфраструктуры как услуги**.
- Убедитесь, что хотя бы один узел настроен и доступен для конфигурации сети контейнера.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Развертывания > Сети**.

На основной панели отобразятся существующие конфигурации сети, которые можно подготовить в процессе развертывания контейнера. Конфигурации сети включают и конфигурации, собранные с добавленных узлов Docker, и конфигурации, созданные в vRealize Automation. На значках, представляющих конфигурации сети, отображаются сетевые драйверы и драйверы управления IP-адресами, сведения о подсети, шлюзе и диапазоне IP-адресов, количество контейнеров, использующих данную конфигурацию сети, и количество узлов.

4. Нажмите кнопку **Новая сеть**.

5. Введите имя сети.

После завершения создания новой конфигурации к значению имени будет добавлен уникальный идентификатор.

6. (дополнительно) Чтобы добавить более подробные параметры конфигурации, установите флажок **Расширенные**.

В области добавления сети появятся дополнительные параметры конфигурации сети.

7. Задайте дополнительные параметры конфигурации сети.

Параметр	Описание
Настройка управления IP-адресами	<p>Подсеть</p> <p>Укажите адреса подсети и шлюза, уникальные для этой конфигурации сети. Они не должны перекрываться с какими-либо другими сетями в том же узле контейнера.</p>
Настраиваемые свойства	<p>Для новой конфигурации сети можно также задать настраиваемые свойства (не обязательно).</p> <p>containers.ipam.driver</p> <p>Только для использования с контейнерами. Определяет, какой драйвер управления IP-адресами будет использоваться при добавлении компонента сети Containers в схему элементов. Набор поддерживаемых значений зависит от того, какие драйверы установлены в среде узла контейнера, в которой используются эти значения. Например, может использоваться поддерживаемое значение <code>infoblox</code> или <code>calico</code> в зависимости от того, какие подключаемые модули управления IP-адресами установлены на узле контейнера.</p> <p>Данные имя и значение свойства следует вводить с учетом регистра. Значение свойства не проверяется при добавлении. Если во время подготовки на узле контейнера не окажется указанного драйвера, отобразится сообщение об ошибке и подготовка будет прервана.</p> <p>containers.network.driver</p> <p>Только для использования с контейнерами. Определяет, какой сетевой драйвер будет использоваться при добавлении компонента сети Containers в схему элементов. Набор поддерживаемых значений зависит от того, какие драйверы установлены в среде узла контейнера, в которой используются эти значения. По умолчанию сетевые драйверы Docker включают <code>bridge</code>, <code>overlay</code> и <code>macvlan</code>, а сетевые драйверы Virtual Container Host (VCH) включают драйвер <code>bridge</code>. Также могут быть доступны сетевые драйверы от сторонних разработчиков, например <code>weave</code> и <code>calico</code>, в зависимости от того, какие подключаемые модули сети установлены на узле контейнера.</p> <p>Данные имя и значение свойства следует вводить с учетом регистра. Значение свойства не проверяется при добавлении. Если во время подготовки на узле контейнера не окажется указанного драйвера, отобразится сообщение об ошибке и подготовка будет прервана.</p>

Примечание При создании сети без использования расширенных параметров vRealize Automation задает параметры автоматически.

8. В раскрывающемся меню выберите узел, к которому необходимо подключить сеть.
9. Щелкните **Создать**.

Добавление сети в шаблон контейнера

В шаблон контейнера можно добавить конфигурацию сети, чтобы подключать контейнеры друг к другу. Эта конфигурация сети автоматически применяется для всех приложений, в которых используется шаблон. Можно добавить существующую сеть или настроить и добавить новую при необходимости.

Необходимые условия

- Убедитесь, что у вас есть шаблон. Если нет, сначала создайте его.
- Убедитесь в наличии прав роли **администратор контейнера**, **архитектор контейнера** или **администратор инфраструктуры как услуги**.
- Убедитесь, что хотя бы один узел настроен и доступен для конфигурации сети контейнера.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.

Появится набор значков для шаблонов и изображений, доступных для подготовки.

4. (дополнительно) Измените представление так, чтобы отображались только шаблоны. Для этого выберите элемент **Представление: шаблоны** в верхнем правом заголовке над значками.
5. Выберите элемент **Изменить** в правой верхней части шаблона, который необходимо настроить.

Появится страница «Изменить шаблон», на которой отображаются значки контейнеров и пустой значок с символом «плюс».

6. Выберите пустой значок.

Появится значок **Добавить сеть**.

7. Щелкните значок **Добавить сеть**.

Появится область добавления сети.

8. Добавьте существующую сеть или настройте и добавьте новую.

Параметр	Описание
Для добавления существующей сети выполните следующее.	а) Установите флажок Существующие . б) Щелкните в любом месте в поле Имя , чтобы появился список существующих сетей. в) Выберите сеть, которую хотите использовать, и нажмите Сохранить
Для настройки и добавления новой сети выполните следующее.	а) Введите имя сети. б) Чтобы добавить более подробные параметры конфигурации, установите флажок Расширенные . в) Нажмите кнопку Сохранить .

9. Подключите сеть к контейнеру. Для этого перетащите значок соединителя сети из контейнера в любую точку на значке в виде горизонтальной линии, представляющем сеть.

Настройка томов для контейнеров

В приложении Контейнеры для vRealize Automation можно создавать, изменять и присоединять тома к контейнерам и их шаблонам.

В Контейнеры для vRealize Automation для непрерывного управления данными используются тома Docker. Благодаря томам можно выполнять следующие задачи:

- распределять тома между разными контейнерами в пределах одного узла;
- мгновенно обновлять данные;
- сохранять данные томов после удаления контейнера.

Создание нового тома для контейнеров

Перед расширением хранилища для контейнеров необходимо создать том данных.

Необходимые условия

- Убедитесь в наличии прав роли **администратор контейнера**, **архитектор контейнера** или **администратор инфраструктуры как услуги**.
- Убедитесь, что хотя бы один узел настроен и доступен для конфигурации тома контейнера.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Развертывания > Тома**.

На основной панели отображаются существующие конфигурации томов, которые можно подключить к развернутому контейнеру. Конфигурации томов включают и конфигурации, собранные с добавленных узлов Docker, и конфигурации, созданные в vRealize Automation. В экземплярах томов отображаются драйвер, область и параметры драйвера.

4. Нажмите кнопку **Новый том**.

5. Введите имя тома.

После завершения создания конфигурации к значению имени добавляется уникальный идентификатор.

6. В текстовом поле **Драйвер** укажите необходимый драйвер подключаемого модуля тома. Если ничего не вводить, в качестве стандартного значения используется локальный драйвер.**7.** (дополнительно) Чтобы добавить более подробные параметры конфигурации, установите флажок **Расширенные**.

Появятся дополнительные параметры конфигурации.

8. (дополнительно) Настройте дополнительные параметры тома.

Параметр	Описание
Параметры драйвера	Укажите нужные параметры драйвера. Они зависят от используемого подключаемого модуля для томов.
Настраиваемые свойства	Укажите для новой конфигурации настраиваемые свойства.

9. В раскрывающемся меню выберите узел, к которому необходимо подключить том.**10.** Щелкните **Создать**.

Панель «Создать том» исчезнет, и добавленный том появится на вкладке «Том».

Следующие шаги

[Добавление тома в шаблон контейнера](#)

Добавление тома в шаблон контейнера

Можно подключить том к контейнеру, добавив его в шаблон.

Необходимые условия

- Убедитесь, что у вас есть шаблон. Если нет, сначала создайте его.
- Убедитесь в наличии прав роли **администратор контейнера**, **архитектор контейнера** или **администратор инфраструктуры как услуги**.
- Убедитесь, что хотя бы один узел настроен и доступен для конфигурации тома контейнера.

Процедура

1. Войдите в vRealize Automation.
2. Откройте вкладку **Контейнеры**.
3. В левой панели выберите **Библиотека > Шаблоны**.

Появится набор значков для шаблонов и изображений, доступных для подготовки.

4. (дополнительно) Измените представление так, чтобы отображались только шаблоны. Для этого выберите элемент **Представление: шаблоны** в верхнем правом заголовке над значками.

5. Выберите элемент **Изменить** в правой верхней части шаблона, который необходимо настроить.

Появится страница «Изменение шаблона», на которой будут показаны значки контейнеров, включая пустой значок со знаком «плюс».

6. Наведите курсор на пустой значок со знаком «плюс» так, чтобы появился значок **Добавить том**.
7. Щелкните значок **Добавить том**.
8. Добавьте существующий том или создайте и добавьте новый.

Параметр	Описание
Для добавления существующего тома выполните следующее.	а) Установите флажок Существующие . б) Щелкните в любом месте в поле Имя , чтобы появился список существующих томов. в) Выберите том, который нужно использовать, и нажмите Сохранить
Для настройки и добавления нового тома выполните следующее.	а) Введите имя тома. б) В текстовом поле Драйвер укажите необходимый драйвер подключаемого модуля тома. Если не используется внешняя система хранения, введите локальный . в) Чтобы добавить более подробные параметры конфигурации, установите флажок Расширенные . г) Нажмите кнопку Сохранить .

Область добавления тома закроется, и добавленный том появится в виде горизонтального значка под значками контейнеров на странице «Изменение шаблона». Также появится значок тома возле нижнего края области значков контейнеров.

9. Подключите том к контейнеру. Для этого перетащите значок соединителя тома из контейнера в любую точку на горизонтальном значке тома.
10. (дополнительно) Щелкните путь контейнера, чтобы изменить расположение для подключения тома.

Следующие шаги

[Подготовка контейнера на основе шаблона или образа](#)

Создание и настройка контейнеров PKS

Служба Pivotal Container Service (PKS) позволяет предприятиям и поставщикам услуг упростить развертывание служб контейнеров на основе Kubernetes и работу с ними.

Использование контейнеров PKS предлагает следующие основные возможности.

- Высокая доступность
 - PKS предоставляет для кластеров Kubernetes встроенные средства обеспечения отказоустойчивости, в том числе процедуры проверки работоспособности и автоматического исправления ошибок.

- Дополнительные сетевые возможности и средства безопасности
 - Служба PKS тесно интегрируется с NSX-T, обеспечивая расширенные функции сетей контейнеров, включая микросегментацию, балансировку нагрузки и реализацию политик безопасности.
- Оптимизированные операции
 - PKS предоставляет возможности развертывания и управления жизненным циклом для кластера Kubernetes.
- Многоарендная архитектура
 - PKS поддерживает многоарендную архитектуру, обеспечивающую изоляцию рабочих нагрузок и конфиденциальность в пределах предприятия и для облачных служб.

Добавление конечной точки PKS

Прежде чем создавать контейнер PKS, нужно добавить конечную точку PKS.

Первый шаг создания контейнера PKS — это добавление конечной точки PKS. Конечные точки PKS позволяют привязать к ним планы, существующие кластеры Kubernetes и бизнес-группы.

Необходимые условия

- Права администратора контейнера
- Учетные данные PKS
- UAA-адрес
- Адрес конечной точки PKS

Процедура

1. Перейдите к учетным данным с помощью меню **Управление удостоверениями > Учетные данные**, чтобы создать и сохранить учетные данные PKS.
2. Выберите в меню **Конечные точки PKS > Создать конечную точку**.
3. Введите сведения о конечной точке PKS и протестируйте данное подключение перед сохранением.

Если соединение не устанавливается, проверьте правильность учетных данных PKS, адреса UAA и адреса конечной точки PKS. Возможно, понадобится проверить эти адреса командой ping, чтобы убедиться, что они активны. Повторите попытку подключения.

4. Нажмите **Создать**, чтобы сохранить новую конечную точку PKS.

Примечание Если появится окно проверки сертификата, можно выбрать **Показать сертификат** и просмотреть сведения о сертификате. Нажмите кнопку **Да**, чтобы продолжить и сохранить эту конечную точку.

Результаты

Конечная точка PKS будет сохранена. После сохранения конечной точки PKS можно нажать ее и просмотреть связанные с ней доступные кластеры Kubernetes. Если какой-либо кластер не был зарегистрирован в vRealize Automation, в столбце запроса будет отображаться значение **Нет**. Чтобы зарегистрировать его, необходимо **добавить кластер**. Если нужно изменить созданную конечную точку, щелкните имя конечной точки PKS и измените ее данные. Можно удалить конечную точку, выбрав ее и нажав кнопку **Удалить**.

Назначение конечных точек PKS бизнес-группам

После создания конечной точки PKS можно предоставить доступ определенным бизнес-группам.

После создания конечной точки PKS можно открыть доступ к ней для конкретных бизнес-групп путем назначения для нее планов. Это можно использовать для ограничения доступа каких-либо групп к определенным функциям.

Примечание Планы можно создать отдельно в PKS. Планы нельзя добавлять и изменять в vRealize Automation.

Необходимые условия

- Права администратора контейнера
- Существующая конечная точка PKS

Процедура

1. Откройте нужную конечную точку PKS и нажмите **Назначение планов**.
2. Выберите нужные группы из списка групп и нужные планы — из списка планов.

Примечание С помощью кнопок «+» и «-» можно назначить несколько планов одной бизнес-группе или назначить один план нескольким бизнес-группам.

3. Нажмите кнопку **Сохранить**, чтобы сохранить назначение планов.

Запрос нового кластера PKS

Если кластера с нужной конфигурацией не существует, для существующей конечной точки PKS можно запросить новый кластер.

Разработчик или администратор контейнеров может запросить новый кластер для конечной точки PKS. Каждая конечная точка PKS может содержать несколько кластеров. После создания нового кластера можно добавить его в свою среду с помощью меню **Добавить кластер** и подготовить его нужным образом.

Необходимые условия

- Существующая конечная точка PKS
- Требуется права разработчика контейнеров или администратора контейнеров

Процедура

1. Выберите **Кластеры PKS > Создать кластер**.

2. Выберите нужную конечную точку PKS.

После выбора конечной точки PKS соответствующий план заполняется автоматически согласно планам, доступным для вашей бизнес-группы.

3. Введите сведения о кластере.

Примечание Хотя количество рабочих узлов определяется данным планом, можно изменить это число в соответствии с конкретными потребностями.

4. Выберите нужный способ подключения к этому кластеру.

- Имя ведущего узла — подключение с использованием имени узла данного кластера при условии, что существует соответствующая DNS-запись.
- IP-адрес ведущего узла — подключение с использованием IP-адреса данного кластера.

5. Щелкните **Создать**.

Результаты

Новый кластер будет создан и появится на домашней странице кластеров PKS.

Добавление кластера PKS

После создания конечной точки PKS можно зарегистрировать в vRealize Automation доступные связанные кластеры.

После создания конечной точки PKS можно зарегистрировать связанные кластеры путем добавления в vRealize Automation одного из кластеров. После регистрации кластеров для них можно подготовить один образ.

Необходимые условия

- Права администратора контейнера
- Конечная точка PSK с доступными кластерами

Процедура

1. Убедитесь, что вы добавляете кластер в правильную бизнес-группу. Имя бизнес-группы указывается в верхней левой панели. Для переключения бизнес-группы нажмите **Группа**.

2. Нажмите **Кластер PKS > Добавить кластер**.

3. Выберите конечную точку PKS, чтобы заполнить поля доступных кластеров.

4. Выберите нужный способ подключения к этому кластеру.

- Имя ведущего узла — подключение с использованием имени узла данного кластера при условии, что существует соответствующая DNS-запись.
- IP-адрес ведущего узла — подключение с использованием IP-адреса данного кластера.

5. Нажмите кнопку **Добавить**.

Результаты

Данный кластер появится на странице кластеров PKS.

Сведения о кластере PKS

В сведениях о кластере содержится информация, а также указаны инструменты для внесения изменений и взаимодействия с кластером.

Можно просмотреть и изменить существующие кластеры PKS, щелкнув имя кластера на странице **Кластеры PKS**. Кроме того, в сведениях о кластере указаны интерактивные инструменты, которые можно использовать для взаимодействия с кластером в более сложных конфигурациях.

Примечание Можно изменить только количество рабочих узлов кластера.

Панель мониторинга

В состоянии поля панели мониторинга указывается, что панель Kubernetes установлена. Если эта панель мониторинга установлена, к ней можно получить доступ, нажав **Установлено** и войдя в систему.

Примечание Для панели управления в кластере должна быть настроена обычная проверка подлинности. Без базовой проверки подлинности невозможно войти в систему.

KubeConfig

Ссылка kubeconfig представляет собой загружаемый файл конфигурации для кластера. Разработчик контейнеров может использовать этот файл конфигурации для подключения и настройки кластера Kubernetes в окне командной строки. Например, можно применить команду **kubect1**.

Подготовка отдельных образов в кластере Kubernetes

Функциональность контейнеров в vRealize Automation позволяет подготовить один образ в кластере PKS.

После добавления кластера PKS можно подготовить на нем отдельный образ как сочетание модуля Kubernetes и развертывания.

Необходимые условия

- Привилегии разработчика контейнера
- Кластер PKS

Процедура

1. Перейдите в меню: **Библиотека > Репозитории**.
2. В раскрывающемся меню выберите нужный реестр.
3. Найдите в этом реестре существующий образ, используя текстовое поле «Репозитории».
4. Нажмите **Подготовить** на плитке нужного образа.

5. Введите параметры подготовки и нажмите **Подготовить**.

Результаты

Выбранный образ будет подготовлен в кластере Kubernetes и отобразится на боковой панели **Запросы**. Для подтверждения он также отобразится в разделе **Kubernetes > Развертывания** и **Kubernetes > Модули**.

Примечание Можно также подготовить кластер, загрузив файл kubeconfig и выполнив команду **kubect1**. Дополнительные сведения см. в разделе [Сведения о кластере PKS](#).

Установка дополнительных подключаемых модулей на заданный по умолчанию сервер vRealize Orchestrator

На заданный по умолчанию сервер vRealize Orchestrator можно установить дополнительные пакеты и подключаемые модули с помощью интерфейса настройки конфигурации vRealize Orchestrator.

На заданный по умолчанию сервер vRealize Orchestrator можно установить дополнительные подключаемые модули и использовать рабочие процессы с помощью Все как услуга.

Кроме того, можно импортировать дополнительные пакеты на сервер vRealize Orchestrator по умолчанию для настройки в качестве типов конечных точек внешних поставщиков IP-адресов vRealize Automation. Например, сведения о получении, импорте и настройке пакета системы управления IP-адресами Infoblox см. в разделе [Контрольный список для обеспечения поддержки стороннего поставщика управления IP-адресами](#).

Пакетные файлы (.package) и установочные файлы подключаемых модулей (.vmoapp или .dar) доступны в VMware Solution Exchange по адресу https://solutionexchange.vmware.com/store/category_groups/cloud-management. Для получения информации о файлах подключаемого модуля см. раздел vRealize Orchestrator Документация по подключаемым модулям по адресу https://www.vmware.com/support/pubs/vco_plugins_pubs.html.

Дополнительные сведения об установке новых подключаемых модулей см. в разделе *Установка и настройка VMware vCenter Orchestrator*.

Работа с политиками Active Directory

Политики Active Directory определяют свойства записи компьютера, например домена, а также организационной единицы, в которой эта запись создана с помощью схемы элементов vRealize Automation.

При применении политики к бизнес-группе все запросы компьютера от членов бизнес-группы добавляются к определенной организационной единице. Можно создать разные политики для разных организационных единиц, а затем применять их к разным бизнес-группам.

Использование настраиваемых свойств для переопределения политики Active Directory

С помощью предоставленных настраиваемых свойств Active Directory можно переопределять политику Active Directory, домен, организационную единицу и другие значения в конкретной схеме элементов при ее развертывании.

Список предоставленных настраиваемых свойств Active Directory включен в раздел *Справочник по настраиваемым свойствам*. Префикс настраиваемого свойства — `ext.policy.activedirectory`.

В дополнение к предоставленным свойствам можно создавать собственные настраиваемые свойства. К собственному настраиваемому свойству необходимо добавить префикс `ext.policy.activedirectory`. Например, `ext.policy.activedirectory.domain.extension` или `ext.policy.activedirectory.yourproperty`. Данные свойства передаются настраиваемым рабочим процессам Active Directory vRealize Orchestrator.

Дополнительные сведения о настраиваемых свойствах см. в разделе *Справочник по настраиваемым свойствам*. В зависимости от переопределяемых значений, возможно, понадобится создать определение свойства. Например, можно создать определение свойства, которое получает доступные политики Active Directory из vRealize Automation. Кроме того, можно создать определение, которое позволяет запрашивающему пользователю выбирать из нескольких альтернативных организационных единиц. См. раздел *Справочник по настраиваемым свойствам*.

Создание и применение политик Active Directory

Следует создать одну или несколько политик Active Directory, чтобы можно было назначать разные политики разным бизнес-группам. Разные политики можно использовать для добавления записей компьютера в разные организационные единицы в зависимости от членства в бизнес-группе.

При необходимости назначенную политику Active Directory можно переопределить.

Процедура

1. Создание политики Active Directory

Создайте политику Active Directory, чтобы определить расположение для добавления записей в экземпляре Active Directory при развертывании компьютеров пользователями. Можно назначить политику для бизнес-группы, чтобы для всех компьютеров, развернутых ее членами, создавалась запись в определенной организационной единице.

2. Сценарий: добавление настраиваемого свойства в схемы элементов для переопределения политики Active Directory

У разработчика архитектуры схемы элементов для бизнес-группы разработки имеется схема элементов, которая включает в себя компьютер приложения и компьютер базы данных. Необходимо добавить запись компьютера базы данных в организационную единицу, которая отличается от применяемой политики Active Directory.

Создание политики Active Directory

Создайте политику Active Directory, чтобы определить расположение для добавления записей в экземпляре Active Directory при развертывании компьютеров пользователями. Можно назначить

политику для бизнес-группы, чтобы для всех компьютеров, развернутых ее членами, создавалась запись в определенной организационной единице.

Создайте разные политики Active Directory, если необходимо, чтобы компьютеры, развернутые различными бизнес-группами, имели различные домены или были добавлены в различные экземпляры Active Directory.

Необходимые условия

- Убедитесь, что создали конечную точку Active Directory. См. раздел [Настройка подключаемого модуля Active Directory в качестве конечной точки](#).
- Если используется внешний сервер vRealize Orchestrator, убедитесь, что он настроен правильно. См. раздел [Настройка внешнего сервера vRealize Orchestrator](#).
- Войдите в vRealize Automation в качестве администратора арендатора.

Процедура

1. Выберите **Администрирование > Политики Active Directory**.
2. Выберите значок **Создать (+)**.
3. Настройте сведения о политике Active Directory.

Параметр	Описание
Идентификатор	Введите постоянное значение. Это значение не может содержать пробелы или специальные символы. Невозможно будет изменить это значение позднее. Можно будет только повторно создать эту политику с другим идентификатором.
Описание	Опишите политику.
Конечная точка Active Directory	Выберите конечную точку Active Directory, для которой создается эта политика.
Домен	Введите корневой домен. Требуемый формат: <i>mycompany.com</i> .
Организационная единица	Введите различающееся имя организационной единицы для данной политики. Иерархия должна быть введена в виде списка, разделенного запятыми. Например, <i>ou=development,dc=corp,dc=domain,dc=com</i> .

4. Нажмите кнопку **ОК**.

Результаты

Конечная точка Active Directory vRealize Orchestrator добавлена к списку. Можно применять данную политику в бизнес-группах или использовать ее в схемах элементов или бизнес-группах.

Следующие шаги

- Чтобы предоставить несколько вариантов политики, создайте дополнительные политики.

- Чтобы добавить записи в Active Directory на основании членства в бизнес-группе при развертывании схемы элементов, добавьте соответствующую политику Active Directory к бизнес-группе. См. раздел [Создание бизнес-группы](#). Можно применить данную политику при создании бизнес-группы или можно добавить ее позже.
- Чтобы переопределить политику Active Directory для бизнес-группы для конкретной схемы элементов, добавьте настраиваемые свойства Active Directory в данную схему элементов. См. раздел [Сценарий: добавление настраиваемого свойства в схемы элементов для переопределения политики Active Directory](#).

Сценарий: добавление настраиваемого свойства в схемы элементов для переопределения политики Active Directory

У разработчика архитектуры схемы элементов для бизнес-группы разработки имеется схема элементов, которая включает в себя компьютер приложения и компьютер базы данных. Необходимо добавить запись компьютера базы данных в организационную единицу, которая отличается от применяемой политики Active Directory.

Есть существующая политика, которая применяется к бизнес-группе разработки. Данная политика добавляет записи компьютера в `ou=development,dc=corp,dc=domain,dc=com`. Необходимо добавить все компьютеры баз данных в `ou=databases,dc=corp,dc=domain,dc=com`. В схеме элементов, которая включает в себя сервер базы данных, переопределите организационную единицу Active Directory, чтобы добавить запись компьютера базы данных в `ou=databases,dc=corp,dc=domain,dc=com`.

В данном сценарии сделаны следующие предположения.

- Active Directory включает в себя организационные единицы разработки и баз данных.
- Имеется тестовая схема элементов, включенная в службу. Эта служба наделена правами.

Кроме этого простого примера переопределения политики, можно использовать настраиваемые свойства с политикой Active Directory, чтобы внести другие изменения в Active Directory при развертывании схем элементов. См. раздел [Работа с политиками Active Directory](#).

Необходимые условия

- Убедитесь, что есть как минимум одна политика Active Directory. См. раздел [Создание политики Active Directory](#). Например, необходимо создать политику разработки, которая добавляет записи в `ou=development,dc=corp,dc=domain,dc=com`.
- Убедитесь, что есть бизнес-группа, к которой применена политика Active Directory. См. раздел [Создание бизнес-группы](#). Например, бизнес-группа разработки использует политику разработки.

Процедура

1. В тестовой схеме элементов выберите компьютер базы данных на холсте.
2. Перейдите на вкладку **Свойства**.
3. Перейдите на вкладку **Настраиваемые свойства**.
4. Выберите значок **Создать** (+).

5. Добавьте настраиваемое свойство, чтобы изменить организационную единицу по умолчанию.

- а) В текстовом поле **Имя** введите **ext.policy.activedirectory.orgunit**.
- б) В текстовом поле **Значение** введите **ou=databases,dc=corp,dc=domain,dc=com**.
- в) Снимите флажок **Допускает переопределение**.
- г) Нажмите кнопку **ОК**.

6. Щелкните элемент **Готово**.

Результаты

Тестовая схема элементов включает в себя настраиваемое свойство, но пользователи не увидят его в форме запроса.

Следующие шаги

Запросите тестовую схему элементов. Убедитесь, что запись для компьютера базы данных была добавлена к организационной единице базы данных и что запись для компьютера приложения добавлена к организационной единице разработки. Когда будут получены удовлетворительные результаты, можете добавить настраиваемое свойство к своим производственным схемам элементов.

Параметры пользователя для уведомлений и делегатов

Используйте параметры пользователя, чтобы переопределить конфигурации по умолчанию для уведомлений утверждающего системы и языковые настройки уведомлений.

Для доступа к пользовательским параметрам нажмите свое имя пользователя в заголовке vRealize Automation и выберите **Параметры**.

Следующие параметры индивидуальны для вас как для пользователя, вошедшего в систему.

Таблица 2-21. Параметры пользователя

Параметр	Описание
Назначение делегатов	Позволяет переназначить запросы на утверждение другим пользователям. Например, вы являетесь утверждающим по запросам каталога, но собираетесь в отпуск. Можно делегировать все уведомления на утверждение одному или нескольким утверждающим. При этом назначении запросы будут сразу перенаправляться делегату. Делегаты будут активными, пока вы не удалите их из списка.
Уведомления	Позволяют изменить язык уведомления, чтобы сообщения электронной почты отправлялись на выбранном языке, а не языке по умолчанию. Выберите язык и добавьте подписку на уведомления, которая поддерживает нужные языковые настройки.

Предоставление пользователям схем элементов служб

3

Чтобы предоставить пользователям услуги по требованию, нужно создать элементы и действия каталога, а затем назначить права и использовать подтверждения, чтобы тщательно контролировать возможность запроса таких услуг.

В эту главу входят следующие разделы:

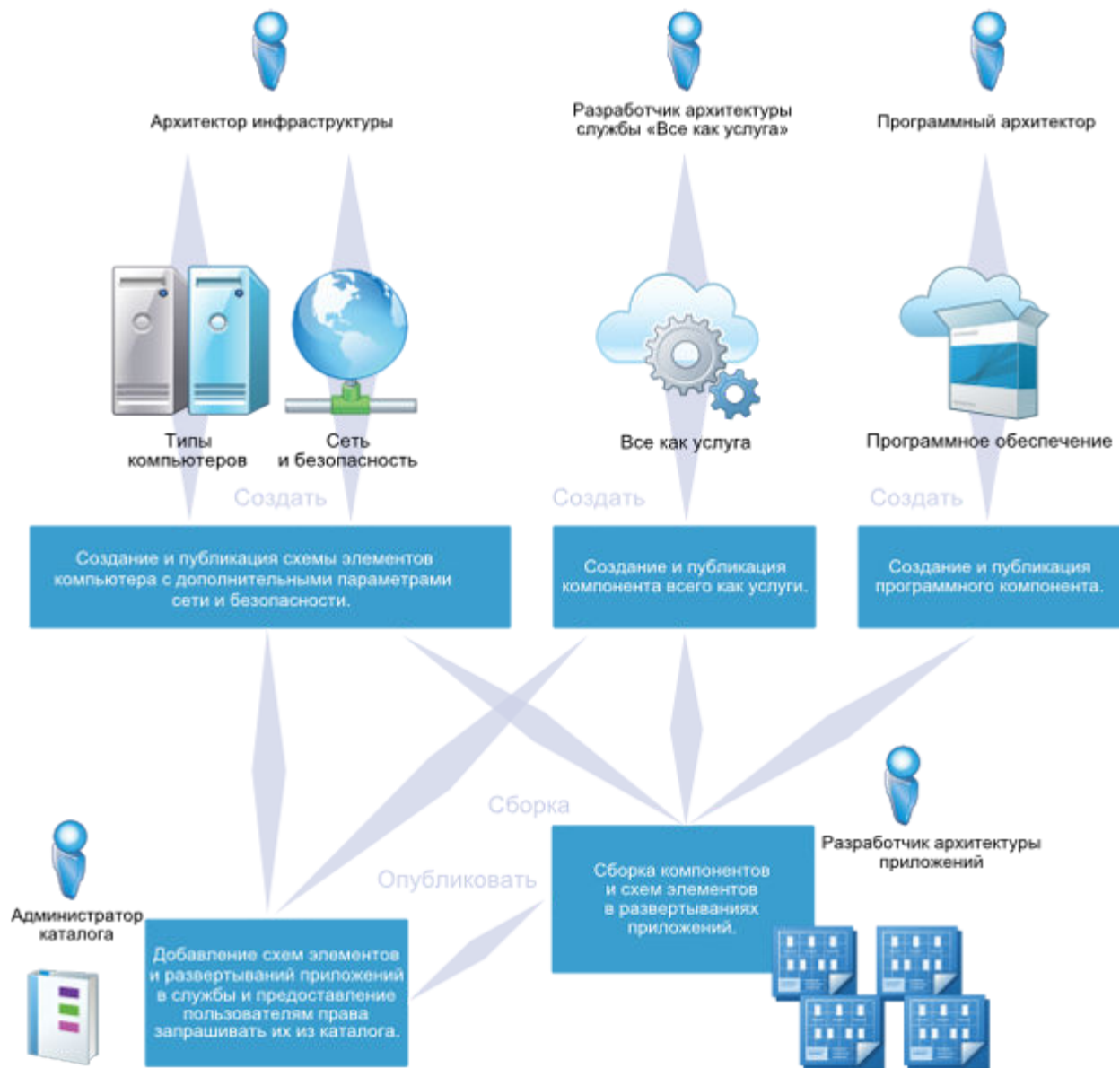
- [Проектирование схем элементов](#)
- [Создание библиотеки проектов](#)
- [Работа со схемами элементов, создаваемыми разработчиками](#)
- [Сборка составных схем элементов](#)
- [Настройка форм запроса схем элементов](#)
- [Тестирование и устранение неполадок неудачных запросов на подготовку](#)
- [Управление каталогом служб](#)

Проектирование схем элементов

Разработчики схем элементов создают компоненты Программное обеспечение, схемы элементов компьютера и настраиваемые схемы элементов Все как услуга, а также собирают такие компоненты в схемы элементов, которые пользователи могут запрашивать из каталога. В каталоге может отображаться форма запроса по умолчанию, либо можно создать настраиваемую форму для каждой публикуемой схемы элементов.

Схемы элементов можно создавать и публиковать для одного компьютера или одной настраиваемой схемы элементов Все как услуга, но также можно объединять компоненты компьютера и схемы элементов Все как услуга с другими структурными блоками для разработки сложных схем элементов каталога, которые включают в себя различные компьютеры, сетевые устройства, компоненты системы безопасности, программное обеспечение с полной поддержкой жизненного цикла, а также настраиваемые функции Все как услуга.

В зависимости от элемента каталога, который необходимо определить, процесс может быть простым, как в случае, когда один разработчик архитектуры инфраструктуры публикует один компонент компьютера в качестве схемы элементов. Либо этот процесс может быть более сложным, как в случае, когда несколько разработчиков архитектуры разрабатывают различные типы компонентов с целью создания полного стека приложений, которые могут запрашиваться пользователями.



Компоненты Программное обеспечение

Вы можете создавать и публиковать программные компоненты для установки программного обеспечения в процессе подготовки компьютеров, а также для поддержки жизненного цикла ПО. Например, для разработчиков можно создать схему элементов для запроса компьютера с уже установленной и настроенной средой разработки. Программные компоненты сами по себе не являются элементами каталога. Для создания схемы элементов каталога их необходимо объединить с соответствующим компонентом компьютера. См. раздел [Проектирование компонентов Программное обеспечение](#).

Схемы элементов компьютеров

Можно создавать и публиковать простые схемы элементов для подготовки отдельных компьютеров либо более сложные, содержащие дополнительные компоненты компьютеров и любую комбинацию следующих типов компонентов на выбор:

- Компоненты Программное обеспечение
- Существующие схемы элементов
- Компоненты сети и безопасности NSX
- Компоненты Все как услуга
- Компоненты Containers
- Настраиваемые и прочие компоненты

См. раздел [Проектирование схем элементов компьютера](#).

Схемы элементов Все как услуга

Рабочие процессы vRealize Orchestrator можно публиковать как схемы элементов Все как услуга. Например, можно создать настраиваемый ресурс для пользователей Active Directory и разработать схему элементов Все как услуга, чтобы менеджеры могли подготавливать новых пользователей в своей группе Active Directory. Создание компонентов Все как услуга и управление ими осуществляются за пределами вкладки «Проектирование». Для создания схем элементов приложения опубликованные схемы элементов Все как услуга можно использовать повторно, но только в сочетании хотя бы с одним компонентом компьютера. См. раздел [Проектирование схем элементов и действий ресурсов Все как услуга](#).

Схемы элементов приложения с несколькими компьютерами, компонентами Все как услуга и Программное обеспечение

В схему элементов компьютера можно добавлять любое количество компонентов компьютера, компонентов Программное обеспечение и схем элементов Все как услуга, чтобы предоставлять пользователям расширенные функциональные возможности.

Например, можно создать схему элементов для менеджеров, которая обеспечивает подготовку новых вакансий. Для подготовки новых пользователей Active Directory можно объединить несколько компонентов компьютера, программных компонентов и схему элементов Все как услуга. Менеджер службы контроля качества может запросить элемент каталога «Новая вакансия». В Active Directory подготовлен новый пользователь — сотрудник службы контроля качества, которому выделены две рабочие виртуальные машины (одна Windows и одна Linux), каждая из которых имеет все требуемое программное обеспечение для выполнения сценариев тестирования в этих средах.

Создание библиотеки проектов

Можно создать библиотеку повторно используемых компонентов схемы элементов, которые архитекторы могут собрать в схеме элементов приложения для предоставления пользователям более сложных служб по требованию.

Создавайте библиотеку из мельчайших проектных компонентов схемы элементов — единичных схем элементов компьютеров, компонентов Программное обеспечение и схем элементов Все как услуга, а затем объединяйте эти базовые структурные элементы в новых различных вариациях для создания более сложных элементов каталога, которые обеспечивают расширение функциональных возможностей системы для пользователей.

Образцы схем элементов доступны на портале VMware Solution Exchange по адресу <https://solutionexchange.vmware.com> и на сайте <https://code.vmware.com>.

Таблица 3-1. Создание библиотеки проектов

Элемент каталога	Роль	Компоненты	Описание	Сведения
Компьютеры	Архитектор инфраструктуры	Создайте схему элементов компьютера на вкладке Схемы элементов .	<p>Создав схемы элементов компьютеров, можно обеспечить быструю доставку пользователям виртуальных машин, а также частных, общедоступных или гибридных облачных компьютеров.</p> <p>Администраторы каталогов могут включить опубликованные схемы элементов компьютеров в каталог в качестве отдельных схем, однако схемы элементов компьютеров можно также объединять с другими компонентами, чтобы создать более сложные элементы каталога, включающие в себя несколько схем элементов компьютеров, Программное обеспечение или схемы элементов Все как услуга.</p>	Настройка схемы элементов компьютера
Сеть и безопасность NSX на компьютерах	Архитектор инфраструктуры	Добавьте компоненты сети и безопасности NSX в схемы элементов компьютеров vSphere на вкладке Схемы элементов .	<p>Чтобы виртуальные машины могли безопасно и эффективно обмениваться данными по физическим и виртуальным сетям, нужно настроить компоненты сети и безопасности, такие как профили сети и группы безопасности.</p> <p>Чтобы администраторы каталога могли включить компоненты сети и безопасности в каталог, нужно объединить их по меньшей мере с одним компонентом компьютера vSphere. Компоненты сети и безопасности NSX можно применять только к схемам элементов компьютеров vSphere.</p>	Проектирование схем элементов с использованием параметров NSX
Программное обеспечение на компьютерах	Программный архитектор Чтобы добавить компоненты программного обеспечения на холст проекта, требуются также права участника бизнес-группы, администратора бизнес-группы или администратора арендатора для доступа к целевому каталогу.	Создайте и опубликуйте компоненты Программное обеспечение на вкладке Программное обеспечение , а затем объедините их со схемами элементов компьютеров на вкладке Схемы элементов .	<p>Добавьте компоненты Программное обеспечение в схемы элементов компьютера, чтобы стандартизировать, развернуть, настроить, обновить и масштабировать сложные приложения в облачных средах. Это могут быть самые разные приложения — от простых веб-приложений до сложных специальных приложений и пакетных приложений.</p> <p>Компоненты Программное обеспечение не могут отображаться только в каталоге. Сначала нужно создать и опубликовать компоненты Программное обеспечение, а затем собрать схему элементов приложения, содержащую по меньшей мере один компьютер.</p>	Создание компонента Программное обеспечение

Таблица 3-1. Создание библиотеки проектов (продолжение)

Элемент каталога	Роль	Компоненты	Описание	Сведения
Специализированные ИТ-услуги	Архитекторы службы «Все как услуга»	Создайте и опубликуйте схемы элементов Все как услуга на вкладке Все как услуга .	Можно создать элементы каталога Все как услуга, расширяющие стандартную функциональность vRealize Automation, связанную с подготовкой компьютеров, сетей, систем безопасности и программного обеспечения. Чтобы автоматизировать предоставление любых ИТ-услуг, можно воспользоваться имеющимися рабочими процессами и подключаемыми модулями vRealize Orchestrator или настраиваемыми сценариями, разработанными в vRealize Orchestrator. Администраторы каталогов могут включить опубликованные схемы элементов Все как услуга в каталог в качестве отдельных схем, однако они могут также объединять их с другими компонентами на вкладке Схемы элементов , чтобы создать более сложные элементы каталога.	Проектирование схем элементов и действий ресурсов Все как услуга
Сборка опубликованных структурных блоков схем элементов в новые элементы каталога	<ul style="list-style-type: none"> ■ Разработчик архитектуры приложений ■ Архитектор инфраструктуры ■ Программный архитектор 	На вкладке Схемы элементов объедините дополнительные схемы элементов компьютера, схемы элементов Все как услуга и компоненты Программное обеспечение по крайней мере с одним компонентом компьютера или одной схемой элементов компьютера.	Повторно используя опубликованные компоненты и схемы элементов и по-новому объединяя их, можно создать пакеты ИТ-услуг, предоставляющие пользователям более специализированные функциональные возможности.	Сборка составных схем элементов

Проектирование схем элементов компьютера

Схемы элементов компьютера являются его полными спецификациями: они определяют атрибуты компьютера, способ его подготовки и его настройки политики и управления. В зависимости от сложности создаваемых элементов каталога можно совмещать компоненты компьютера в схеме элементов с другими компонентами в проекте холста, чтобы создавать более сложные элементы каталога, включающие в себя элементы сети и безопасности, компоненты Программное обеспечение, компоненты Все как услуга и другие компоненты схемы элементов.

Компактное хранилище для виртуальной подготовки

Технология компактного хранилища позволяет устранить неэффективность традиционных методов хранения за счет использования той емкости хранения, которая фактически необходима для выполнения операций компьютера. Как правило, это только часть емкости хранения, фактически выделенной для компьютеров. В vRealize Automation поддерживаются два способа подготовки с использованием технологии, способствующей экономии места, — тонкая подготовка и подготовка с помощью FlexClone.

При использовании стандартного хранилища его емкость, выделенная подготовленному компьютеру, назначена ему полностью, даже если он выключен. Такое использование ресурсов хранения может быть чрезвычайно неэкономным, поскольку только некоторые виртуальные машины фактически используют всю выделенную им емкость хранилища и лишь некоторые физические компьютеры работают с диском, заполненным на 100%. При использовании технологии компактного хранилища выделенная емкость хранилища и используемая емкость хранилища отслеживаются отдельно, и подготовленному компьютеру полностью назначается только используемая емкость хранилища.

Thin Provisioning

Все методы виртуальной подготовки поддерживают тонкую подготовку. Тонкую подготовку всегда можно использовать при подготовке компьютера. При этом учитывается платформа виртуализации, тип хранилища и конфигурация хранилища по умолчанию. Например, тонкая подготовка всегда применяется для интеграций сервера vSphere ESX, использующих хранилище сетевой файловой системы. Однако для интеграций сервера vSphere ESX, использующих локальное хранилище или хранилище iSCSI, тонкая подготовка применяется для подготовки компьютеров, только если в схеме элементов указано настраиваемое свойство `VirtualMachine.Admin.ThinProvision`. Дополнительные сведения о тонкой подготовке см. в документации, предоставляемой платформой виртуализации.

Подготовка Net App FlexClone

При работе в среде vSphere, в которой используются хранилище с сетевой файловой системой (Network File System, NFS) и технология FlexClone, можно создать схему элементов для подготовки, осуществляемой с помощью Net App FlexClone.

Можно использовать только хранилище с сетевой файловой системой. В противном случае подготовка компьютера завершится ошибкой. Путь к хранилищу FlexClone можно указать для других типов подготовки компьютеров, но этот путь будет использоваться так же, как и в случае стандартного хранилища.

Ниже приведен общий обзор последовательности действий, необходимых для подготовки компьютеров, на которых используется технология FlexClone:

1. Администратор инфраструктуры как услуги создает конечную точку NetApp ONTAP. См. раздел [Справочник по параметрам конечных точек](#).
2. Администратор инфраструктуры как услуги выполняет сбор данных в конечной точке, чтобы конечная точка стала видимой в вычислительном ресурсе и на страницах резервирования.

Параметр FlexClone отображается в столбце конечной точки на странице резервирования, если конечная точка NetApp ONTAP существует и используется виртуальный узел. Если конечная точка NetApp ONTAP существует, на странице резервирования отображается конечная точка, назначенная пути к хранилищу.

3. Администратор структуры создает резервирование vSphere, включает хранилище FlexClone и указывает путь к хранилищу с сетевой файловой системой, в котором используется технология FlexClone. См. раздел [Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer](#).
4. Архитектор инфраструктуры или другой авторизованный пользователь создает схему элементов для подготовки, осуществляемой с помощью FlexClone.

Общие сведения о параметризации схем элементов и ее использование

Профили компонентов можно использовать для параметризации схем элементов. Вместо создания отдельных схем элементов небольшого, среднего и крупного размера для конкретного типа развертывания можно создать одну схему с возможностью выбора виртуальной машины нужного размера. Пользователи могут выбрать один из этих размеров при развертывании элемента каталога.

Профили компонентов предотвращают рост количества схем элементов и упрощают предложения каталога. С помощью профилей компонентов можно определить компоненты компьютеров vSphere в схеме элементов. Доступные типы профилей компонентов — Size и Image. Параметры профилей компонентов, добавленных в компонент компьютера, переопределяют другие параметры компонента компьютера, такие как число ЦП и емкость хранилища.

Профили компонентов доступны только для компонентов компьютеров vSphere.

Сведения об определении наборов значений для профилей компонентов Size и Image см. в разделе в *Справочник по настраиваемым свойствам*.

Сведения о добавлении профилей компонентов и выбранных наборов значений для компонента компьютера vSphere в схеме элементов см. в разделе [Настройки компонентов компьютера vSphere в vRealize Automation](#).

Информацию о добавлении сведений о профиле компонента с помощью параметров, импортированных из файла OVF, см. в разделе [Настройка схемы элементов для подготовки из файла OVF](#).

Сведения об использовании профилей компонентов при запросе на подготовку компьютера см. в разделе [Запрос подготовки компьютера с помощью параметризованной схемы элементов](#).

Можно создать политики подтверждения, чтобы требовать предварительное подтверждение при запросе на подготовку компьютера для схем элементов в сопоставлении с условиями набора значений для профилей компонентов Size и Image. Дополнительные сведения см. в разделе [Примеры политик подтверждения, основанных на типе политики виртуальной машины](#).

Примечание

Сведения об использовании параметризации схем элементов при запросе на подготовку компьютеров из каталога см. в разделе [Запрос подготовки компьютера с помощью параметризованной схемы элементов](#).

Настройка схемы элементов компьютера

Настройте и опубликуйте компонент компьютера как автономную схему элементов, которую другие разработчики архитектуры могут использовать в качестве компонента в схемах элементов приложений, а администраторы каталога смогут включать в службы каталога.

Эта процедура кратко описывает процесс создания схемы элементов. Дополнительные сведения см. здесь:

- [Проектирование схем элементов с использованием параметров NSX](#)
- [Общие сведения о параметризации схем элементов и ее использование](#)
- [Настройки свойств схемы элементов](#)
- [Настройка схемы элементов для подготовки из файла OVF](#)
- [Экспорт и импорт схем элементов и содержимого](#)
- [Создание схем элементов Microsoft Azure и включение действий ресурсов](#)
- [Добавление возможности управления конфигурацией в схемы элементов vSphere](#)

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Завершите внешние приготовления для подготовки, в том числе создание шаблонов, WinPE и ISO, или получите сведения о внешних приготовлениях у администраторов.
- Настройте арендатор. См. раздел [Настройка параметров арендатора](#).
- Настройте ресурсы инфраструктуры как услуги. См. раздел [Контрольный список для настройки ресурсов инфраструктуры как услуги](#).
- См. раздел *Настройка vRealize Automation*.

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Выберите значок **Создать** (+).
3. Чтобы настроить общие параметры, работайте с запросами в диалоговом окне **Новая схема элементов**.
4. Нажмите кнопку **ОК**.
5. Щелкните **Типы компьютеров** в области «Категории», чтобы отобразить список доступных типов компьютеров.
6. Перетащите тип компьютера, который нужно подготовить, на холст проекта.
7. Введите информацию на каждой из вкладок, чтобы настроить данные о подготовке компьютера, как описано в [Настройки свойств схемы элементов](#).
8. Щелкните элемент **Готово**.
9. Выберите схему элементов и нажмите кнопку **Опубликовать**.

Результаты

Вы настроили и опубликовали компонент компьютера в качестве автономной схемы элементов. Администраторы каталогов могут добавить эту схему элементов компьютера в службы каталога и дать пользователям возможность запрашивать эту схему элементов. Другие разработчики архитектуры могут с помощью этой схемы элементов компьютера создавать более сложные схемы элементов приложения, которые включают в себя компоненты Программное обеспечение, схемы элементов Все как услуга или дополнительные схемы элементов компьютера.

Следующие шаги

Схему элементов компьютера можно объединить с компонентами Программное обеспечение, схемами элементов Все как услуга или дополнительными схемами элементов компьютеров, чтобы создать более сложные схемы элементов приложения. См. [Сборка составных схем элементов](#) и [Общие сведения о поведении вложенных схем элементов](#).

Параметры схемы элементов компьютера

Параметры конфигурации и настраиваемые свойства можно определить для всей схемы элементов.

Настройки свойств схемы элементов

Во время создания схемы элементов можно настроить параметры, которые будут применяться ко всей схеме элементов, на странице **Свойства схемы элементов**. После создания схемы элементов эти настройки можно изменить на странице «Свойства схемы элементов».

Вкладка **Общие**

Параметры на вкладке «Общие» применяются к общей схеме элементов vRealize Automation.

Таблица 3-2. Настройки вкладки **Общие**

Параметр	Описание
Имя	Введите имя своей схемы элементов.
Идентификатор	Поле идентификатора заполняется автоматически на основе введенного имени. Сейчас это поле можно изменить, но после сохранения схемы элементов изменить его будет невозможно. Идентификаторы в пределах арендатора являются постоянными и уникальными. Идентификаторы можно использовать для программного взаимодействия со схемами элементов и создания привязок свойств.
Описание	Составьте сводку по схеме элементов, чтобы ею было удобно пользоваться другим разработчикам архитектуры. Это описание также отображается для пользователей в форме запроса.
Ограничение числа развертываний	Укажите максимальное число развертываний, которые можно создать при использовании этой схемы элементов для подготовки компьютеров.

Таблица 3-2. Настройки вкладки **Общие** (продолжение)

Параметр	Описание
Аренда (дн.): минимальное значение и максимальное значение	<p>Введите минимальное и максимальные значения, чтобы пользователи могли выбрать продолжительность аренды в пределах заданного диапазона. Когда заканчивается период аренды, развертывание удаляется или архивируется. Если не указать минимальное или максимальное значение, аренда будет длиться бесконечно.</p> <p>Сведения об аренде компьютеров необходимо указать в схеме элементов vRealize Automation, а не в приложении исходной конечной точки. Если информация об аренде указана во внешнем приложении, она не распознается в vRealize Automation.</p>
Хранение в архиве (дн.)	<p>Развертывания можно не удалять сразу по истечении срока аренды, а задать период архивного хранения, чтобы временно сохранить их. Укажите 0, чтобы развертывание удалялось по истечении срока аренды. Период архивного хранения начинается в день истечения срока аренды. Когда заканчивается период архивного хранения, компьютер удаляется. Значение по умолчанию — 0.</p>
Распространение обновлений на существующие развертывания	<p>Расширенные диапазоны значений для ЦП, памяти или хранилища передаются в активные развертывания, подготовленные на основе схемы элементов. Новый диапазон должен включать в себя старый диапазон. Например, если исходное минимальное значение составляет 32, а максимальное — 128 (32, 128), расширенный диапазон (16, 128), (32, 256) или (2, 1000) может вступить в силу после перенастройки или горизонтального масштабирования, но для диапазона (33, 512) или (4, 64) это невозможно.</p>

Вкладка **Параметры NSX**

Если были настроены параметры NSX, то при создании или редактировании схемы элементов можно указать зону транспорта NSX, политику резервирования сети и параметры изоляции приложений. Эти настройки доступны на вкладке **Параметры NSX** на страницах **Схема элементов** и **Свойства схемы элементов**.

Дополнительные сведения о настройках NSX см. в разделе [Настройка страниц «Новая схема элементов» и «Свойства схемы элементов» в vRealize Automation с помощью NSX](#).

Вкладка **Свойства**

Настраиваемые свойства, добавленные на уровне схемы элементов, применяются ко всей схеме элементов, в том числе ко всем компонентам. Информацию о порядке приоритетов настраиваемых свойств см. в разделе *Справочник по настраиваемым свойствам*.

Таблица 3-3. Настройки вкладки **Свойства**

Вкладка	Параметр	Описание
Группы свойств	Группы свойств	Группы свойств — это многоразовые группы свойств, которые упрощают процесс добавления настраиваемых свойств в схемы элементов.
	Добавить	<p>Добавьте одну существующую группу свойств или несколько и примените их к общей схеме элементов.</p> <p>Предоставляются следующие группы свойств, связанных с контейнерами.</p> <ul style="list-style-type: none"> ■ Свойства узла контейнера с проверкой подлинности при помощи сертификата ■ Свойства узла контейнера с проверкой подлинности при помощи имени пользователя и пароля
	Вверх /Вниз	Управление приоритетностью каждой группы свойств относительно других групп. Первая группа в списке имеет наивысший приоритет, а ее настраиваемые свойства наиболее приоритетны. Для изменения порядка можно перемещать ползунков.
	Просмотр свойств	Просмотр настраиваемых свойств в выбранной группе свойств.
	Просмотр объединенных свойств	Если настраиваемое свойство входит в несколько групп свойств, более высокий приоритет имеет значение, которое входит в группу свойств с наивысшим приоритетом.
Настраиваемые свойства	Вместо групп свойств можно добавить отдельные настраиваемые свойства.	
	Создать	Добавьте отдельное настраиваемое свойство и примените его к общей схеме элементов.
	Имя	Введите имя свойства. Список настраиваемых свойств и их определения см. в разделе <i>Справочник по настраиваемым свойствам</i> .
	Значение	Введите значение настраиваемого свойства.
	Зашифровано	Шифрование значения свойства, например в случае, когда это значение является паролем.
	Допускает переопределение	Пользователь схемы элементов может переопределить значение свойства. Если выбран параметр Показывать в запросе , пользователи смогут просматривать и изменять значения свойств при запросе элементов каталога.
	Показывать в запросе	Имя и значение этого свойства будут видны пользователям в форме запроса на подготовку. Чтобы разрешить пользователям самостоятельно вводить значения, выберите Допускает переопределение .

Настройки компонентов компьютера vSphere в vRealize Automation

Рассмотрим настройки и параметры, которые можно задать для компонентов компьютера vSphere на холсте проекта схемы элементов vRealize Automation.

Вкладка **Общие**

Настройте общие параметры для компонента компьютера vSphere.

Таблица 3-4. Настройки вкладки **Общие**

Параметр	Описание
Идентификатор	Введите имя компонента компьютера или оставьте значение по умолчанию.
Описание	Составьте сводку по компоненту компьютера, чтобы ею было удобно пользоваться другим разработчикам архитектуры.
Отобразить расположение по запросу	<p>В облачной среде, например vCloud Air, это позволяет пользователям выбирать область для размещения подготовленных компьютеров.</p> <p>В виртуальной среде можно разрешить пользователям выбирать расположение центра обработки данных, где будут подготавливаться запрошенные компьютеры. Системный администратор должен добавить сведения о центре обработки данных в файл расположений. Администратор структуры должен отредактировать вычислительный ресурс, чтобы связать его с расположением.</p>
Политика резервирования	Политика резервирования применяется к схеме элементов, чтобы компьютеры, подготовленные с использованием этой схемы, были ограничены набором доступных резервирований. Доступны только те политики резервирования, которые применимы к текущему арендатору.
Префикс компьютера	<p>Префиксы компьютеров используются для именования подготовленных компьютеров. Если выбрать Использовать значение для группы по умолчанию, компьютеры получают имя в соответствии с префиксом, который используется по умолчанию для вашей бизнес-группы. Если префикс не указан, он создается на основе имени бизнес-группы. Доступны только те префиксы компьютера, которые применимы к текущему арендатору.</p> <p>Если администратор структуры настроит и сделает другие префиксы компьютеров доступными для выбора, вы сможете применить один префикс ко всем компьютерам, подготовленным по схеме элементов, независимо от того, кто является запрашивающей стороной.</p>
Экземпляры: минимальное значение и максимальное значение	<p>Настройте максимальное и минимальное количество экземпляров, которые пользователи могут запрашивать для развертывания или действий по уменьшению или увеличению масштаба. Если в полях Минимум и Максимум будет введено одно и то же значение, оно будет указывать точное количество экземпляров, которые нужно подготовить.</p> <p>Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операции масштабирования. Если в схеме элементов используются компоненты Все как услуга, можно создать действие для ресурсов, которое пользователи могут запустить после операции масштабирования, чтобы масштабировать или обновить компоненты Все как услуга необходимым образом. Масштабирование можно деактивировать, указав количество экземпляров, доступных каждому компоненту компьютера.</p>

Вкладка **Сведения о сборке**

Настройте параметры сведений о сборке для компонента компьютера vSphere.

Таблица 3-5. Вкладка **Сведения о сборке**

Параметр	Описание
Тип схемы элементов	Для хранения записей и лицензирования выберите, как следует классифицировать компьютеры, подготовленные по этой схеме элементов: как настольные системы или как серверы.
Действие	<p>Варианты, которые отображаются в раскрывающемся меню действия, зависят от типа выбранного компьютера.</p> <p>Доступны следующие действия:</p> <ul style="list-style-type: none"> ■ Создать <p>Создайте спецификацию компонента компьютера, не используя параметр клонирования.</p> ■ Клонировать <p>Создайте копии виртуальной машины из шаблона и объекта настройки.</p> ■ Связанный клон <p>Подготовка копии виртуального компьютера с более эффективным использованием пространства, именуемой связанным клоном. Связанные клоны создаются на основе моментального снимка виртуальной машины и используют цепочку дельта-дисков для отслеживания отличий от родительской виртуальной машины</p> <p>Перед подготовкой виртуальных машин связанного клона выключите моментальный снимок виртуальной машины.</p> ■ NetApp FlexClone <p>Если в резервированиях используется хранилище NetApp FlexClone, можно клонировать компактные копии компьютеров.</p>

Таблица 3-5. Вкладка **Сведения о сборке** (продолжение)

Параметр	Описание
Рабочий процесс подготовки	<p>Варианты, которые отображаются в раскрывающемся меню рабочего процесса подготовки, зависят от типа выбранного компьютера и действия.</p> <ul style="list-style-type: none"> ■ BasicVmWorkflow <p>Подготовка компьютера без гостевой операционной системы.</p> ■ ExternalProvisioningWorkflow <p>Создание компьютера путем запуска из экземпляра виртуальной машины или облачного образа.</p> ■ ImportOvfWorkflow <p>Дает возможность развернуть виртуальную машину vSphere из шаблона OVF аналогично тому, как CloneWorkflow позволяет развернуть виртуальную машину vSphere с помощью шаблона виртуальной машины. Можно импортировать компонент vSphere в схему элементов компьютера или в профиль компонента Image для параметризованной схемы элементов.</p> ■ LinuxKickstartWorkflow <p>Подготовка компьютера путем загрузки из образа ISO, используя файл конфигурации kickstart или autoYaSt и образ дистрибутива Linux для установки операционной системы на компьютер</p> ■ VirtualSccmProvisioningWorkflow <p>Подготовка компьютера и передача управления последовательности задач SCCM для загрузки из образа ISO, развертывания операционной системы Windows и установки гостевого агента vRealize Automation</p> ■ WIMImageWorkflow <p>Подготовка компьютера путем его загрузки в среду WinPE и установки операционной системы с помощью образа WIM существующего эталонного компьютера Windows</p> <p>При использовании рабочего процесса подготовки WIM в схеме элементов укажите размер хранилища, равный суммарной емкости всех дисков, которые будут использоваться в компьютере. В качестве минимального размера хранилища для компонента компьютера укажите общую емкость всех дисков. Укажите также размер каждого диска, емкости которого достаточно, чтобы вместить операционную систему.</p>

Таблица 3-5. Вкладка **Сведения о сборке** (продолжение)

Параметр	Описание
Клонировать из	<p>Выберите шаблон компьютера, который необходимо клонировать. Список доступных шаблонов можно уточнить с помощью параметра Фильтры в раскрывающемся меню каждого из столбцов.</p> <p>Для связанного клона будут отображаться только компьютеры с моментальными снимками, доступными для клонирования, а также компьютеры, которыми управляют от имени администратора арендатора или диспетчера бизнес-групп.</p> <p>Вы можете использовать для клонирования только шаблоны, существующие на компьютерах, которыми вы управляете как диспетчер бизнес-групп или администратор арендатора.</p>
Клонировать из моментального снимка	<p>Для связанного клона выберите существующий моментальный снимок для клонирования в соответствии с выбранным шаблоном компьютера. Компьютеры отображаются в списке только при наличии их моментального снимка и если пользователь управляет ими в качестве администратора арендатора или диспетчера бизнес-групп.</p> <p>Если выбран параметр Использовать текущий моментальный снимок, то создается клон с параметрами, соответствующими последнему состоянию виртуальной машины. Если необходимо выполнить клонирование на основе фактического моментального снимка, щелкните раскрывающееся меню и выберите в списке моментальный снимок.</p> <p>Примечание Название «моментальный снимок» может иногда вводить в заблуждение. Если выбран существующий моментальный снимок, эта функция создает новый диск на основе моментального снимка. Функция Использовать текущий моментальный снимок не использует никакой базовый диск в качестве родительского элемента, она автоматически выполняет полное клонирование.</p> <p>Альтернативный вариант: создать моментальные снимки на базовом диске или использовать рабочий процесс vRealize Orchestrator для создания моментального снимка, а затем немедленно выполнить клонирование на основе этого снимка.</p> <p>Этот вариант доступен только для действия «Связанный клон».</p>
Спецификация настройки	<p>Укажите доступную спецификацию настройки. Эта спецификация нужна, только если клонирование выполняется с помощью статического IP-адреса.</p> <p>Компьютеры Windows нельзя настраивать без спецификации настройки. Для настройки клонированных компьютеров Linux можно использовать спецификацию настройки, внешний сценарий или и то, и другое.</p>

Вкладка **Ресурсы компьютера**

Укажите настройки ЦП, памяти и хранилища для компонента компьютера vSphere.

Таблица 3-6. Вкладка **Ресурсы компьютера**

Параметр	Описание
ЦП: минимальное значение и максимальное значение	Укажите минимальное и максимальное количество ЦП, которые могут использоваться подготовленными компьютерами.
Память (МБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем памяти, который может использоваться подготовленными компьютерами.
Хранилище (ГБ): минимальное значение и максимальное значение	<p>Укажите минимальный и максимальный объем хранилища, который может использоваться подготовленными компьютерами.</p> <p>При использовании рабочего процесса подготовки WIM в схеме элементов укажите размер хранилища, равный суммарной емкости всех дисков, которые будут использоваться в компьютере. В качестве минимального размера хранилища для компонента компьютера укажите общую емкость всех дисков. Укажите также размер каждого диска, емкости которого достаточно, чтобы вместить операционную систему.</p>

Вкладка **Хранилище**

Чтобы контролировать пространство в хранилище, можно добавить в компонент компьютера настройки тома хранилища, в том числе одну или несколько политик резервирования хранилищ.

Таблица 3-7. Настройки вкладки **Хранилище**

Параметр	Описание
Идентификатор	Введите идентификатор или имя тома хранилища.
Емкость (ГБ)	Введите значение емкости системы хранения для тома хранилища.
Буква диска/путь подключения	<p>Введите букву диска или путь монтирования для тома хранилища.</p> <p>Этот параметр используется во время подготовки применительно к гостевому агенту. Его нельзя изменить после подготовки компьютера. Если гостевой агент не используется, этот параметр игнорируется.</p>
Метка	<p>Введите метку для буквы диска и пути монтирования для тома хранилища.</p> <p>Этот параметр используется во время подготовки применительно к гостевому агенту. Его нельзя изменить после подготовки компьютера. Если гостевой агент не используется, этот параметр игнорируется.</p>
Политика резервирования хранилища	Введите существующую политику резервирования хранилища, которая будет использоваться для этого тома хранилища. Доступны только те политики резервирования хранилищ, которые применимы к текущему арендатору.
Настраиваемые свойства	Введите любые настраиваемые свойства, которые будут использоваться с этим томом хранилища.

Таблица 3-7. Настройки вкладки **Хранилище** (продолжение)

Параметр	Описание
Максимальное количество томов	Введите максимально допустимое количество томов хранилищ, которые можно использовать при подготовке из компонента компьютера. Введите 0, чтобы другие пользователи не могли добавлять тома хранилищ. Значение по умолчанию — 60.
Разрешить пользователю просматривать и менять политики резервирования хранилища	Установите этот флажок, чтобы разрешить пользователям удалять соответствующие политики резервирования или указать другую политику резервирования при подготовке.

Вкладка **Сеть**

Параметры сети для компонента компьютера vSphere можно настроить на основе параметров сети и подсистемы балансировки нагрузки NSX, которые настраиваются за пределами vRealize Automation. Настройки одного или нескольких существующих и предоставляемых по требованию сетевых компонентов NSX можно использовать на холсте проекта.

Дополнительные сведения см. в разделах [Настройка параметров компонентов сети и безопасности в vRealize Automation](#) и [Настройка страниц «Новая схема элементов» и «Свойства схемы элементов» в vRealize Automation с помощью NSX](#).

Таблица 3-8. Настройки вкладки **Сеть**

Параметр	Описание
Сеть	Выберите компонент сети в раскрывающемся меню. В нем перечислены только сетевые компоненты, которые существуют на холсте проекта. Доступны только те профили сети, которые применимы к текущему арендатору. Выбранная сеть определяет тип сети и указывает, чем управляется кластер, который развертывается в сети — NSX for vSphere или NSX-T.
Тип назначения	Примите значение, назначенное по умолчанию в соответствии с настройками сетевого компонента, или выберите тип назначения в раскрывающемся меню. Значения параметров DHCP и Статический задаются на основе настроек сетевого компонента.
Адрес	Укажите IP-адрес сети. Этот параметр доступен только для адресов статического типа.
Балансировка нагрузки	Введите службу, которую следует использовать для балансировки нагрузки.
Настраиваемые свойства	Отображение настраиваемых свойств, заданных для выбранного сетевого компонента или профиля сети.
Максимальное количество сетевых адаптеров	Укажите максимально допустимое количество сетевых адаптеров для этого компонента компьютера. По умолчанию значение является неограниченным. Установите значение 0, чтобы деактивировать добавление сетевых адаптеров для компонентов компьютера.

Вкладка **Безопасность**

Параметры безопасности для компонента компьютера vSphere можно настроить на основе параметров NSX, которые настраиваются за пределами vRealize Automation. При необходимости настройки существующих и предоставляемых по требованию компонентов безопасности NSX можно использовать на холсте проекта.

Параметры безопасности существующих и предоставляемых по требованию компонентов «Группа безопасности» и «Тег безопасности» на холсте проекта доступны автоматически.

Дополнительные сведения о добавлении и настройке компонентов сети и безопасности NSX перед использованием параметров вкладки «Безопасность» в компоненте компьютера vSphere см. в разделе [Настройка параметров компонентов сети и безопасности в vRealize Automation](#).

Дополнительные сведения об указании данных NSX, применимых ко всем компонентам компьютера vSphere в схеме элементов, см. в разделе [Настройка страниц «Новая схема элементов» и «Свойства схемы элементов» в vRealize Automation с помощью NSX](#).

Таблица 3-9. Настройки вкладки **Безопасность**

Параметр	Описание
Имя	Отображение имени группы или тега безопасности NSX. Имена создаются на основе компонентов безопасности на холсте проекта. Установите флажок рядом с группой или тегом безопасности в списке, чтобы использовать эту группу или тег для подготовки из этого компонента компьютера.
Тип	Укажите группу, к которой принадлежит элемент безопасности (предоставляемая по требованию группа безопасности, существующая группа безопасности или тег безопасности).
Описание	Отображение описания, определенного для группы или тега безопасности.
Конечная точка	Отображение конечной точки, используемой группой или тегом безопасности NSX.

Вкладка **Свойства**

Укажите информацию о настраиваемых свойствах и группе свойств для компонента компьютера vSphere.

На вкладке **Свойства** можно добавить в компонент компьютера отдельные настраиваемые свойства или их группы. Кроме того, при создании или редактировании схемы элементов на вкладке **Свойства** на странице **Свойства схемы элементов** можно добавлять настраиваемые свойства и группы свойств в общую схему элементов.

На вкладке **Настраиваемые свойства** можно добавлять и настраивать параметры существующих настраиваемых свойств. Некоторые настраиваемые свойства изначально предусмотрены в vRealize Automation, однако можно также создать новые настраиваемые свойства.

Таблица 3-10. Настройки вкладки **Свойства > Настраиваемые свойства**

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню. В раскрывающемся меню свойства отображаются, только если администратор арендатора или администратор структуры создал определения свойств.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства. Например, установите значение <code>true</code> , чтобы разрешить пользователям подключаться к виртуальным машинам по SSH.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Если выбран параметр Показывать в запросе , пользователи могут изменять значения свойств при запросе элементов каталога.
Показывать в запросе	Для пользователей, запрашивающих подготовку компьютеров, можно отображать имя и значение свойства. Чтобы пользователи могли вводить необходимое значение, выберите параметр «Допускает переопределение».

На вкладке **Группы свойств** можно добавлять и настраивать параметры существующих групп настраиваемых свойств. Можно создать собственные или использовать уже созданные группы свойств.

Таблица 3-11. Настройки вкладки **Свойства > Группы свойств**

Параметр	Описание
Имя	Выберите доступную группу свойств в раскрывающемся меню.
Вверх и Вниз	Позволяет управлять уровнем приоритета групп свойств в порядке убывания. Первая в списке группа свойств имеет более высокий приоритет, чем вторая и так далее.
Просмотр свойств	Позволяет отобразить настраиваемые свойства в выбранной группе свойств.
Просмотр объединенных свойств	Отображение настраиваемых свойств в том порядке, в котором они отображаются в списке групп свойств. Если одно и то же свойство присутствует в нескольких группах, это свойство отображается в списке только один раз, когда оно встречается впервые.

Вкладка «Профили»

Профили компонентов предоставляют инструменты для параметризации схем элементов. Например, вместо создания отдельных схем элементов можно создать малую, среднюю и большую возможность в одной схеме элементов. Размер схемы элементов можно выбрать во время развертывания. Профили компонентов позволяют упростить каталог.

Если вы создали наборы значений для предоставленных профилей компонентов Size и Image vRealize Automation, вы можете настроить эти параметры компонентов компьютеров в схеме элементов. Можно также выбрать другой набор значений при развертывании элемента каталога.

Профили компонентов доступны только для компонентов компьютеров vSphere.

Профиль компонента переопределяет параметры компонента компьютера, например количество ЦП и хранилище.

Набор значений профиля компонента применяется ко всем компьютерам vSphere в кластере.

С помощью профилей компонентов Size и Image компьютеры перенастроить нельзя. Диапазон ресурсов ЦП, памяти и хранилища из рассчитывается из профиля и остается доступным при выполнении действий по перенастройке. Например, можно использовать следующие наборы значений Size: малый (1 ЦП, объем памяти — 1024 МБ, объем хранилища — 10 ГБ), средний (3 ЦП, объем памяти — 2048 МБ, объем хранилища — 12 ГБ) и большой (5 ЦП, объем памяти — 3072 МБ памяти, объем хранилища — 15 ГБ) . При перенастройке компьютера доступны следующие диапазоны ресурсов: количество ЦП — от 1 до 5, объем памяти — от 1024 до 3072 ГБ, объем хранилища — от 1 до 15 ГБ.

Дополнительные сведения см. в разделе *Справочник по настраиваемым свойствам*.

Таблица 3-12. Настройки вкладки **Профили**

Параметр	Описание
Добавить	Добавление профиля компонента Size или Image.
Изменить наборы значений	Назначение одного или нескольких наборов значений для выбранного профиля компонента путем выбора из списка определенных наборов значений. Можно выбрать один из наборов значений для использования по умолчанию.
Удалить	Удаление профиля компонента Size или Image.

Настройки компонентов компьютера vCloud Air

Рассмотрим настройки и параметры, которые можно задать для компонентов компьютера vCloud Air на холсте проекта схемы элементов vRealize Automation.

Вкладка **Общие**

Настройте общие параметры для компонента компьютера vCloud Air.

Таблица 3-13. Настройки вкладки **Общие**

Параметр	Описание
Идентификатор	Введите имя компонента компьютера или оставьте значение по умолчанию.
Описание	Составьте сводку по компоненту компьютера, чтобы ею было удобно пользоваться другим разработчикам архитектуры.

Таблица 3-13. Настройки вкладки **Общие** (продолжение)

Параметр	Описание
Отобразить расположение по запросу	<p>В облачной среде, например vCloud Air, это позволяет пользователям выбирать область для размещения подготовленных компьютеров.</p> <p>В виртуальной среде можно разрешить пользователям выбирать расположение центра обработки данных, где будут подготавливаться запрошенные компьютеры. Системный администратор должен добавить сведения о центре обработки данных в файл расположений. Администратор структуры должен отредактировать вычислительный ресурс, чтобы связать его с расположением.</p>
Политика резервирования	<p>Политика резервирования применяется к схеме элементов, чтобы компьютеры, подготовленные с использованием этой схемы, были ограничены набором доступных резервирований. Доступны только те политики резервирования, которые применимы к текущему арендатору.</p>
Префикс компьютера	<p>Префиксы компьютеров используются для именования подготовленных компьютеров. Если выбрать Использовать значение для группы по умолчанию, компьютеры получают имя в соответствии с префиксом, который используется по умолчанию для вашей бизнес-группы. Если префикс не указан, он создается на основе имени бизнес-группы. Доступны только те префиксы компьютера, которые применимы к текущему арендатору.</p> <p>Если администратор структуры настроит и сделает другие префиксы компьютеров доступными для выбора, вы сможете применить один префикс ко всем компьютерам, подготовленным по схеме элементов, независимо от того, кто является запрашивающей стороной.</p>
Экземпляры: минимальное значение и максимальное значение	<p>Настройте максимальное и минимальное количество экземпляров, которые пользователи могут запрашивать для развертывания или действий по уменьшению или увеличению масштаба. Если в полях Минимум и Максимум будет введено одно и то же значение, оно будет указывать точное количество экземпляров, которые нужно подготовить.</p> <p>Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операции масштабирования. Если в схеме элементов используются компоненты Все как услуга, можно создать действие для ресурсов, которое пользователи могут запустить после операции масштабирования, чтобы масштабировать или обновить компоненты Все как услуга необходимым образом. Масштабирование можно деактивировать, указав количество экземпляров, доступных каждому компоненту компьютера.</p>

Вкладка **Сведения о сборке**

Настройте параметры сведений о сборке для компонента компьютера vCloud Air.

Таблица 3-14. Вкладка **Сведения о сборке**

Параметр	Описание
Тип схемы элементов	Для хранения записей и лицензирования выберите, как следует классифицировать компьютеры, подготовленные по этой схеме элементов: как настольные системы или как серверы.
Действие	<p>Варианты, которые отображаются в раскрывающемся меню действия, зависят от типа выбранного компьютера.</p> <p>Единственное действие подготовки, доступное для компонента компьютера vCloud Air, — клонирование.</p> <p>■ Клонировать</p> <p>Создайте копии виртуальной машины из шаблона и объекта настройки.</p>
Рабочий процесс подготовки	<p>Варианты, которые отображаются в раскрывающемся меню рабочего процесса подготовки, зависят от типа выбранного компьютера и действия.</p> <p>Единственное действие подготовки, доступное для компонента компьютера vCloud Air — клонирование рабочего процесса.</p> <p>■ CloneWorkflow</p> <p>Создание копий виртуальной машины в форме клона, связанного клона или NetApp FlexClone.</p>
Клонировать из	<p>Выберите шаблон компьютера, который необходимо клонировать. Список доступных шаблонов можно уточнить с помощью параметра Фильтры в раскрывающемся меню каждого из столбцов.</p> <p>Для связанного клона будут отображаться только компьютеры с моментальными снимками, доступными для клонирования, а также компьютеры, которыми управляют от имени администратора арендатора или диспетчера бизнес-групп.</p> <p>Вы можете использовать для клонирования только шаблоны, существующие на компьютерах, которыми вы управляете как диспетчер бизнес-групп или администратор арендатора.</p>

Вкладка **Ресурсы компьютера**

Укажите настройки ЦП, памяти и хранилища для компонента компьютера vCloud Air.

Таблица 3-15. Вкладка **Ресурсы компьютера**

Параметр	Описание
ЦП: минимальное значение и максимальное значение	Укажите минимальное и максимальное количество ЦП, которые могут использоваться подготовленными компьютерами.
Память (МБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем памяти, который может использоваться подготовленными компьютерами.
Хранилище (ГБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем хранилища, который может использоваться подготовленными компьютерами.

Вкладка **Хранилище**

Чтобы контролировать пространство в хранилище, можно добавить в компонент компьютера настройки тома хранилища, в том числе одну или несколько политик резервирования хранилищ.

Таблица 3-16. Настройки вкладки **Хранилище**

Параметр	Описание
Идентификатор	Введите идентификатор или имя тома хранилища.
Емкость (ГБ)	Введите значение емкости системы хранения для тома хранилища.
Буква диска/путь подключения	Введите букву диска или путь монтирования для тома хранилища. Этот параметр используется во время подготовки применительно к гостевому агенту. Его нельзя изменить после подготовки компьютера. Если гостевой агент не используется, этот параметр игнорируется.
Метка	Введите метку для буквы диска и пути монтирования для тома хранилища. Этот параметр используется во время подготовки применительно к гостевому агенту. Его нельзя изменить после подготовки компьютера. Если гостевой агент не используется, этот параметр игнорируется.
Политика резервирования хранилища	Введите существующую политику резервирования хранилища, которая будет использоваться для этого тома хранилища. Доступны только те политики резервирования хранилищ, которые применимы к текущему арендатору.
Настраиваемые свойства	Введите любые настраиваемые свойства, которые будут использоваться с этим томом хранилища.
Максимальное количество томов	Введите максимально допустимое количество томов хранилищ, которые можно использовать при подготовке из компонента компьютера. Введите 0, чтобы другие пользователи не могли добавлять тома хранилищ. Значение по умолчанию — 60.
Разрешить пользователю просматривать и менять политики резервирования хранилища	Установите этот флажок, чтобы разрешить пользователям удалять соответствующие политики резервирования или указать другую политику резервирования при подготовке.

Вкладка **Свойства**

При необходимости укажите информацию о настраиваемых свойствах и группе свойств для компонента компьютера vCloud Air.

На вкладке **Свойства** можно добавить в компонент компьютера отдельные настраиваемые свойства или их группы. Кроме того, при создании или редактировании схемы элементов на вкладке **Свойства** на странице **Свойства схемы элементов** можно добавлять настраиваемые свойства и группы свойств в общую схему элементов.

На вкладке **Настраиваемые свойства** можно добавлять и настраивать параметры существующих настраиваемых свойств. Некоторые настраиваемые свойства изначально предусмотрены в vRealize Automation, однако можно также создать новые настраиваемые свойства.

Таблица 3-17. Настройки вкладки **Свойства > Настраиваемые свойства**

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню. В раскрывающемся меню свойства отображаются, только если администратор арендатора или администратор структуры создал определения свойств.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства. Например, установите значение <code>true</code> , чтобы разрешить пользователям подключаться к виртуальным машинам по SSH.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Если выбран параметр Показывать в запросе , пользователи могут изменять значения свойств при запросе элементов каталога.
Показывать в запросе	Для пользователей, запрашивающих подготовку компьютеров, можно отображать имя и значение свойства. Чтобы пользователи могли вводить необходимое значение, выберите параметр «Допускает переопределение».

На вкладке **Группы свойств** можно добавлять и настраивать параметры существующих групп настраиваемых свойств. Можно создать собственные или использовать уже созданные группы свойств.

Таблица 3-18. Настройки вкладки **Свойства > Группы свойств**

Параметр	Описание
Имя	Выберите доступную группу свойств в раскрывающемся меню.
Вверх и Вниз	Позволяет управлять уровнем приоритета групп свойств в порядке убывания. Первая в списке группа свойств имеет более высокий приоритет, чем вторая и так далее.
Просмотр свойств	Позволяет отобразить настраиваемые свойства в выбранной группе свойств.
Просмотр объединенных свойств	Отображение настраиваемых свойств в том порядке, в котором они отображаются в списке групп свойств. Если одно и то же свойство присутствует в нескольких группах, это свойство отображается в списке только один раз, когда оно встречается впервые.

Настройки компонентов компьютера Amazon

Рассмотрим настройки и параметры, которые можно задать для компонентов компьютера Amazon на холсте проекта схемы элементов vRealize Automation.

Вкладка **Общие**

Настройте общие параметры для компонента компьютера Amazon.

Таблица 3-19. Настройки вкладки **Общие**

Параметр	Описание
Идентификатор	Введите имя компонента компьютера или оставьте значение по умолчанию.
Описание	Составьте сводку по компоненту компьютера, чтобы ею было удобно пользоваться другим разработчикам архитектуры.
Отобразить расположение по запросу	<p>В облачной среде, например vCloud Air, это позволяет пользователям выбирать область для размещения подготовленных компьютеров.</p> <p>В виртуальной среде можно разрешить пользователям выбирать расположение центра обработки данных, где будут подготавливаться запрошенные компьютеры. Системный администратор должен добавить сведения о центре обработки данных в файл расположений. Администратор структуры должен отредактировать вычислительный ресурс, чтобы связать его с расположением.</p>
Политика резервирования	Политика резервирования применяется к схеме элементов, чтобы компьютеры, подготовленные с использованием этой схемы, были ограничены набором доступных резервирований. Доступны только те политики резервирования, которые применимы к текущему арендатору.
Префикс компьютера	<p>Префиксы компьютеров используются для именования подготовленных компьютеров. Если выбрать Использовать значение для группы по умолчанию, компьютеры получают имя в соответствии с префиксом, который используется по умолчанию для вашей бизнес-группы. Если префикс не указан, он создается на основе имени бизнес-группы. Доступны только те префиксы компьютера, которые применимы к текущему арендатору.</p> <p>Если администратор структуры настроит и сделает другие префиксы компьютеров доступными для выбора, вы сможете применить один префикс ко всем компьютерам, подготовленным по схеме элементов, независимо от того, кто является запрашивающей стороной.</p>
Экземпляры: минимальное значение и максимальное значение	<p>Настройте максимальное и минимальное количество экземпляров, которые пользователи могут запрашивать для развертывания или действий по уменьшению или увеличению масштаба. Если в полях Минимум и Максимум будет введено одно и то же значение, оно будет указывать точное количество экземпляров, которые нужно подготовить.</p> <p>Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операции масштабирования. Если в схеме элементов используются компоненты Все как услуга, можно создать действие для ресурсов, которое пользователи могут запустить после операции масштабирования, чтобы масштабировать или обновить компоненты Все как услуга необходимым образом. Масштабирование можно деактивировать, указав количество экземпляров, доступных каждому компоненту компьютера.</p>

Вкладка **Сведения о сборке**

Настройте параметры сведений о сборке для компонента компьютера Amazon.

Таблица 3-20. Вкладка «Сведения о сборке»

Параметр	Описание
Тип схемы элементов	Для хранения записей и лицензирования выберите, как следует классифицировать компьютеры, подготовленные по этой схеме элементов: как настольные системы или как серверы.
Рабочий процесс подготовки	<p>Единственный рабочий процесс подготовки, доступный для компонента компьютера Amazon, — CloudProvisioningWorkflow.</p> <ul style="list-style-type: none"> ■ CloudProvisioningWorkflow <p>Создание компьютера путем запуска из экземпляра виртуальной машины или облачного образа.</p>
Образ компьютера Amazon	<p>Выберите доступный образ компьютера Amazon. Образ компьютера Amazon — это шаблон, который содержит данные конфигурации программного обеспечения, в том числе операционной системы. Для управления образами компьютеров используются учетные записи Amazon Web Services. Список имен образов компьютеров Amazon можно уточнить с помощью параметра Фильтры в раскрывающемся меню столбца Идентификатор AMI.</p>
Пара ключей	<p>Для подготовки с помощью служб Amazon Web Services необходимы пары ключей.</p> <p>Пары ключей используются для подготовки экземпляра облака и подключения к нему. Они также используются для расшифровки паролей Windows и входа в компьютер Linux.</p> <p>Доступны следующие параметры пар ключей:</p> <ul style="list-style-type: none"> ■ Не указано <p>Управляет поведением пары ключей на уровне схемы элементов, а не на уровне резервирования.</p> ■ Автоматически создаются для каждой бизнес-группы <p>Указывает, что все компьютеры, подготовленные в одной и той же бизнес-группе, имеют одинаковые пары ключей, включая компьютеры, подготовленные в других резервированиях, если у них такие же вычислительные ресурсы и бизнес-группа. Так как эти пары ключей связаны с бизнес-группой, они удаляются при удалении бизнес-группы.</p> ■ Автоматически создаются для каждого компьютера <p>Указывает, что для каждого компьютера используется уникальная пара ключей. Автоматически созданный для каждого компьютера параметр является наиболее безопасным методом, поскольку компьютеры не используют одинаковые пары ключей.</p>

Таблица 3-20. Вкладка «Сведения о сборке» (продолжение)

Параметр	Описание
Включение параметров сети Amazon на компьютере	Укажите, нужно ли разрешить пользователям подготавливать компьютер в Virtual Private Cloud (VPC) или в другом расположении вне VPC при отправке запроса.
Типы экземпляров	<p>Выберите один или несколько типов экземпляров Amazon. Экземпляр Amazon представляет собой виртуальный сервер, на котором могут выполняться приложения в Amazon Web Services. Экземпляры создаются на основе образа компьютера Amazon при выборе соответствующего типа экземпляра. С помощью vRealize Automation можно управлять доступными для подготовки типами экземпляров образов компьютеров.</p> <p>Сведения о типах экземпляров Amazon в vRealize Automation см. в разделах Общие сведения о типах экземпляров Amazon и Добавление типа экземпляра Amazon.</p>

Вкладка **Ресурсы компьютера**

Укажите настройки ЦП, памяти, хранилища и тома EBS для компонента компьютера Amazon.

Можно также перенастроить все тома хранилища компьютера Amazon в развертывании, за исключением корневого тома.

Таблица 3-21. Вкладка **Ресурсы компьютера**

Параметр	Описание
ЦП: минимальное значение и максимальное значение	Укажите минимальное и максимальное количество ЦП, которые могут использоваться подготовленными компьютерами.
Память (МБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем памяти, который может использоваться подготовленными компьютерами.
Хранилище (ГБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем хранилища, который может использоваться подготовленными компьютерами.

Таблица 3-21. Вкладка **Ресурсы компьютера** (продолжение)

Параметр	Описание
Хранилище EBS (ГБ): минимальное значение и максимальное значение	<p>Укажите минимальный и максимальный объем хранилища Amazon Elastic Block Store (EBS), который может использоваться подготовленными компьютерами.</p> <p>При уничтожении развертывания, в котором содержится компонент компьютера Amazon, все тома EBS, добавленные на компьютер во время его жизненного цикла, отделяются, а не уничтожаются. vRealize Automation не предоставляет параметр для уничтожения объемов EBS.</p>
Удалить тома	<p>Указывает, можно ли при удалении развертываний Amazon удалять тома EC2 по отдельности или в пакетном режиме. Оба ответа («Да» и «Нет») дают возможность удалить в пакетном режиме все тома в развертывании. Значение по умолчанию — null или пустое поле.</p> <ul style="list-style-type: none"> ■ «Да» — удалить развертывание Amazon и тома. ■ «Нет» — удалить развертывание Amazon и сохранить тома. ■ null или пустое поле — при удалении развертываний Amazon пользователь должен выбрать значение «Да» или «Нет».

Вкладка **Свойства**

При необходимости укажите информацию о настраиваемых свойствах и группе свойств для компонента компьютера Amazon.

На вкладке **Свойства** можно добавить в компонент компьютера отдельные настраиваемые свойства или их группы. Кроме того, при создании или редактировании схемы элементов на вкладке **Свойства** на странице **Свойства схемы элементов** можно добавлять настраиваемые свойства и группы свойств в общую схему элементов.

На вкладке **Настраиваемые свойства** можно добавлять и настраивать параметры существующих настраиваемых свойств. Некоторые настраиваемые свойства изначально предусмотрены в vRealize Automation, однако можно также создать новые настраиваемые свойства.

Таблица 3-22. Настройки вкладки **Свойства > Настраиваемые свойства**

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню. В раскрывающемся меню свойства отображаются, только если администратор арендатора или администратор структуры создал определения свойств.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства. Например, установите значение true, чтобы разрешить пользователям подключаться к виртуальным машинам по SSH.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.

Таблица 3-22. Настройки вкладки **Свойства > Настраиваемые свойства** (продолжение)

Параметр	Описание
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Если выбран параметр Показывать в запросе , пользователи могут изменять значения свойств при запросе элементов каталога.
Показывать в запросе	Для пользователей, запрашивающих подготовку компьютеров, можно отображать имя и значение свойства. Чтобы пользователи могли вводить необходимое значение, выберите параметр «Допускает переопределение».

На вкладке **Группы свойств** можно добавлять и настраивать параметры существующих групп настраиваемых свойств. Можно создать собственные или использовать уже созданные группы свойств.

Таблица 3-23. Настройки вкладки **Свойства > Группы свойств**

Параметр	Описание
Имя	Выберите доступную группу свойств в раскрывающемся меню.
Вверх и Вниз	Позволяет управлять уровнем приоритета групп свойств в порядке убывания. Первая в списке группа свойств имеет более высокий приоритет, чем вторая и так далее.
Просмотр свойств	Позволяет отобразить настраиваемые свойства в выбранной группе свойств.
Просмотр объединенных свойств	Отображение настраиваемых свойств в том порядке, в котором они отображаются в списке групп свойств. Если одно и то же свойство присутствует в нескольких группах, это свойство отображается в списке только один раз, когда оно встречается впервые.

Настройки компонентов компьютера OpenStack

Рассмотрим настройки и параметры, которые можно задать для компонентов компьютера OpenStack на холсте проекта схемы элементов vRealize Automation.

Вкладка **Общие**

Настройте общие параметры для компонента компьютера OpenStack.

Таблица 3-24. Настройки вкладки **Общие**

Параметр	Описание
Идентификатор	Введите имя компонента компьютера или оставьте значение по умолчанию.
Описание	Составьте сводку по компоненту компьютера, чтобы ею было удобно пользоваться другим разработчикам архитектуры.

Таблица 3-24. Настройки вкладки **Общие** (продолжение)

Параметр	Описание
Отобразить расположение по запросу	<p>В облачной среде, например vCloud Air, это позволяет пользователям выбирать область для размещения подготовленных компьютеров.</p> <p>В виртуальной среде можно разрешить пользователям выбирать расположение центра обработки данных, где будут подготавливаться запрошенные компьютеры. Системный администратор должен добавить сведения о центре обработки данных в файл расположений. Администратор структуры должен отредактировать вычислительный ресурс, чтобы связать его с расположением.</p>
Политика резервирования	Политика резервирования применяется к схеме элементов, чтобы компьютеры, подготовленные с использованием этой схемы, были ограничены набором доступных резервирований. Доступны только те политики резервирования, которые применимы к текущему арендатору.
Префикс компьютера	<p>Префиксы компьютеров используются для именования подготовленных компьютеров. Если выбрать Использовать значение для группы по умолчанию, компьютеры получают имя в соответствии с префиксом, который используется по умолчанию для вашей бизнес-группы. Если префикс не указан, он создается на основе имени бизнес-группы. Доступны только те префиксы компьютера, которые применимы к текущему арендатору.</p> <p>Если администратор структуры настроит и сделает другие префиксы компьютеров доступными для выбора, вы сможете применить один префикс ко всем компьютерам, подготовленным по схеме элементов, независимо от того, кто является запрашивающей стороной.</p>
Экземпляры: минимальное значение и максимальное значение	<p>Настройте максимальное и минимальное количество экземпляров, которые пользователи могут запрашивать для развертывания или действий по уменьшению или увеличению масштаба. Если в полях Минимум и Максимум будет введено одно и то же значение, оно будет указывать точное количество экземпляров, которые нужно подготовить.</p> <p>Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операции масштабирования. Если в схеме элементов используются компоненты Все как услуга, можно создать действие для ресурсов, которое пользователи могут запустить после операции масштабирования, чтобы масштабировать или обновить компоненты Все как услуга необходимым образом. Масштабирование можно деактивировать, указав количество экземпляров, доступных каждому компоненту компьютера.</p>

Вкладка **Сведения о сборке**

Настройте параметры сведений о сборке для компонента компьютера OpenStack.

Таблица 3-25. Вкладка **Сведения о сборке**

Параметр	Описание
Тип схемы элементов	Для хранения записей и лицензирования выберите, как следует классифицировать компьютеры, подготовленные по этой схеме элементов: как настольные системы или как серверы.
Рабочий процесс подготовки	<p>Для компонентов компьютеров OpenStack доступны следующие рабочие процессы подготовки:</p> <ul style="list-style-type: none"> ■ CloudLinuxKickstartWorkflow Подготовка компьютера путем загрузки из образа ISO, используя файл конфигурации kickstart или autoYaSt и образ дистрибутива Linux для установки операционной системы на компьютер ■ CloudProvisioningWorkflow Создание компьютера путем запуска из экземпляра виртуальной машины или облачного образа. ■ CloudWIMImageWorkflow Подготовка компьютера путем его загрузки в среду WinPE и установки операционной системы с помощью образа WIM существующего эталонного компьютера Windows При использовании рабочего процесса подготовки WIM в схеме элементов укажите размер хранилища, равный суммарной емкости всех дисков, которые будут использоваться в компьютере. В качестве минимального размера хранилища для компонента компьютера укажите общую емкость всех дисков. Укажите также размер каждого диска, емкости которого достаточно, чтобы вместить операционную систему.
Образ OpenStack	Выберите доступный образ OpenStack. Образ OpenStack — это шаблон, который содержит данные конфигурации программного обеспечения, в том числе операционной системы. Для управления образами используются учетные записи OpenStack. Список имен образов OpenStack можно уточнить с помощью параметра Фильтры в раскрывающемся меню столбца Имена .

Таблица 3-25. Вкладка **Сведения о сборке** (продолжение)

Параметр	Описание
Пара ключей	<p>Пары ключей необязательны для подготовки с использованием OpenStack.</p> <p>Пары ключей используются для подготовки экземпляра облака и подключения к нему. Они также используются для расшифровки паролей Windows и входа в компьютер Linux.</p> <p>Доступны следующие параметры пар ключей:</p> <ul style="list-style-type: none"> ■ Не указано <p>Управляет поведением пары ключей на уровне схемы элементов, а не на уровне резервирования.</p> ■ Автоматически создаются для каждой бизнес-группы <p>Указывает, что все компьютеры, подготовленные в одной и той же бизнес-группе, имеют одинаковые пары ключей, включая компьютеры, подготовленные в других резервированиях, если у них такие же вычислительные ресурсы и бизнес-группа. Так как эти пары ключей связаны с бизнес-группой, они удаляются при удалении бизнес-группы.</p> ■ Автоматически создаются для каждого компьютера <p>Указывает, что для каждого компьютера используется уникальная пара ключей. Автоматически созданный для каждого компьютера параметр является наиболее безопасным методом, поскольку компьютеры не используют одинаковые пары ключей.</p>
Версии	<p>Выберите нужные версии OpenStack. Версия OpenStack представляет собой шаблон виртуального оборудования, по которому определяются спецификации ресурсов компьютера для экземпляров, подготовленных в OpenStack. За управление версиями отвечает поставщик OpenStack. Они импортируются при сборе данных.</p>

Вкладка **Ресурсы компьютера**

Укажите настройки ЦП, памяти и хранилища для компонента компьютера OpenStack.

Таблица 3-26. Вкладка **Ресурсы компьютера**

Параметр	Описание
ЦП: минимальное значение и максимальное значение	Укажите минимальное и максимальное количество ЦП, которые могут использоваться подготовленными компьютерами.
Память (МБ): минимальное значение и максимальное значение	Укажите минимальный и максимальный объем памяти, который может использоваться подготовленными компьютерами.
Хранилище (ГБ): минимальное значение и максимальное значение	<p>Укажите минимальный и максимальный объем хранилища, который может использоваться подготовленными компьютерами.</p> <p>При использовании рабочего процесса подготовки WIM в схеме элементов укажите размер хранилища, равный суммарной емкости всех дисков, которые будут использоваться в компьютере. В качестве минимального размера хранилища для компонента компьютера укажите общую емкость всех дисков. Укажите также размер каждого диска, емкости которого достаточно, чтобы вместить операционную систему.</p>

Вкладка **Свойства**

При необходимости укажите информацию о настраиваемых свойствах и группе свойств для компонента компьютера OpenStack.

На вкладке **Свойства** можно добавить в компонент компьютера отдельные настраиваемые свойства или их группы. Кроме того, при создании или редактировании схемы элементов на вкладке **Свойства** на странице **Свойства схемы элементов** можно добавлять настраиваемые свойства и группы свойств в общую схему элементов.

На вкладке **Настраиваемые свойства** можно добавлять и настраивать параметры существующих настраиваемых свойств. Некоторые настраиваемые свойства изначально предусмотрены в vRealize Automation, однако можно также создать новые настраиваемые свойства.

Таблица 3-27. Настройки вкладки **Свойства > Настраиваемые свойства**

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню. В раскрывающемся меню свойства отображаются, только если администратор арендатора или администратор структуры создал определения свойств.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства. Например, установите значение <code>true</code> , чтобы разрешить пользователям подключаться к виртуальным машинам по SSH.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.

Таблица 3-27. Настройки вкладки **Свойства > Настраиваемые свойства** (продолжение)

Параметр	Описание
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Если выбран параметр Показывать в запросе , пользователи могут изменять значения свойств при запросе элементов каталога.
Показывать в запросе	Для пользователей, запрашивающих подготовку компьютеров, можно отображать имя и значение свойства. Чтобы пользователи могли вводить необходимое значение, выберите параметр «Допускает переопределение».

На вкладке **Группы свойств** можно добавлять и настраивать параметры существующих групп настраиваемых свойств. Можно создать собственные или использовать уже созданные группы свойств.

Таблица 3-28. Настройки вкладки **Свойства > Группы свойств**

Параметр	Описание
Имя	Выберите доступную группу свойств в раскрывающемся меню.
Вверх и Вниз	Позволяет управлять уровнем приоритета групп свойств в порядке убывания. Первая в списке группа свойств имеет более высокий приоритет, чем вторая и так далее.
Просмотр свойств	Позволяет отобразить настраиваемые свойства в выбранной группе свойств.
Просмотр объединенных свойств	Отображение настраиваемых свойств в том порядке, в котором они отображаются в списке групп свойств. Если одно и то же свойство присутствует в нескольких группах, это свойство отображается в списке только один раз, когда оно встречается впервые.

Использование настраиваемых свойств сети

Указать сведения о сети и безопасности для компонентов другого компьютера (не vSphere) и схем элементов, которые не содержат NSX, можно с помощью настраиваемых свойств на уровне схемы элементов или компонентов компьютера.

Компоненты **сети и безопасности** можно использовать только с компонентами компьютеров vSphere. У компонентов компьютера, не относящихся к vSphere, нет вкладок **Сеть** и **Безопасность**.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

Настраиваемые свойства можно определить отдельно или в составе существующей группы свойств на вкладке **Свойства** при настройке компонента компьютера на холсте проекта. Настраиваемые свойства, определенные для компонента компьютера, относятся к компьютерам того типа, для которого была выполнена подготовка из схемы элементов.

Сведения о доступных настраиваемых свойствах см. в разделе *Справочник по настраиваемым свойствам*.

Устранение проблем со схемами элементов при работе с клонами и связанными клонами

При создании связанного клона или клона отсутствуют схема элементов, компьютер или шаблоны. При использовании общей схемы элементов клона для запроса компьютеров происходит сбой подготовки компьютеров.

Проблема

При работе со схемами элементов клона или связанного клона может произойти одна из следующих проблем:

- При создании схемы элементов связанного клона в списке для клонирования не отображаются компьютеры или не отображается компьютер, который нужно клонировать.
- При создании схемы элементов клона в списке для клонирования не отображаются шаблоны или не отображается шаблон, который нужно клонировать.
- При использовании общей схемы элементов клона для запроса компьютеров происходит сбой подготовки.
- Вследствие согласования сбора данных по времени удаленный шаблон все еще отображается пользователям, когда они создают или изменяют схемы элементов связанного клона.

Имейте в виду, что связанные клоны не поддерживаются при подготовке в SDRS. Связанные клоны создаются в том же хранилище данных, в котором находится родительский объект, и не перераспределяются между хранилищами данных кластера. При этом хранилище, где находится родительский объект, со временем может переполниться.

Причина

Стандартные проблемы со схемами элементов клона или связанного клона происходят по нескольким возможным причинам.

Дополнительные сведения об использовании функций **Клонировать из** и **Клонировать из моментального снимка** с параметром **Использовать текущий моментальный снимок** во время создания схемы элементов см. в разделе [Настройки компонентов компьютера vSphere в vRealize Automation](#).

Таблица 3-29. Причины возникновения стандартных проблем со схемами элементов клона или связанного клона

Проблема	Причина	Решение
Отсутствуют компьютеры	Вы можете создавать схемы элементов связанного клона на компьютерах, которыми управляет администратор арендатора или диспетчер бизнес-групп.	<p>Пользователю в арендаторе или бизнес-группе нужно запросить компьютер vSphere. Если у вас есть соответствующие роли, вы можете сделать это самостоятельно.</p> <p>В этом диалоговом окне также отображаются неуправляемые компьютеры.</p> <p>Возможно, управляемые компьютеры импортированы.</p> <p>Компьютеры, подготовленные из vRealize Automation, не обязательно должны отображаться в этом диалоговом окне.</p>
Отсутствуют шаблоны	В данной конечной точке произошел сбой во время сбора данных, или на платформе компонента нет доступных конечных точек.	<ul style="list-style-type: none"> ■ При использовании кластерных конечных точек, содержащих несколько вычислительных ресурсов, убедитесь, что ваш администратор инфраструктуры как услуги добавил кластер, содержащий шаблоны, в группу структур. ■ Для новых шаблонов убедитесь, что ИТ-администратор разместил шаблоны в кластере, который входит в вашу группу структур.
Сбой подготовки для общей схемы элементов	Для схем элементов невозможно проверить, существует ли выбранный шаблон в резервировании, используемом для подготовки компьютера из общей схемы элементов клона.	Рекомендуется применять права, чтобы ограничить использование схем элементов пользователями, у которых есть резервирование в вычислительном ресурсе, в котором содержится шаблон.

Таблица 3-29. Причины возникновения стандартных проблем со схемами элементов клона или связанного клона (продолжение)

Проблема	Причина	Решение
Сбой подготовки с гостевым агентом	Виртуальная машина может перезагрузиться сразу после завершения настройки гостевой операционной системы, но до завершения настройки рабочих элементов гостевого агента. Из-за этого может произойти сбой подготовки. Можно использовать настраиваемое свойство <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> , чтобы увеличить значение времени задержки.	Убедитесь, что вы добавили настраиваемое свойство <code>VirtualMachine.Admin.CustomizeGuestOSDelay</code> . Формат значения должен быть такой: ЧЧ:ММ:СС. Если значение не задано, то значение по умолчанию — это одна минута (00:01:00).
Подготовка схемы элементов клона или связанного клона завершается сбоем, поскольку не удастся найти шаблон, который лежит в основе клона	Невозможно подготовить компьютеры из схемы элементов, клонированной из несуществующего шаблона. vRealize Automation периодически выполняет сбор данных (по умолчанию — каждые 24 часа). Если шаблон удален, изменение отображается только после следующего сбора данных, поэтому схему элементов можно создать на основе несуществующего шаблона.	Переопределите схему элементов с помощью существующего шаблона, а затем запросите подготовку. В качестве меры предосторожности по возможности выполняйте сбор данных до определения схемы элементов клона или связанного клона.

Проектирование схем элементов с использованием параметров NSX

Если интеграция vRealize Automation настроена с NSX for vSphere или NSX-T, можно использовать компоненты сети, безопасности и подсистемы балансировки нагрузки, чтобы настроить схему элементов для подготовки компьютера.

В общую схему элементов можно также добавить следующие параметры сети и безопасности NSX.

- **Транспортная зона**
Содержит сети, используемые для развертывания подготовленных компьютеров.
- **Политика резервирования сети**
Управляет передачей данных по сети при развертывании подготовленных компьютеров.
- **Изоляция приложений**
Разрешает только внутренний трафик между компьютерами, которые используются при развертывании подготовленных компьютеров.

Дополнительные сведения по интеграции vRealize Automation и NSX см. в статье блога [vRA and NSX - Intro to Network and Security Automation \(vRA и NSX — введение в автоматизацию сетей и систем безопасности\)](#), а также в материалах для предварительного просмотра по серии курсов [Networking and Security with vRealize Automation and NSX \(Сеть и безопасность с vRealize Automation и NSX\)](#).

Параметры NSX применяются только к типам компонентов компьютеров vSphere.

Настройка страниц «Новая схема элементов» и «Свойства схемы элементов» в vRealize Automation с помощью NSX

Во время создания схемы элементов можно настроить параметры, которые будут применяться ко всей схеме элементов vRealize Automation, включая некоторые параметры NSX, с помощью страницы **Новая схема элементов**. После создания схемы элементов эти настройки можно изменить на странице **Свойства схемы элементов**.

Вкладка **Общие**

Параметры на вкладке «Общие» применяются к общей схеме элементов vRealize Automation.

Таблица 3-30. Настройки вкладки **Общие**

Параметр	Описание
Имя	Введите имя своей схемы элементов.
Идентификатор	Поле идентификатора заполняется автоматически на основе введенного имени. Сейчас это поле можно изменить, но после сохранения схемы элементов изменить его будет невозможно. Идентификаторы в пределах арендатора являются постоянными и уникальными. Идентификаторы можно использовать для программного взаимодействия со схемами элементов и создания привязок свойств.
Описание	Составьте сводку по схеме элементов, чтобы ею было удобно пользоваться другим разработчикам архитектуры. Это описание также отображается для пользователей в форме запроса.
Ограничение числа развертываний	Укажите максимальное число развертываний, которые можно создать при использовании этой схемы элементов для подготовки компьютеров.
Аренда (дн.): минимальное значение и максимальное значение	Введите минимальное и максимальное значения, чтобы пользователи могли выбрать продолжительность аренды в пределах заданного диапазона. Когда заканчивается период аренды, развертывание удаляется или архивируется. Если не указать минимальное или максимальное значение, аренда будет длиться бесконечно. Сведения об аренде компьютеров необходимо указать в схеме элементов vRealize Automation, а не в приложении исходной конечной точки. Если информация об аренде указана во внешнем приложении, она не распознается в vRealize Automation.
Хранение в архиве (дн.)	Развертывания можно не удалять сразу по истечении срока аренды, а задать период архивного хранения, чтобы временно сохранить их. Укажите 0, чтобы развертывание удалялось по истечении срока аренды. Период архивного хранения начинается в день истечения срока аренды. Когда заканчивается период архивного хранения, компьютер удаляется. Значение по умолчанию — 0.
Распространение обновлений на существующие развертывания	Расширенные диапазоны значений для ЦП, памяти или хранилища передаются в активные развертывания, подготовленные на основе схемы элементов. Новый диапазон должен включать в себя старый диапазон. Например, если исходное минимальное значение составляет 32, а максимальное — 128 (32, 128), расширенный диапазон (16, 128), (32, 256) или (2, 1000) может вступить в силу после перенастройки или горизонтального масштабирования, но для диапазона (33, 512) или (4, 64) это невозможно.

Вкладка **Параметры NSX**

Если были настроены параметры NSX, то при создании или редактировании схемы элементов можно указать зону транспорта NSX, политику резервирования сети и параметры изоляции приложений. Эти настройки доступны на вкладке **Параметры NSX** на страницах **Схема элементов** и **Свойства схемы элементов**.

Дополнительные сведения о приложении NSX см. в [документации по VMware NSX Data Center for vSphere VMware](#) или в [документации по VMware NSX-T Data Center](#).

Таблица 3-31. Настройки вкладки **Параметры NSX**

Параметр	Описание
Транспортная зона	<p>Выберите существующую транспортную зону NSX, содержащую одну или несколько сетей, которые могут использоваться в подготовленном развертывании компьютера.</p> <p>Транспортная зона определяет, какие кластеры могут охватывать сети. Если при инициализации компьютеров транспортная зона указана в резервировании и схеме элементов, значения транспортной зоны должны совпадать. Доступны только те транспортные зоны, которые применимы к текущему арендатору.</p> <p>Транспортная зона требуется для схем элементов, содержащих объекты сети и безопасности по требованию NSX for vSphere или NSX-T.</p> <p>Дополнительные сведения см. в разделе Применение транспортной зоны NSX к схеме элементов.</p> <p>Укажите транспортную зону, которая подходит для развертывания NSX for vSphere или NSX-T.</p>
Политика резервирования сети	<p>Для NSX for vSphere выберите политику резервирования сети, чтобы определить, где в развертывании следует разместить Edge или DLR.</p> <p>Когда решение vRealize Automation подготавливает компьютер с помощью сети NAT или маршрутизируемой сети, оно подготавливает маршрутизируемый шлюз в качестве сетевого маршрутизатора.</p> <p>Пограничный или маршрутизируемый шлюз — это управляющий компьютер, потребляющий вычислительные ресурсы. Он также управляет сетевыми коммуникациями между всеми компьютерами в развертывании.</p> <p>От резервирования, с помощью которого подготавливается пограничный или маршрутизируемый шлюз, зависит, какая внешняя сеть используется для NAT и виртуальных IP-адресов подсистемы балансировки нагрузки. Лучший способ — использовать отдельный кластер управления для компьютеров управления, например NSX Edge.</p> <p>Для NSX-T выберите политику резервирования сети, чтобы определить, где разместить логический маршрутизатор нулевого уровня в развертывании схемы элементов.</p> <p>Дополнительные сведения см. в разделе Применение политики резервирования сети NSX к схеме элементов.</p> <p>Укажите политику резервирования, которая подходит для развертывания NSX for vSphere или NSX-T. Кластеры, развернутые посредством схемы элементов, могут управляться NSX for vSphere или NSX-T.</p>
Изоляция приложений	<p>Установите флажок Изоляция приложения, чтобы использовать политику безопасности для изоляции приложений, настроенную в NSX for vSphere.</p> <p>Политика изоляции приложений применяется ко всем компонентам компьютеров vSphere в схеме элементов. Можно также добавить группы безопасности и теги, чтобы vRealize Orchestrator мог открыть изолированную сеть для создания дополнительных путей ввода и вывода при изоляции приложений.</p> <p>Дополнительные сведения см. в разделе Применение изоляции приложений NSX к схеме элементов.</p>

Вкладка **Свойства**

Настраиваемые свойства, добавленные на уровне схемы элементов, применяются ко всей схеме элементов, в том числе ко всем компонентам. Информацию о порядке приоритетов настраиваемых свойств см. в разделе *Справочник по настраиваемым свойствам*.

Таблица 3-32. Настройки вкладки **Свойства**

Вкладка	Параметр	Описание
Группы свойств	Группы свойств	Группы свойств — это многозначные группы свойств, которые упрощают процесс добавления настраиваемых свойств в схемы элементов.
	Добавить	<p>Добавьте одну существующую группу свойств или несколько и примените их к общей схеме элементов.</p> <p>Предоставляются следующие группы свойств, связанных с контейнерами.</p> <ul style="list-style-type: none"> ■ Свойства узла контейнера с проверкой подлинности при помощи сертификата ■ Свойства узла контейнера с проверкой подлинности при помощи имени пользователя и пароля
	Вверх /Вниз	Управление приоритетностью каждой группы свойств относительно других групп. Первая группа в списке имеет наивысший приоритет, а ее настраиваемые свойства наиболее приоритетны. Для изменения порядка можно перемещать ползунок.
	Просмотр свойств	Просмотр настраиваемых свойств в выбранной группе свойств.
	Просмотр объединенных свойств	Если настраиваемое свойство входит в несколько групп свойств, более высокий приоритет имеет значение, которое входит в группу свойств с наивысшим приоритетом.
Настраиваемые свойства	Вместо групп свойств можно добавить отдельные настраиваемые свойства.	
	Создать	Добавьте отдельное настраиваемое свойство и примените его к общей схеме элементов.
	Имя	Введите имя свойства. Список настраиваемых свойств и их определения см. в разделе <i>Справочник по настраиваемым свойствам</i> .
	Значение	Введите значение настраиваемого свойства.
	Зашифровано	Шифрование значения свойства, например в случае, когда это значение является паролем.

Таблица 3-32. Настройки вкладки **Свойства** (продолжение)

Вкладка	Параметр	Описание
	Допускает переопределение	Пользователь схемы элементов может переопределить значение свойства. Если выбран параметр Показывать в запросе , пользователи смогут просматривать и изменять значения свойств при запросе элементов каталога.
	Показывать в запросе	Имя и значение этого свойства будут видны пользователям в форме запроса на подготовку. Чтобы разрешить пользователям самостоятельно вводить значения, выберите Допускает переопределение .

Применение транспортной зоны NSX к схеме элементов

Администратор NSX может создавать транспортные зоны для контроля кластерного использования сетей.

Транспортная зона управляет тем, какие узлы может достигать логический коммутатор. Она может охватывать один или несколько кластеров узлов, включая узлы в нескольких экземплярах vCenter.

Для схем элементов, содержащих сеть NAT по требованию или маршрутизируемую сеть по требованию, необходимо указать транспортную зону, содержащую сети, которые будут использоваться при развертывании подготовленных компьютеров.

Для схем элементов, которые включают конечную точку NSX-T, необходимо указать транспортную зону.

Транспортная зона, указанная для схемы элементов, должна совпадать с транспортной зоной, указанной для резервирования, используемого в схеме элементов. См. раздел [Применение политики резервирования сети NSX к схеме элементов](#).

- Если в схеме элементов не используются компоненты NSX-T по требованию, значение транспортной зоны игнорируется.
- NSX-T поддерживает несколько транспортных зон с наложением и несколько транспортных зон VLAN.
- Для создания логического коммутатора требуется транспортная зона. Логические коммутаторы создаются в транспортных зонах.
- При создании схемы элементов предоставляются только транспортные зоны для текущего арендатора. Предоставляются только транспортные зоны, которые используются в резервировании в текущем арендаторе.

Применение политики резервирования сети NSX к схеме элементов

При подготовке схемы элементов политика резервирования используется для группировки резервирований, которые можно учесть для развертывания. Сетевые сведения содержатся в каждом резервировании.

Если в этой политике резервирования есть транспортная зона, она должна соответствовать транспортной зоне, указанной в схеме элементов. См. раздел [Применение транспортной зоны NSX к схеме элементов](#).

Чтобы применить политику резервирования на уровне схемы элементов, воспользуйтесь страницами

Новая схема элементов или **Свойства схемы элементов**.

Факторы, касающиеся NSX for vSphere

Для NSX for vSphere эта политика резервирования позволяет определить размещение Edge NSX или выбор логического распределенного маршрутизатора (DLR), связанного с сетями по требованию. Это также называется политикой резервирования маршрутизированных шлюзов или политикой пограничного резервирования.

Например, для NSX for vSphere профиль сети NAT и подсистема балансировки нагрузки позволяют vRealize Automation развернуть шлюз служб Edge NSX. В профиле маршрутизируемой сети используется логический распределенный маршрутизатор (DLR) NSX for vSphere. Маршрутизатор DLR следует создать в NSX до использования в vRealize Automation. В vRealize Automation нельзя создавать маршрутизаторы DLR. После сбора данных в vRealize Automation можно использовать DLR для подготовки виртуальных машин.

Edge NSX предоставляет службы маршрутизации и обеспечивает подключение к сетям, которые являются внешними по отношению к развертыванию NSX. Шлюз Edge NSX соединяет изолированные подсети с общими сетями (исходящей связи), предоставляя стандартные службы шлюзов, такие как NAT и динамическая маршрутизация. Общие развертывания Edge NSX включают среды с несколькими арендаторами, где Edge NSX создает виртуальные границы для каждого арендатора.

vRealize Automation подготавливает маршрутизируемый шлюз, например шлюз служб Edge, для сетей NAT и подсистем балансировки нагрузки. Для маршрутизируемых сетей vRealize Automation использует существующие распределенные маршрутизаторы.

Резервирование, с помощью которого подготавливается пограничный или маршрутизируемый шлюз, определяет доступные профили сети NAT, частной сети и маршрутизируемой сети, а также виртуальные IP-адреса подсистемы балансировки нагрузки.

Факторы, касающиеся NSX-T

Для NSX-T эта политика резервирования помогает выбрать логический маршрутизатор нулевого уровня, используемый для развертывания.

Логические маршрутизаторы нулевого уровня имеют порты нисходящей связи для подключения к логическим маршрутизаторам уровня 1 и порты исходящей связи для подключения к внешним сетям. vRA подключает логический маршрутизатор уровня 1 к логическому маршрутизатору уровня 0 для организации доступа к вышестоящему маршрутизатору и назначает пограничный кластер какому-либо логическому маршрутизатору для выполнения функций NAT и запуска служб балансировки нагрузки.

Применение изоляции приложений NSX к схеме элементов

Можно включить изоляцию приложений, чтобы разрешить внутренний трафик между компонентами, подготовленными схемой элементов.

Политика изоляции приложения NSX действует как брандмауэр для блокировки всего входящего и исходящего трафика, идущего к подготовленным компьютерам развертывания и исходящего от них. Если указать определенную политику изоляции приложения NSX, компьютеры, подготовленные схемой элементов, смогут обмениваться данными между собой, но не смогут устанавливать подключение за пределами брандмауэра.

Если задано правило изоляции приложений, а правила безопасности заданы с использованием групп безопасности в схеме элементов, параметр изоляции приложений является последним правилом, обрабатываемым во время развертывания схемы элементов.

Чтобы применить изоляцию приложений на уровне схемы элементов, воспользуйтесь страницами **Новая схема элементов** или **Свойства схемы элементов**.

Факторы, касающиеся NSX for vSphere

Подготовленные компоненты размещаются в группе безопасности, которая изолируется с помощью правил брандмауэра. Для регистрации требуется, чтобы в конечной точке vSphere была настроена поддержка изоляции приложений NSX.

При использовании политики изоляции приложений NSX for vSphere разрешен только внутренний трафик между компьютерами, подготовленными на основе схемы элементов. Когда запрашивается подготовка, для компьютеров создается группа безопасности. Политика изоляции приложений создается в NSX for vSphere и применяется к группе безопасности. Правила брандмауэра определяются в политике безопасности для допуска только внутреннего трафика между компонентами в развертывании.

Когда подготовка выполняется с помощью схемы элементов, которая использует подсистему балансировки нагрузки NSX for vSphere Edge и политику безопасности изоляции приложения NSX for vSphere, динамически подготовленная подсистема балансировки нагрузки не добавляется в группу безопасности. Таким образом предотвращается обмен данными между подсистемой балансировки нагрузки и компьютерами, для которых эта подсистема должна обрабатывать подключения. Так как устройства Edge исключены из распределенного брандмауэра NSX for vSphere, их нельзя добавлять в группы безопасности. Чтобы балансировка нагрузки функционировала надлежащим образом, воспользуйтесь другой группой безопасности или другой политикой безопасности, которая впускает нужный трафик в виртуальные машины компонента для балансировки нагрузки.

Политика изоляции приложений имеет менее высокий приоритет по сравнению с другими политиками безопасности в NSX for vSphere. Например, если в подготовленном развертывании содержатся компьютер веб-компонента и компьютер компонента приложений, и на компьютере веб-компонента размещена веб-служба, то служба должна пропускать входящий трафик через порты 80 и 443. В этом случае пользователи должны создать политику веб-безопасности в NSX for vSphere. Правила брандмауэра в этой политике должны разрешать входящий трафик через эти порты. В vRealize Automation пользователи должны применять политику веб-безопасности в веб-компоненте подготовленного развертывания компьютера.

Примечание Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Если компьютеру веб-компонента нужен доступ к компьютеру компонента приложений, использующему подсистему балансировки нагрузки на портах 8080 и 8443, то политика веб-безопасности, кроме существующих правил брандмауэра, пропускающих входящий трафик через порты 80 и 443, должна включать в себя правила брандмауэра, пропускающие исходящий трафик через порты 8080 и 8443.

Факторы, касающиеся NSX-T

Подготовленные компоненты размещаются в группе NS Group, которая изолируется с помощью правил брандмауэра. Для регистрации требуется, чтобы в конечной точке vSphere была настроена поддержка изоляции приложений NSX.

NSX-T поддерживает создание двухуровневой топологии логического маршрутизатора: логический маршрутизатор верхнего (нулевого) уровня и логический маршрутизатор нижнего (первого) уровня. Эта структура дает администраторам поставщика и арендатора полный контроль над их службами и политиками. В NSX-T администраторы управляют и настраивают маршрутизацию и службы на нулевом уровне, а администраторы арендаторов — на первом.

Настройка параметров компонентов сети и безопасности в vRealize Automation

vRealize Automation поддерживает виртуализированные сети на основе платформы NSX. Также поддерживаются интегрированные сети Контейнеры для vRealize Automation.

Для интеграции сети и системы безопасности NSX с vRealize Automation администратору инфраструктуры как услуги необходимо настроить vSphere и конечные точки NSX. vRealize Automation поддерживает NSX for vSphere и NSX-T.

Сведения о внешних приготовлениях см. в разделе *Настройка vRealize Automation*.

Вы можете создать профили сети, в которых будут заданы параметры сети для резервирования и схемы элементов. Профили внешней сети определяют существующие физические сети. NAT по требованию и профили маршрутизируемой сети могут создать логические коммутаторы NSX и соответствующие параметры маршрутизации для нового сетевого пути.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

Если профиль сети указан в резервировании и схеме элементов, то значения в схеме элементов имеет более высокий приоритет.

В зависимости от вычислительного ресурса можно выбрать транспортную зону, которая определяет конечную точку vSphere. Транспортная зона определяет, какие узлы и кластеры можно связать с логическими коммутаторами, созданными в рамках зоны. Транспортная зона может включать в себя несколько кластеров vSphere. Для схемы элементов и резервирований, используемых при подготовке, нужно задать один и тот же параметр транспортной зоны. Транспортные зоны задаются в средах NSX.

Для настройки параметров безопасности можно указать сведения в резервировании, схеме элементов или сценарии гостевого агента. Если для компьютеров требуется гостевой агент, добавьте правило безопасности в резервирование или в схему элементов.

В схему элементов можно также добавить компонент сети Containers.

Дополнительные сведения о настройке сети и безопасности для NSX-T в vRealize Automation см. в статье блога VMware [Application Networking and Security with vRealize Automation and NSX-T](#).
Управление доступом к объектам безопасности из арендаторов в vRealize Automation
 Можно настроить доступность объектов безопасности NSX в vRealize Automation для нескольких арендаторов.

При создании объекта безопасности NSX для него по умолчанию задается либо глобальная доступность (доступность во всех арендаторах, для которых создано резервирование связанной конечной точки), либо статус «Скрыт» (Hidden) (для всех пользователей, кроме администратора).

Доступность объектов безопасности в различных арендаторах зависит от того, имеется ли у связанной конечной точки резервирование или политика резервирования в арендаторе.

NSX не разделяет группы безопасности по арендаторам. Тем не менее доступность групп безопасности в vRealize Automation можно контролировать с помощью настраиваемого свойства `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects`.

По умолчанию новые объекты безопасности доступны во всех арендаторах для связанных конечных точек NSX, в которых у вас есть резервирование. Если в выбранном арендаторе нет резервирований для данной конечной точки, объекты безопасности недоступны в выбранном арендаторе.

Если настраиваемое свойство `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` не установлено на конечных точках NSX, новые объекты безопасности по умолчанию доступны во всех арендаторах. Объекты безопасности, которые существовали до перехода на эту версию vRealize Automation, доступны во всех арендаторах независимо от настраиваемого свойства.

Примечание При обновлении до версии vRealize Automation группы безопасности из предыдущей версии становятся доступны во всех арендаторах по умолчанию. Существующие группы безопасности и теги безопасности доступны во всех арендаторах, в которых есть резервирование для связанной конечной точки.

Можно по умолчанию скрывать новые группы безопасности. Для этого нужно добавить настраиваемое свойство `VMware.Endpoint.NSX.HideDiscoveredSecurityObjects` для связанной конечной точки NSX. Этот параметр вступает в силу при следующем сборе данных конечной точки NSX и применяется только к новым объектам безопасности.

Кроме того, можно изменить доступность существующего объекта безопасности для арендаторов программными средствами. Например, если группа безопасности доступна для всех арендаторов, можно изменить доступность объекта безопасности для арендаторов с помощью параметра идентификатора арендатора связанной конечной точки NSX в REST API vRealize Automation или в vRealize CloudClient. Доступны следующие параметры идентификатора арендатора для конечной точки NSX.

- "<global>" — объект безопасности доступен во всех арендаторах. Это параметр по умолчанию, используемый для существующих объектов безопасности после обновления до этой версии, а также для всех создаваемых объектов безопасности.
- "<unscoped>" — объект безопасности недоступен ни для одного арендатора. Только системный администратор может получить доступ к такому объекту безопасности. Это идеальный параметр для объектов безопасности, которые планируется назначить определенному арендатору.
- "*tenant_id_name*" — объект безопасности доступен только в одном указанном арендаторе.

Средства REST API vRealize Automation или vRealize CloudClient можно использовать для назначения идентификаторов арендатора (*tenantId*) объектов безопасности, связанных с определенной конечной точкой, конкретному арендатору.

Сведения о командах vRealize Automation REST API см. в *справочнике по API-интерфейсу vRealize Automation* в разделе [Документация по API-интерфейсу vRealize Automation](#) для версии vRealize Automation 7.x. Дополнительные сведения см. в *руководстве по программированию vRealize Automation* в разделе [Документация по API-интерфейсу vRealize Automation](#) для версии vRealize Automation 7.x.

Сведения о vRealize CloudClient см. в разделе <https://code.vmware.com/web/dp/tool/cloudclient>. Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки

В зависимости от настроек сети и системы безопасности NSX-T и компонентов подсистем балансировки нагрузки в схеме элементов vRealize Automation можно настроить и использовать различные топологии развертывания.

Сеть и система безопасности

■ Маршрутизируемые сети

Если компонент маршрутизируемой сети NSX-T присоединить в схеме элементов к компоненту компьютера vSphere, то в NSX-T подготавливается следующая топология.

- Создается маршрутизатор первого уровня.
 - Создается логический коммутатор.
 - Маршрутизатор первого уровня подключается к логическому коммутатору с помощью нисходящего соединения.
 - На маршрутизаторе первого уровня объявляются определенные пути маршрутизации.
- Сети NAT (статический IP-адрес)

Если компонент сети NAT NSX-T подключается в схеме элементов к компоненту компьютера vSphere, то в NSX-T подготавливается следующая топология.

- Создается маршрутизатор первого уровня.
- Создается логический коммутатор.
- Маршрутизатор первого уровня подключается к кластеру периметра.
- Маршрутизатор первого уровня подключается к маршрутизатору нулевого уровня с помощью восходящего соединения. Маршрутизатор нулевого уровня выбирается из резервирования.
- Маршрутизатор первого уровня подключается к логическому коммутатору с помощью нисходящего соединения.
- На маршрутизаторе первого уровня объявляются определенные маршруты NAT.
- Для каждой сети NAT в профиле внешней сети выделяется один внешний IP-адрес, который поддерживает профиль сети NAT по требованию. Этот IP-адрес используется для правил SNAT и DNAT.
- Сети NAT (DHCP)

Если компонент NSX-T сети NAT с DHCP подключается в схеме элементов к компоненту компьютера vSphere, то в NSX-T подготавливается следующая топология.

- Создается маршрутизатор первого уровня.
- Создается логический коммутатор.
- Маршрутизатор первого уровня подключается к кластеру периметра.
- Маршрутизатор первого уровня подключается к маршрутизатору нулевого уровня с помощью восходящего соединения. Маршрутизатор нулевого уровня выбирается из резервирования.
- Маршрутизатор первого уровня подключается к логическому коммутатору с помощью нисходящего соединения.
- Подготавливается сервер DHCP с пулом IP-адресов.
- На маршрутизаторе первого уровня объявляются определенные маршруты NAT.
- Изоляция приложений

Если для схемы элементов с компонентами NSX-T требуется изоляции приложений, в NSX-T подготавливается следующая топология.

Примечание Настроить изоляции приложений для схемы элементов можно на странице свойств этой схемы элементов при ее создании или изменении.

- Создается группа NS.
- Создается раздел брандмауэра с правилами изоляции.
- Компьютеры данной схемы элементов добавляются в группы NS изоляции приложений с помощью тегов.

- Виртуальный IP-адрес подсистемы балансировки нагрузки и внешние IP-адреса для сетей NAT из данного набора IP-адресов добавляются в группу NS изоляции приложений.

Для поддержки групп NS изоляции приложений необходимо подключить эти компьютеры к непрозрачным сетям.

■ Существующие группы NS

Если компонент существующей группы NS подключается в схеме элементов к компоненту компьютера vSphere, то в NSX-T подготавливается следующая топология.

- Компьютеры, которые связаны с группой NS, добавляются в NSX-T в эту группу NS с использованием тегов как критериев членства.

Чтобы работать с существующими группами NS, необходимо подключить компьютеры к непрозрачным сетям.

Подсистемы балансировки нагрузки

Для подсистем балансировки нагрузки при развертывании схем элементов NSX-T поддерживаются следующие топологии.

- Одноканальная в сети NAT по требованию.
- Одноканальная в маршрутизируемой сети по требованию.
- Одноканальная во внешней (существующей) сети.
- Двухканальная (один канал в NAT, второй — во внешнюю сеть).
- Двухканальная (один канал в маршрутизируемую, второй — во внешнюю сеть).

Если в схему элементов добавляется подсистема балансировки нагрузки NSX-T, то в дополнение к указанным топологиям сети в развертывании подготавливается также следующая топология.

- Для всех топологий, за исключением тех, где подсистема балансировки нагрузки подключена к внешней сети по одному каналу, подготавливается следующее.
 - Создается одна служба балансировки нагрузки, даже если в схеме элементов указано несколько подсистем балансировки нагрузки.
 - Служба балансировки нагрузки подключается к маршрутизатору первого уровня данного развертывания. Маршрутизатор первого уровня создается по требованию.
- Для топологий, где подсистема балансировки нагрузки подключена к внешней сети по одному каналу, подготавливается следующее.
 - Внешняя сеть, которая указана в резервировании, должна быть непрозрачной сетью VC (логический коммутатор NSX-T).
 - Маршрутизатор первого уровня должен уже существовать и должен быть подключен к внешней сети (логический коммутатор NSX-T).
 - Если маршрутизатор первого уровня еще не существует, сервер балансировки нагрузки создается по требованию и подключается к маршрутизатору первого уровня. В противном случае используется уже существующая подсистема балансировки нагрузки.

- Объявляется маршрут к соответствующему виртуальному IP-адресу, за исключением случая, когда этот виртуальный IP-адрес принадлежит частной сети NAT.
- В службе балансировки нагрузки создаются один или несколько виртуальных серверов.
Размер подсистемы балансировки нагрузки ограничивает количество виртуальных серверов в одной такой службе.
- Для каждого виртуального сервера создается профиль приложения.
- Для каждого виртуального сервера, у которого настроены параметры сохранения устойчивости, создается профиль устойчивости.
- Настраивается пул членства, содержащий статический IP-адрес для каждого компьютера, входящего в этот пул.
- Создается одна служба балансировки нагрузки, даже если в схеме элементов указано несколько подсистем балансировки нагрузки.
- Для каждого участника пула создается и настраивается средство мониторинга работоспособности.

Для виртуальных серверов с поддержкой HTTPS в подсистемах балансировки нагрузки NSX-T, в отличие от подсистем балансировки нагрузки в NSX for vSphere, не поддерживается сквозной режим SSL. vRealize Automation настраивает виртуальный сервер балансировки нагрузки, который блокирует сквозное подключение SSL в своей подсистеме и для балансировки нагрузки участников своего пула использует обычный протокол HTTP. И имя сертификата, и имя профиля клиента SSL должны существовать в NSX-T. Их нужно указать при настройке HTTPS на виртуальном сервере. Сертификаты можно импортировать в диспетчер доверия NSX-T.

Если в схеме элементов указано более одного компонента NSX-T, то маршрутизатор первого уровня будет общим для всех компонентов и должен быть настроен соответствующим образом. Идентификатор внешнего маршрутизатора первого уровня отображается на странице развертываний vRealize Automation в представлении сведений для каждого из компонентов.

Использование компонентов сети NSX for vSphere в схеме элементов vRealize Automation

На холст проекта можно добавить один или несколько компонентов сети NSX for vSphere и настроить их параметры для компонентов компьютера vSphere в схеме элементов vRealize Automation.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere. Дополнительные сведения о настройке NSX for vSphere см. в *руководстве по администрированию NSX* в [документации по продукту NSX for vSphere](#).

Добавление компонента существующей сети NSX for vSphere

Компонент существующей сети NSX for vSphere можно добавить на холст проекта, чтобы связать его параметры с одним или несколькими компонентами компьютера vSphere в схеме элементов.

С помощью существующего компонента сети можно добавить сеть NSX for vSphere на холст проекта и настроить ее параметры, чтобы использовать ее с компонентами компьютеров vSphere и компонентами Программное обеспечение или Все как услуга, которые принадлежат к vSphere.

При связывании существующего сетевого компонента или сетевого компонента по требованию с компонентом компьютера сведения о сетевом адаптере сохраняются в компоненте компьютера. Указанные сведения о профиле сети хранятся в компоненте сети.

На холст проекта можно добавить несколько компонентов сети и безопасности.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

При создании схемы элементов доступны только те профили сети, которые применимы к текущему арендатору. В частности профили сети доступны в том случае, если в текущем арендаторе есть хотя бы одно резервирование, в котором данному профилю назначена хотя бы одна сеть.

Необходимые условия

- Создайте и настройте параметры сети для NSX. См. контрольный список конфигураций NSX в *Настройка vRealize Automation* и руководстве по администрированию NSX for vSphere в [документации по продукту NSX for vSphere](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Создайте профиль сети.
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Существующая сеть**.
3. Щелкните в текстовом поле **Существующая сеть** и выберите существующий профиль сети.
Значения в полях «Описание» (Description), «Маска подсети» (Subnet Mask) и «Шлюз» (Gateway) заполняются на основе параметров выбранного профиля сети.
4. (дополнительно) Перейдите на вкладку **DNS/WINS**.
5. (дополнительно) Укажите параметры DNS и WINS для профиля сети.
 - Основной сервер DNS
 - Дополнительный сервер DNS
 - Суффикс DNS
 - Предпочитаемая служба WINS
 - Альтернативная служба WINS

Для существующей сети параметры DNS или WINS изменять нельзя.

6. (дополнительно) Откройте вкладку Диапазоны IP-адресов.

Отобразится один или несколько диапазонов IP-адресов, указанных в профиле сети. Порядок сортировки и отображение столбцов можно изменить. Для сетей NAT также можно изменять значения диапазонов IP-адресов.

7. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите Сохранить или Готово.

Следующие шаги

Параметры сети можно добавить на вкладке **Сеть** компонента компьютера vSphere.

Добавление компонента частной сети для NSX for vSphere в vRealize Automation

Компонент частной сети NSX for vSphere можно добавить на холст проекта, чтобы связать его параметры с одним или несколькими компонентами компьютера vSphere в схеме элементов vRealize Automation.

При создании схемы элементов доступны только те профили сети, которые применимы к текущему арендатору.

Этот параметр частной сети доступен только для NSX for vSphere. Он недоступен для NSX-T.

Необходимые условия

- Создайте и настройте параметры сети для NSX. См. контрольный список конфигураций NSX в *Настройка vRealize Automation* и *руководстве по администрированию NSX for vSphere* в [документации по продукту NSX for vSphere](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Создайте профиль сети.
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент частной сети по требованию.
3. Чтобы добавить уникальную метку для компонента на холст проекта, введите имя компонента в текстовом поле **Идентификатор**.
4. Выберите существующий профиль сети в раскрывающемся меню **Профиль родительской сети**.
5. (дополнительно) В текстовом поле **Описание** введите описание компонента.

6. (дополнительно) Перейдите на вкладку **DNS/WINS**.
7. (дополнительно) Укажите параметры DNS и WINS для профиля сети.

- Основной сервер DNS
- Дополнительный сервер DNS
- Суффикс DNS
- Предпочитаемая служба WINS
- Альтернативная служба WINS

Для существующей сети параметры DNS или WINS изменять нельзя.

8. Откройте вкладку **Диапазоны IP-адресов**.

- а) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.
- б) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.

9. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Создание и использование правил NAT для NSX for vSphere

Правила NAT можно добавлять к сетевым компонентам NAT «один к многим» в схеме элементов, если сетевой компонент NAT связан с некластеризованным компонентом компьютера vSphere или с компонентом подсистемы балансировки нагрузки NSX for vSphere по требованию.

Можно определить правила NAT для любого совместимого с NSX for vSphere протокола. Можно сопоставить порт или диапазон портов от внешнего IP-адреса Edge до закрытого IP-адреса в сетевом компоненте NAT.

- Компонент компьютера vSphere

Можно создавать правила NAT для сетевых компонентов NAT «один к многим», которые связаны с некластеризованными компонентами компьютера vSphere.

Например, если два компьютера связаны с сетевым компонентом NAT «один к многим» в схеме элементов, можно определить правило NAT, которое позволит порту 443 на внешнем IP-адресе подключаться к компьютерам через порт 80 в сети NAT, используя протокол TCP.

- Компонент подсистемы балансировки нагрузки NSX for vSphere

Можно создавать правила NAT для сетевых компонентов NAT «один к многим», которые связаны с сетью виртуальных IP-адресов в компоненте подсистемы балансировки нагрузки NSX for vSphere.

Например, если сетевой компонент NAT связан с компонентом подсистемы балансировки нагрузки, который балансирует нагрузку трех компьютеров, можно задать правило NAT, позволяющее порту 90 на внешнем IP-адресе подключаться к виртуальному IP-адресу подсистемы балансировки нагрузки через порт 80 в сети NAT, используя протокол UDP.

Можно создать любое количество правил NAT и контролировать порядок, в котором они выполняются.

В правилах NAT не поддерживаются следующие элементы.

- Сетевые адаптеры, находящиеся не в текущей сети
- Сетевые адаптеры, настроенные на получение IP-адресов с использованием протокола DHCP
- Кластеры компьютеров

Сведения о добавлении правил NAT в компонент сети NAT в схеме элементов см. в разделе [Добавление компонента «Сеть NAT по требованию» или «Маршрутизируемая сеть по требованию» в vRealize Automation](#).

Дополнительные сведения об использовании правил NAT см. в общедоступных статьях, например в этой [записи блога vmwarelab](#).

Добавление компонента «Сеть NAT по требованию» или «Маршрутизируемая сеть по требованию» в vRealize Automation

Компонент NSX for vSphere «Сеть NAT по требованию» или компонент NSX for vSphere «Маршрутизируемая сеть по требованию» можно добавить на холст проекта при подготовке, чтобы связать их параметры с одним или несколькими компонентами компьютеров vSphere в схеме элементов vRealize Automation.

При связывании существующего сетевого компонента или сетевого компонента по требованию с компонентом компьютера сведения о сетевом адаптере сохраняются в компоненте компьютера. Указанные сведения о профиле сети хранятся в компоненте сети.

На холст проекта можно добавить несколько компонентов сети и безопасности.

В одной схеме элементов может быть несколько сетевых компонентов, предоставляемых по требованию. Однако все профили сети по требованию, используемые в схеме элементов, должны ссылаться на один и тот же внешний профиль сети.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

При создании схемы элементов доступны только те профили сети, которые применимы к текущему арендатору. В частности, профили сети доступны в том случае, если в текущем арендаторе есть хотя бы одно резервирование, в котором данному профилю назначена хотя бы одна сеть.

Необходимые условия

- Создайте и настройте параметры сети для NSX for vSphere. См. *Настройка vRealize Automation и NSX Руководство по администрированию* в [документации по продукту NSX for vSphere](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.

Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.

- Создайте профиль внешней сети по требованию. См. раздел [Создание профиля сети в vRealize Automation](#).

Например, сведения о добавлении сетевого компонента NAT по требованию см. в разделе [Создание профиля сети NAT для сети по требованию](#).

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.
- Чтобы задать правила NAT для сетевого компонента NAT, необходимо использовать профиль сети NAT «один ко многим». См. раздел [Создание профиля сети NAT с помощью указанной конечной точки управления IP-адресами](#) или [Создание профиля сети NAT в vRealize Automation с помощью сторонней конечной точки управления IP-адресами](#). Сведения о правилах NAT см. в разделе [Создание и использование правил NAT для NSX for vSphere](#).

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент «Сеть NAT по требованию» или «Маршрутизируемая сеть по требованию».
3. Чтобы добавить уникальную метку для компонента на холст проекта, введите имя компонента в текстовом поле **Идентификатор**.
4. Выберите советующий профиль сети в раскрывающемся меню **Профиль родительской сети**. Например, чтобы добавить сетевой компонент NAT, выберите профиль сети NAT, настроенный для поддержки выбранных параметров сети.

Чтобы задать правила NAT в сетевом компоненте NAT, необходимо использовать родительский профиль сети, настроенный для профиля сети NAT «один ко многим».

Следующие параметры сети заполняются с учетом выбранного типа профиля. В профиле сети нужно изменить следующие значения:

- Имя профиля внешней сети
 - Тип NAT («NAT по требованию»)
 - Маска подсети
 - Маска подсети диапазона («Направлено по маршруту по требованию»)
 - Маска подсети диапазона («Направлено по маршруту по требованию»)
 - Базовый IP-адрес («Направлено по маршруту по требованию»)
5. (дополнительно) В текстовом поле **Описание** введите описание компонента.
 6. (дополнительно) Перейдите на вкладку **DNS/WINS**.

7. (дополнительно) Укажите параметры DNS и WINS для профиля сети.

- Основной сервер DNS
- Дополнительный сервер DNS
- Суффикс DNS
- Предпочитаемая служба WINS
- Альтернативная служба WINS

Для существующей сети параметры DNS или WINS изменять нельзя.

8. Откройте вкладку Диапазоны IP-адресов.

Отобразится один или несколько диапазонов IP-адресов, указанных в профиле сети. Порядок сортировки и отображение столбцов можно изменить. Для сетей NAT также можно изменять значения диапазонов IP-адресов.

- а) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.
- б) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.

9. Если используется сеть NAT на основе профиля сети NAT «один ко многим», которая использует диапазоны статических IP-адресов, можно перейти на вкладку Правила NAT для добавления правил, разрешающих внешним IP-адресам доступ к компонентам внутренней сети NAT.

Для сети NAT «один ко многим» можно определить правила NAT, которые настраиваются при добавлении компонента сети NAT в схему элементов. Правило NAT можно изменить при редактировании сети NAT в развертывании.

Доступные для выбора варианты зависят от vSphere характеристик компьютера или компонентов NSX for vSphere подсистемы балансировки нагрузки, для которых настроена связь с сетевым компонентом NAT.

- **Имя** — укажите уникальное имя правила.
- **Компонент** — выберите в списке компьютер vSphere или компонент подсистемы балансировки нагрузки, для которого настроена связь с сетью NAT.

Правила NAT поддерживаются только для компьютеров, не входящих в кластеры. Если указано, что размер кластера больше 1, ни один из компонентов не будет отображаться, так как такая конфигурация не поддерживается.

- **Порт источника** — выберите ЛЮБОЙ вариант, укажите допустимый порт или диапазон портов либо укажите допустимую привязку свойства.
- **Порт назначения** — выберите ЛЮБОЙ вариант, укажите допустимый порт или диапазон портов либо укажите допустимую привязку свойства.
- **Протокол** — укажите любой допустимый протокол, поддерживаемый NSX for vSphere, или выберите TCP UDP либо ЛЮБОЙ параметр.
- **Описание** — введите краткое описание правила NAT.

- 10.** Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Следующие шаги

Параметры сети можно добавить на вкладке **Сеть** компонента компьютера vSphere.

Использование компонентов сети NSX-T в схеме элементов

На холст проекта можно добавить один или несколько компонентов сети NSX-T и настроить их параметры для компонентов компьютера vSphere в схеме элементов.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX-T. Дополнительные сведения о настройке NSX-T см. в *руководстве по администрированию NSX-T* в [документации по продукту NSX-T](#).

При развертывании схемы элементов, которая содержит конечную точку NSX-T, развертывание назначает тег компонентам NSX-T в развертывании. Имя тега совпадает с именем развертывания.

Дополнительные сведения о NSX-T конкретном развертывании и особенности топологии см. в разделе [Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Добавление компонента существующей сети NSX-T

Компонент существующей сети NSX-T можно добавить на холст проекта, чтобы связать его параметры с одним или несколькими компонентами компьютера vSphere в схеме элементов.

С помощью существующего компонента сети можно добавить сеть NSX-T на холст проекта и настроить ее параметры, чтобы использовать ее с компонентами компьютеров vSphere и компонентами Программное обеспечение или Все как услуга, которые принадлежат к vSphere.

При связывании существующего сетевого компонента или сетевого компонента по требованию с компонентом компьютера сведения о сетевом адаптере сохраняются в компоненте компьютера. Указанные сведения о профиле сети хранятся в компоненте сети.

На холст проекта можно добавить несколько компонентов сети и безопасности.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

При создании схемы элементов доступны только те профили сети, которые применимы к текущему арендатору. В частности, профили сети доступны в том случае, если в текущем арендаторе есть хотя бы одно резервирование, в котором данному профилю назначена хотя бы одна сеть.

Необходимые условия

- Создайте и настройте параметры сети для NSX-T. См. *Настройка vRealize Automation* и *NSX-T Руководство по администрированию* в [документации по продукту NSX-T](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.

Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.

- Создайте профиль сети.
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).

2. Перетащите на холст проекта компонент **Существующая сеть**.

3. Щелкните в текстовом поле **Существующая сеть** и выберите существующий профиль сети.

Значения в полях «Описание» (Description), «Маска подсети» (Subnet Mask) и «Шлюз» (Gateway) заполняются на основе параметров выбранного профиля сети.

4. (дополнительно) Перейдите на вкладку **DNS/WINS**.
5. (дополнительно) Укажите параметры DNS и WINS для профиля сети.

- Основной сервер DNS
- Дополнительный сервер DNS
- Суффикс DNS
- Предпочитаемая служба WINS
- Альтернативная служба WINS

Для существующей сети параметры DNS или WINS изменять нельзя.

6. (дополнительно) Откройте вкладку **Диапазоны IP-адресов**.

Отобразится один или несколько диапазонов IP-адресов, указанных в профиле сети. Порядок сортировки и отображение столбцов можно изменить. Для сетей NAT также можно изменять значения диапазонов IP-адресов.

7. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Следующие шаги

Параметры сети можно добавить на вкладке **Сеть** компонента компьютера vSphere.

Создание и использование правил NAT для NSX-T

Правила NAT можно добавлять к сетевым компонентам NAT «один к многим» в схеме элементов, если сетевой компонент NAT связан с компонентом компьютера vSphere, не входящим в кластер.

Можно определить правила NAT для любого совместимого с NSX-T протокола. Можно сопоставить порт или диапазон портов от внешнего IP-адреса Edge до закрытого IP-адреса в сетевом компоненте NAT.

Можно создавать правила NAT для сетевых компонентов NAT «один к многим», которые связаны с некластеризованными компонентами компьютера vSphere. Например, если два компьютера связаны в схеме элементов с сетевым компонентом NAT по схеме «один к многим», можно определить правило NAT, которое позволит порту 443 по внешнему IP-адресу подключаться к компьютерам через порт 80 в сети NAT, используя протокол TCP.

Правила NAT не поддерживаются для подсистем балансировки нагрузки NSX-T и для NSX-T версии 2.2.

Можно создать любое количество правил NAT и контролировать порядок, в котором они выполняются.

В правилах NAT не поддерживаются следующие элементы.

- Сетевые адаптеры, находящиеся не в текущей сети
- Сетевые адаптеры, настроенные на получение IP-адресов с использованием протокола DHCP
- Кластеры компьютеров

Сведения о добавлении правил NAT в компонент сети NAT в схеме элементов см. в разделе [Добавление компонента NSX-T «Сеть NAT по требованию» или компонента NSX-T «Маршрутизируемая сеть по требованию»](#).

Добавление компонента NSX-T «Сеть NAT по требованию» или компонента NSX-T «Маршрутизируемая сеть по требованию»

Компонент NSX-T «Сеть NAT по требованию» или NSX-T «Маршрутизируемая сеть по требованию» можно добавить на холст проекта при подготовке, чтобы связать их параметры с одним или несколькими компонентами компьютеров vSphere в схеме элементов.

При связывании существующего сетевого компонента или сетевого компонента по требованию с компонентом компьютера сведения о сетевом адаптере сохраняются в компоненте компьютера. Указанные сведения о профиле сети хранятся в компоненте сети.

На холст проекта можно добавить несколько компонентов сети и безопасности.

В одной схеме элементов может быть несколько сетевых компонентов, предоставляемых по требованию. Однако все профили сети по требованию, используемые в схеме элементов, должны ссылаться на один и тот же внешний профиль сети.

Для NSX-T диапазоны сети, которые в данной схеме элементов используются разными сетями, не должны перекрываться. Это ограничение применяется при настройке сетей маршрутизатора NSX-T уровня 1.

Для компонентов компьютеров vSphere со связанным компонентом NSX используйте настройку сети, безопасности и балансировки нагрузки в пользовательском интерфейсе. Для компонентов компьютеров, в которых нет вкладки **Сеть** или **Безопасность**, можно добавить настраиваемые свойства для сети и безопасности, например `VirtualMachine.Network0.Name`, на вкладку **Свойства** на холсте проекта. Свойства сети, безопасности и подсистемы балансировки нагрузки NSX применимы только к компьютерам vSphere.

При создании схемы элементов доступны только те профили сети, которые применимы к текущему арендатору. В частности, профили сети доступны в том случае, если в текущем арендаторе есть хотя бы одно резервирование, в котором данному профилю назначена хотя бы одна сеть.

Необходимые условия

- Создайте и настройте параметры сети для NSX for vSphere. См. *Настройка vRealize Automation и NSX for vSphere Руководство по администрированию* в [документации по продукту NSX-T](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Создайте профиль внешней сети по требованию. См. раздел [Создание профиля сети в vRealize Automation](#).
Например, сведения о добавлении сетевого компонента NAT по требованию см. в разделе [Создание профиля сети NAT для сети по требованию](#).
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.
- Чтобы задать правила NAT для сетевого компонента NAT, необходимо использовать профиль сети NAT «один ко многим». См. раздел [Создание профиля сети NAT с помощью указанной конечной точки управления IP-адресами](#) или [Создание профиля сети NAT в vRealize Automation с помощью сторонней конечной точки управления IP-адресами](#). Сведения о правилах NAT см. в разделе [Создание и использование правил NAT для NSX for vSphere](#).

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент NSX-T «Сеть NAT по требованию» или компонент NSX-T «Маршрутизируемая сеть по требованию».
3. Чтобы добавить уникальную метку для компонента на холст проекта, введите имя компонента в текстовом поле **Идентификатор**.
4. Выберите советуемый профиль сети в раскрывающемся меню **Профиль родительской сети**.
Например, чтобы добавить сетевой компонент NAT, выберите профиль сети NAT, настроенный для поддержки выбранных параметров сети.

Чтобы задать правила NAT в сетевом компоненте NAT, необходимо использовать родительский профиль сети, настроенный для профиля сети NAT «один ко многим».

Следующие параметры сети заполняются с учетом выбранного типа профиля. В профиле сети нужно изменить следующие значения:

- Имя профиля внешней сети
- Тип NAT (NSX-T «NAT по требованию»)
- Маска подсети
- Маска подсети диапазона (NSX-T «Маршрутизируемая сеть по требованию»)

- Маска подсети диапазона (NSX-T «Маршрутизируемая сеть по требованию»)
 - Базовый IP-адрес (NSX-T «Маршрутизируемая сеть по требованию»)
5. (дополнительно) В текстовом поле **Описание** введите описание компонента.
 6. (дополнительно) Перейдите на вкладку **DNS/WINS**.
 7. (дополнительно) Укажите параметры DNS и WINS для профиля сети.

- Основной сервер DNS
- Дополнительный сервер DNS
- Суффикс DNS
- Предпочитаемая служба WINS
- Альтернативная служба WINS

Для существующей сети параметры DNS или WINS изменять нельзя.

8. Откройте вкладку **Диапазоны IP-адресов**.

Отобразится один или несколько диапазонов IP-адресов, указанных в профиле сети. Порядок сортировки и отображение столбцов можно изменить. Для сетей NAT также можно изменять значения диапазонов IP-адресов.

- а) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.
- б) Введите значение начального IP-адреса в текстовом поле **Начало диапазона IP-адресов**.

9. Если используется сеть NAT на основе профиля сети NAT «один ко многим», которая использует диапазоны статических IP-адресов, можно перейти на вкладку **Правила NAT** для добавления правил, разрешающих внешним IP-адресам доступ к компонентам внутренней сети NAT.

Для сети NAT «один ко многим» можно определить правила NAT, которые настраиваются при добавлении компонента сети NAT в схему элементов. Правило NAT можно изменить при редактировании сети NAT в развертывании.

Доступные для выбора варианты зависят от компонентов компьютера vSphere, для которых настроена связь с данным сетевым компонентом NAT.

- **Имя** — укажите уникальное имя правила.
- **Компонент** — выберите в списке компьютер vSphere или компонент подсистемы балансировки нагрузки, для которого настроена связь с сетью NAT.

Правила NAT поддерживаются только для компьютеров, не входящих в кластеры. При указании размера кластера больше 1 ни один из компонентов не отображается, так как такая конфигурация не поддерживается.

- **Порт источника** — выберите ЛЮБОЙ вариант, укажите допустимый порт или диапазон портов либо укажите допустимую привязку свойства.
- **Порт назначения** — выберите ЛЮБОЙ вариант, укажите допустимый порт или диапазон портов либо укажите допустимую привязку свойства.

- **Протокол** — укажите любой допустимый протокол, поддерживаемый NSX-T, или выберите TCP UDP либо ЛЮБОЙ параметр.
- **Описание** — укажите краткое описание функций правила NAT.

10. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Следующие шаги

Параметры сети можно добавить на вкладке **Сеть** компонента компьютера vSphere.

Использование компонентов подсистемы балансировки нагрузки NSX for vSphere в схеме элементов

Чтобы настроить параметры компонентов компьютера vSphere в схеме элементов, на холст проекта можно добавить один или несколько компонентов подсистемы балансировки нагрузки NSX for vSphere по требованию.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

К пулам подсистем балансировки нагрузки и параметрам сети виртуальных IP-адресов в схеме элементов применяются следующие правила.

- При использовании профиля сети пула NAT профиль сети виртуальных IP-адресов может быть частью профиля сети NAT.
- При использовании маршрутизируемого профиля сети пула профиль сети виртуальных IP-адресов может быть только в такой же маршрутизируемой сети.
- При использовании внешнего профиля сети пула профиль сети виртуальных IP-адресов может быть только таким же профилем внешней сети.

Для каждого из компонентов «Подсистема балансировки нагрузки» могут использоваться несколько виртуальных серверов, которые также называются службами подсистемы балансировки нагрузки. На каждом из виртуальных серверов в компоненте «Подсистема балансировки нагрузки» может использоваться один порт и протокол. Например, можно применить балансировку нагрузки к службе HTTP или службе HTTPS. Подсистема балансировки нагрузки может применять балансировку к нескольким службам.

NSX Edge — это сетевое устройство, в котором содержатся виртуальные серверы подсистемы балансировки нагрузки. Поскольку в одной схеме элементов может быть больше одного компонента подсистемы балансировки нагрузки, при подготовке развертывания виртуальные серверы, определенные для каждого компонента подсистемы балансировки нагрузки, содержатся в одном устройстве NSX Edge.

Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Можно перенастроить параметры подсистемы балансировки нагрузки в существующем развертывании, чтобы добавить, изменить или удалить виртуальные серверы.

Факторы, которые необходимо учитывать при работе с обновленными или перенесенными компонентами подсистемы балансировки нагрузки

При работе с компонентами подсистемы балансировки нагрузки NSX в целевом выпуске vRealize Automation важно понять следующие факторы и действовать соответствующим образом.

Данная информация относится к компонентам подсистемы балансировки нагрузки NSX for vSphere, которые были обновлены или перенесены в этот выпуск vRealize Automation.

- До и после обновления или переноса в этот выпуск необходимо запустить сбор данных по инвентаризации сети и системы безопасности NSX, чтобы предотвратить проблемы при выполнении действия «Перенастройка подсистемы балансировки нагрузки». Это не касается действия «Перенастройка подсистемы балансировки нагрузки» для новых развертываний.

Дополнительные сведения см. здесь: *Обновление версии vRealize Automation 7.1 и более поздних версий и Перенос vRealize Automation*.

- Вы можете изменить подсистему балансировки нагрузки. Требуется право «Перенастройка (подсистема балансировки нагрузки)» для каталога.
- В случае развертываний, которые были обновлены или перенесены из vRealize Automation 7.x в этот выпуск vRealize Automation, перенастройка выполняется только для развертываний, содержащих одну подсистему балансировки нагрузки.
- Операция «Перенастройка подсистемы балансировки нагрузки» не поддерживается для развертываний, которые были обновлены или перенесены из vRealize Automation 6.2.x в этот выпуск vRealize Automation.

Добавление компонента «Подсистема балансировки нагрузки по требованию»

Можно перетащить компонент подсистемы балансировки нагрузки NSX по требованию на холст проекта и настроить его параметры для использования с компонентами компьютеров vSphere и компонентами контейнеров в схеме элементов.

Дополнительные сведения о создании профилей приложений NSX for vSphere для определения особенностей передачи конкретного типа сетевого трафика см. в *руководстве по администрированию NSX* в [документации по продукту NSX for vSphere](#).

Процедура

1. Определение параметров участника подсистемы балансировки нагрузки

Можно определить компонент подсистемы балансировки нагрузки NSX по требованию, чтобы распределить обработку задач между подготовленными компьютерами участников или компьютерами контейнеров vSphere в сети.

2. Определение общих параметров виртуального сервера

Можно определить один протокол и порт виртуального сервера для подсистемы балансировки нагрузки или можно добавить дополнительные виртуальные серверы, чтобы настроить дополнительные компоненты подсистемы балансировки нагрузки NSX.

3. Определение параметров распределения виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать сведения об участниках пула — например, порт, через который участникам поступает трафик, тип протокола, который подсистема балансировки NSX может использовать для обращения к этому порту, алгоритм, используемый для балансировки нагрузки, а также параметры сохранения устойчивости.

4. Определение параметров проверки работоспособности виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать, должна ли подсистема балансировки нагрузки NSX проверять работоспособность участников пула на виртуальном сервере и как это следует делать.

5. Определение дополнительных параметров виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно настроить компонент подсистемы балансировки нагрузки NSX и указать такие параметры, как количество одновременных подключений, которые может распознать один участник пула, и максимальное количество одновременных подключений, которые может обработать виртуальный сервер.

6. Определение параметров ведения журнала подсистемы балансировки нагрузки

Можно определить типы действий по ведению журнала подсистемы балансировки нагрузки, которые записываются в ее журналах.

Определение параметров участника подсистемы балансировки нагрузки

Можно определить компонент подсистемы балансировки нагрузки NSX по требованию, чтобы распределить обработку задач между подготовленными компьютерами участников или компьютерами контейнеров vSphere в сети.

При добавлении компонента подсистемы балансировки нагрузки в схему элементов на холсте проекта, можно выбрать индивидуальный вариант или вариант по умолчанию при создании или изменении определений виртуального сервера в компоненте подсистемы балансировки нагрузки. Вариант по умолчанию позволяет выбрать протокол, порт и описание виртуального сервера и использовать значения по умолчанию для всех остальных параметров. Вариант индивидуальной настройки позволяет определить дополнительные уровни детализации.

Если подсистема балансировки нагрузки подготовлена с помощью внешней сети, виртуальный IP-адрес (сеть виртуальных IP-адресов) и пул участников (сеть участников) должны находиться в одной существующей сети. Если виртуальный IP-адрес и пул участников находятся в разных внешних сетях, при попытке подготовки произойдет ошибка.

Необходимые условия

- Создайте и настройте параметры подсистемы балансировки нагрузки для NSX. См. *Настройка vRealize Automation* и *руководство по администрированию NSX*.
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Создайте профиль сети.
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.
- Убедитесь, что как минимум один компонент компьютера vSphere или компонент контейнера существует в схеме элементов.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Подсистема балансировки нагрузки по требованию**.
3. Чтобы добавить уникальную метку для компонента на холст проекта, введите имя компонента в текстовом поле **Идентификатор**.
4. Выберите имя компонента компьютера vSphere или компонента контейнера из раскрывающегося меню **Участник**.
Это список содержит только компоненты компьютера vSphere и компоненты контейнера в активной схеме элементов.
5. В раскрывающемся меню **Сеть участников** выберите сетевой адаптер для балансировки нагрузки.
Список содержит сетевые адаптеры, которые определены для выбранного участника-компьютера vSphere.

6. Выберите доступную сеть виртуальных IP-адресов в раскрывающемся меню **Сеть виртуальных IP-адресов**. Например, выберите доступную внешнюю сеть или сеть NAT.

В схеме элементов может быть несколько подсистем балансировки нагрузки NSX и компонентов сети по требованию NSX, но все они должны быть связаны с одной сетью виртуальных IP-адресов.

7. (дополнительно) В текстовом поле **IP-адрес** укажите допустимый IP-адрес для сетевого адаптера.

По умолчанию это статический IP-адрес, который связан с сетью виртуальных VIP-адресов. Однако можно указать другой IP-адрес или диапазон IP-адресов. По умолчанию следующий доступный IP-адрес выделяется из связанной сети виртуальных IP-адресов.

Оставьте поле IP-адреса пустым, чтобы во время подготовки такой адрес мог быть выделен из связанной сети виртуальных IP-адресов.

Если указать IP-адрес для любого типа сети, то можно будет подготовить только одно развертывание. При последующих развертываниях произойдет ошибка выделения IP-адресов, так как данный IP-адрес уже будет использоваться первым развертыванием.

8. Чтобы создать определение виртуального сервера, нажмите кнопку **Создать** и ознакомьтесь с разделом [Определение общих параметров виртуального сервера](#).

Для каждого компонента подсистемы балансировки нагрузки требуется хотя бы один виртуальный сервер.

Чтобы указать варианты ведения журнала, см. раздел [Определение параметров ведения журнала подсистемы балансировки нагрузки](#).

Определение общих параметров виртуального сервера

Можно определить один протокол и порт виртуального сервера для подсистемы балансировки нагрузки или можно добавить дополнительные виртуальные серверы, чтобы настроить дополнительные компоненты подсистемы балансировки нагрузки NSX.

Например, можно настроить компонент подсистемы балансировки нагрузки, чтобы определить такие параметры, как протокол и порт проверки работоспособности, алгоритм, сохранение устойчивости и прозрачность.

Необходимые условия

[Определение параметров участника подсистемы балансировки нагрузки](#).

Процедура

1. Откройте вкладку **Общие** на странице **Новый виртуальный сервер**.
2. Выберите протокол сетевого трафика, который следует использовать для балансировки нагрузки виртуального сервера, в раскрывающемся меню **Протокол**.

Варианты протокола: HTTP, HTTPS, TCP и UDP.

3. В текстовом поле **Порт** введите значение порта.

Выбранный протокол определяет порт по умолчанию.

Протокол	Порт по умолчанию
HTTP	80
HTTPS	443
TCP	8080
UDP	нет по умолчанию

Для протоколов HTTP, HTTPS и TCP можно задать общий порт с UDP. Например, если служба 1 использует TCP, HTTP или HTTPS на порте 80, служба 2 может использовать UDP на том же порте. Если служба 1 использует UDP на порте 80, служба 2 не может использовать UDP на том же порте.

4. (дополнительно) Введите описание компонента виртуального сервера.

5. Выберите один из вариантов в меню **Параметры**.

■ **Использовать значение по умолчанию для всех других параметров**

Примите все другие параметры по умолчанию. Нажмите кнопку **ОК**, чтобы завершить определение компонента подсистемы балансировки нагрузки и продолжить работу в схеме элементов.

Щелкнув пункт **Индивидуальная настройка**, можно отобразить значения по умолчанию и изучить дополнительные параметры на вкладке. Если значения параметров по умолчанию имеют подходят, щелкните **Использовать значение по умолчанию для всех других параметров** на вкладке **Общие**.

■ **Индивидуальная настройка**

Настройте компонент подсистемы балансировки нагрузки с дополнительными параметрами, например, чтобы определить другой протокол для отслеживания работоспособности или другой порт для отслеживания трафика участников.

Появятся дополнительные вкладки, которые позволят вам добавить индивидуальные параметры.

После выбора пункта **Использовать значение по умолчанию для всех других параметров** и нажатия кнопка **ОК**, вы закончили и можете продолжать определять или изменять схему элементов на холсте проекта. Если выбран пункт **Индивидуальная настройка**, продолжайте выполнять действия до данного этапа.

6. Щелкните вкладку **Распределение** и перейдите к разделу [Определение параметров распределения виртуального сервера](#), чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX.

Определение параметров распределения виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать сведения об участниках пула — например, порт, через который участникам поступает трафик, тип протокола, который подсистема балансировки NSX может использовать для обращения к этому порту, алгоритм, используемый для балансировки нагрузки, а также параметры сохранения устойчивости.

Пул представляет собой кластер компьютеров с балансировкой нагрузки. Участник пула — это отдельный компьютер в данном кластере.

Параметры протокола и порта участника по умолчанию соответствуют параметрам протокола и порта на странице **Общие**.

Пул компьютеров-участников отображается в значении параметра **Участник** в пользовательском интерфейсе компонента подсистемы балансировки нагрузки схемы элементов. Запись **Участник** указывает пул или кластер компьютеров.

Необходимые условия

Определение общих параметров виртуального сервера.

Процедура

1. (дополнительно) Параметр **Протокол участника** соответствует протоколу, определенному на вкладке **Общие**. Этот параметр определяет, как участник пула должен получать сетевой трафик.
2. (дополнительно) Введите номер порта в текстовом поле **Порт участника**, чтобы указать порт, по которому участник пула должен получать сетевой трафик.

Например, если входящий запрос на виртуальный IP-адрес (VIP) подсистемы балансировки нагрузки приходит на порт 80, возможно, понадобится направить этот запрос на другой порт (например, порт 8080) для участников пула.

3. (дополнительно) Выберите алгоритм метода балансировки для этого пула.

Варианты алгоритма и его параметры для вариантов, которым они требуются, описаны в таблице ниже.

Параметр	Описание и параметры алгоритма
ROUND_ROBIN	<p>Каждый сервер используется по очереди в соответствии назначенным ему с весом. Если подсистема балансировки нагрузки была создана в vRealize Automation, у всех участников одинаковый вес.</p> <p>Это самый уравновешенный и самый справедливый алгоритм, в котором время обработки сервера остается равно распределенным.</p> <p>Параметры алгоритма деактивированы для этого варианта.</p>
IP-HASH	<p>Выбирает сервер на основании хэша исходного IP-адреса и общего веса всех работающих серверов.</p> <p>Параметры алгоритма деактивированы для этого варианта.</p>
LEASTCONN	<p>Распределяет запросы клиентов по нескольким серверам на основании количества подключений к серверу, которые уже существуют.</p> <p>Новые подключения отправляются на сервер, к которому меньше всего подключений.</p> <p>Параметры алгоритма деактивированы для этого варианта.</p>

Параметр	Описание и параметры алгоритма
URI	<p>Левая часть URI (перед знаком вопроса) хэшируется и делится на общий вес работающих серверов.</p> <p>Результат этого действия определяет, какой сервер получает запрос. Благодаря этому URI всегда направляется к одному и тому же серверу, пока количество работающих серверов остается неизменным.</p> <p>Этот параметр алгоритма URI имеет два компонента: <code>uriLength=<len></code> и <code>uriDepth=<dep></code>. Введите параметры длины и глубины в отдельных строках в текстовом поле Параметры алгоритма.</p> <p>Параметры длины и глубины должны быть положительными целыми числами. Эти компоненты могут выполнять балансировку серверов, основываясь только на первой части URI.</p> <p>Параметр длины указывает, что алгоритм должен принимать во внимание только определенные символы в начале URI для вычисления хэша. Диапазон параметра длины должен составлять $1 \leq \text{len} < 256$.</p> <p>Параметр глубины определяет максимальную глубину каталога, который следует использовать для вычисления хэша. С каждой косой чертой в запросе добавляется один уровень. Диапазон параметра глубины должен составлять $1 \leq \text{len} < 10$.</p> <p>Если определены оба параметра, проверка прекращается, когда один из параметров достигается.</p>
HTTPHEADER	<p>Имя заголовка HTTP проверяется в каждом запросе HTTP.</p> <p>В имени заголовка в круглых скобках не учитывается регистр, что похоже на функцию ACL <code>'hdr()'</code>.</p> <p>Параметр алгоритма HTTPHEADER имеет один компонент <code>headerName=<name></code>. Например, можно использовать host как параметр алгоритма HTTPHEADER.</p> <p>Если заголовок отсутствует или не содержит никакого значения, применяется алгоритм циклического перебора.</p>
URL-адрес	<p>Поиск параметра URL-адреса, указанного в аргументе, выполняется в строке запроса для каждого запроса HTTP GET.</p> <p>Этот параметр алгоритма URL-адреса имеет один компонент <code>urlParam=<url></code>.</p> <p>Если за параметром следует знак равенства (=) и значение, это значение хэшируется и делится на общий вес работающих серверов. Результат этого действия определяет, какой сервер получает запрос. Этот процесс используется для отслеживания идентификаторов пользователей в запросах, благодаря чему один и тот же ИД пользователя всегда отправляется на один и тот же сервер, пока количество работающих серверов остается неизменным.</p> <p>Если значение или параметр не найдены, применяется алгоритм циклического перебора.</p>

4. (дополнительно) Выберите метод сохранения устойчивости для этого пула.

Устойчивость отслеживает и сохраняет такие данные сеанса, как конкретный участник пула, который обслужил запрос клиента. Благодаря сохранению устойчивости запросы клиента направляются к одному и тому же участнику пула во время существования сеанса или в течение последующих сеансов.

Протокол	Поддерживаемый метод сохранения устойчивости
HTTP	Нет, файлы cookie, исходный IP-адрес
HTTPS	Нет, IP-адрес источника и идентификатор сеанса SSL

Протокол	Поддерживаемый метод сохранения устойчивости
TCP	Нет, исходный IP-адрес, MSRDP
UDP	Нет, исходный IP-адрес

- Выберите **файлы Cookie**, чтобы вставить уникальный файл cookie для определения сеанса при первом входе клиента на сайт. Для сохранения подключения к соответствующему серверу в последующих запросах на этот файл cookie имеется ссылка.
- Выберите **Исходный IP-адрес**, чтобы отслеживать сеансы на основании исходных IP-адресов. Когда клиент запрашивает подключение к виртуальному серверу, поддерживающему сохранение сходства адресов источника, подсистема балансировки нагрузки проверяет, подключался ли этот клиент ранее, и, если подключался, перенаправляет клиента к тому же участнику пула.
- Выберите **идентификатор сеанса SSL**, а затем «Сквозной режим SSL» в качестве шаблона трафика HTTPS.
 - Сквозной режим SSL — Клиент -> HTTPS -> LB (сквозной режим SSL) -> HTTPS -> сервер
 - Клиент — HTTP-> LB -> HTTP -> серверы

Примечание vRealize Automation в настоящее время поддерживает только сквозной режим SSL. Метод «Сквозной режим SSL» используется вне зависимости от вашего выбора.

- Выберите **MSRDP**, чтобы поддерживать непрерывные сеансы между клиентами Windows и серверами, на которых запущена служба протокола удаленного рабочего стола Майкрософт (RDP). Рекомендованный сценарий для включения сохранения устойчивости MSRDP включает в себя создание пула балансировки нагрузки, состоящего из участников, работающих под управлением поддерживаемого сервера Windows Server, в котором все участники принадлежат кластеру Windows и принимают участие в каталоге сеанса Windows.
 - Выберите **Нет**, чтобы указать, что действия сеанса не сохраняются для последующего использования.
- 5.** При использовании параметра сохранения устойчивости файлов cookie введите имя файла cookie.

6. (дополнительно) Выберите режим, при котором файл cookie вставляется из раскрывающегося меню **Режим**.

Параметр	Описание
Вставка	NSX Edge отправляет файл cookie. Если сервер отправляет один файл cookie или несколько, клиент получает дополнительный файл cookie (файлы cookie сервера + файл cookie NSX Edge). Если сервер не отправляет файл cookie, клиент получает файл cookie NSX Edge.
Префикс	Сервер отправляет файл cookie. Используйте этот параметр, если ваш клиент поддерживает только один файл cookie. Если у вас закрытое приложение, использующее закрытый клиент, который поддерживает только один файл cookie, веб-сервер отправляет файл cookie, но NSXEdge вставляет (как префикс) свою информацию cookie в значение файла cookie сервера
Сеанс приложения	Сервер не отправляет файл cookie. Вместо этого он отправляет сведения о сеансе пользователя в виде URL-адреса. Например, http://mysite.com/admin/UpdateUserServlet;jsessionid=X000X0XXX0XXXX, где jsessionid — это сведения о сеансе пользователя, которые используются для устойчивости.

7. (дополнительно) Введите срок окончания действия сохранения для файлов cookie в секундах.

Например, для балансировки нагрузки L7 с исходным IP-адресом TCP срок действия механизма устойчивости истекает, если в указанный срок не создается ни одного нового подключения TCP, даже если существующие подключения все еще активны.

8. (дополнительно) Щелкните вкладку **Проверка работоспособности** и перейдите к разделу [Определение параметров проверки работоспособности виртуального сервера](#), чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX.

Определение параметров проверки работоспособности виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать, должна ли подсистема балансировки нагрузки NSX проверять работоспособность участников пула на виртуальном сервере и как это следует делать.

Параметры протокола и порта проверки работоспособности по умолчанию соответствуют параметрам протокола и порта на вкладке **Общие**.

Дополнительные сведения см. в разделе *Создание контроля за службой* в документации по продукту NSX по адресу https://www.vmware.com/support/pubs/nsx_pubs.html. Обратите внимание, что в документации NSX участники виртуального сервера называются участниками пула.

Необходимые условия

[Определение общих параметров виртуального сервера.](#)

Процедура

1. (дополнительно) Выберите протокол проверки работоспособности в раскрывающемся меню **Протокол проверки работоспособности**, чтобы указать, как осуществляется доступ к участнику пула, когда подсистема балансировки нагрузки прослушивает, чтобы определить работоспособность участника пула.

Варианты протокола: **HTTP, HTTPS, TCP, ICMP, UDP** и **Нет**.

Можно также принять протокол по умолчанию, указанный на вкладке "Общие".

2. (дополнительно) В поле **Порт проверки работоспособности** укажите номер порта, который прослушивает подсистема балансировки нагрузки для слежения за работоспособностью участника виртуального сервера или участника пула.

Обратите внимание, что в документации NSX участники виртуального сервера называются участниками пула.

Для протоколов HTTP, HTTPS и TCP можно задать общий порт с UDP. Например, если служба 1 использует TCP, HTTP или HTTPS на порте 80, служба 2 может использовать UDP на том же порте. Если служба 1 использует UDP на порте 80, служба 2 не может использовать UDP на том же порте.

3. Введите **Интервал** в секундах, по истечении которого сервер должен проверяться.
4. Введите максимальное **Время ожидания** в секундах, в течение которого должен быть получен ответ от сервера.
5. Введите **Макс. число попыток**, указывающее, сколько раз сервер должен проверяться, прежде чем он будет объявлен отключенным.
6. Укажите дополнительные параметры проверки работоспособности в соответствии с выбранным **протоколом проверки работоспособности**.

а) Укажите **Метод**, который следует использовать для определения состояния сервера. Возможные параметры — GET, OPTIONS и POST.

б) Укажите **URL-адрес**, который следует использовать в запросе на определение состояния сервера. Это URL-адрес, который используется в параметрах методов GET и POST (по умолчанию — «/»).

в) В поле **Отправить** укажите строку, которая отправляется серверу после установления соединения.

В поле **Отправить** укажите строку, которая отправляется серверу после установления соединения.

г) В поле **Получить** укажите строку, получение которой ожидается от сервера.

Сервер будет считаться работающим, только если полученная от него строка соответствует заданной.

Строка может являться заголовком либо находиться в тексте ответа.

- Щелкните вкладку **Дополнительные** и перейдите к разделу [Определение дополнительных параметров виртуального сервера](#), чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX.

Чтобы указать варианты ведения журнала, см. раздел [Определение параметров ведения журнала подсистемы балансировки нагрузки](#).

Определение дополнительных параметров виртуального сервера

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно настроить компонент подсистемы балансировки нагрузки NSX и указать такие параметры, как количество одновременных подключений, которые может распознать один участник пула, и максимальное количество одновременных подключений, которые может обработать виртуальный сервер.

Необходимые условия

[Определение общих параметров виртуального сервера.](#)

Процедура

- Введите значение в текстовое поле **Ограничение подключений**, чтобы указать максимальное количество одновременных подключений в NSX, которые может обработать виртуальный сервер.

Этот параметр учитывает количество подключений всех участников.

Введите значение 0, чтобы указать отсутствие ограничения.
- Введите значение в текстовое поле **Максимальная скорость подключений**, чтобы указать максимальное количество входящих запросов на подключение в NSX, которое может быть принято в секунду.

Этот параметр учитывает количество подключений всех участников.

Введите значение 0, чтобы указать отсутствие ограничения.
- (дополнительно) Установите флажок **Включить ускорение**, чтобы указать, что каждый виртуальный IP-адрес (VIP) использует более быструю подсистему балансировки нагрузки L4, а не подсистему L7.
- (дополнительно) Установите флажок **Прозрачные**, чтобы разрешить участникам пула подсистемы балансировки нагрузки просматривать IP-адреса компьютеров, которые вызывают подсистему балансировки нагрузки.

Если этот пункт не выбран, участники пула подсистемы балансировки нагрузки видят исходный IP-адрес трафика как внутренний IP-адрес подсистемы балансировки нагрузки.
- Введите значение в текстовое поле **Максимальное количество подключений**, чтобы задать максимальное количество одновременных подключений, которые может распознать один участник пула.

Если количество входящих запросов превышает это значение, запросы ставятся в очередь, а затем обрабатываются в том порядке, в котором они были получены, по мере освобождения подключений.

Введите значение 0, чтобы указать отсутствие максимального значения.

6. Введите значение в текстовое поле **Минимальное количество подключений**, чтобы задать минимальное количество одновременных подключений, которые один участник пула всегда должен принимать.

Введите значение 0, чтобы указать отсутствие минимального значения.

7. Нажмите кнопку **ОК**, чтобы завершить определение виртуального сервера.
8. Чтобы задать параметры ведения журнала, см. [Определение параметров ведения журнала подсистемы балансировки нагрузки](#). Если это не требуется, нажмите кнопку **Сохранить** или **Готово**

Определение параметров ведения журнала подсистемы балансировки нагрузки

Можно определить типы действий по ведению журнала подсистемы балансировки нагрузки, которые записываются в ее журналах.

После или во время определения компонента подсистемы балансировки нагрузки можно указать уровень ведения журнала для сбора журналов о трафике этой подсистемы. Уровни ведения журнала, определяемые для любого компонента подсистемы балансировки нагрузки в схеме элементов, применяются ко всем указанным в ней подсистемам балансировки нагрузки.

Предусмотрены следующие уровни ведения журнала: отладка, информация, предупреждение, ошибка и критическая ошибка. На уровнях «Отладка» и «Информация» в журнал записываются запросы пользователей, а на уровнях «Ошибка» и «Критическая ошибка» — нет.

Дополнительные сведения о ведении журнала подсистемы балансировки нагрузки NSX см. в *Руководстве по администрированию NSX*.

Необходимые условия

[Определение параметров участника подсистемы балансировки нагрузки.](#)

Процедура

1. Выберите вкладку **Глобальный** в компоненте подсистемы балансировки нагрузки на холсте проекта.
2. Выберите один или несколько параметров ведения журнала в раскрывающемся меню **Уровень ведения журнала**.

Выберите уровень ведения протокола для сохранения журналов регистрации трафика подсистемы балансировки нагрузки. Данный параметр применяется ко всем компонентам подсистемы балансировки нагрузки NSX в данной схеме элементов.

Параметры ведения журнала определяются в веб-клиенте vSphere.

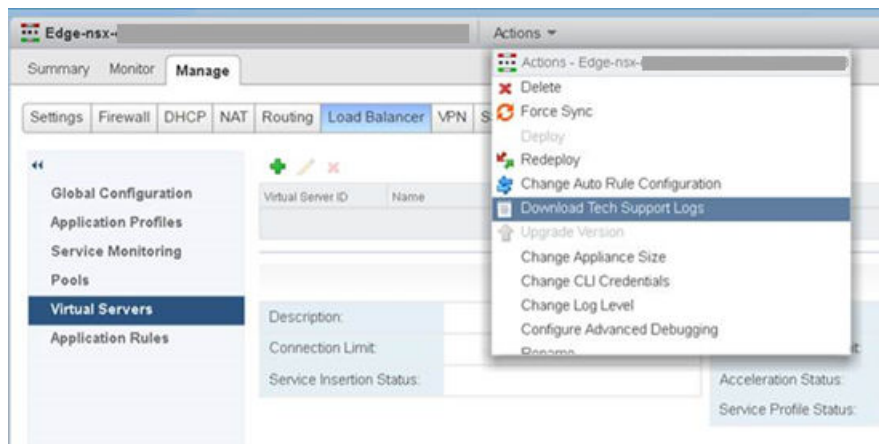
- Нет
- Информация
- Авария
- Оповещение
- Критическая ошибка
- Ошибка

- Предупреждение
- Уведомление
- Отладка

3. Нажмите кнопку **Сохранить**.

Результаты

Просмотреть и загрузить журналы можно в веб-клиенте vSphere, используя меню **Действия** для NSX Edge, как описано в разделе *Загрузка журналов для службы технической поддержки в NSX Edge* в документации по продукту NSX по адресу https://www.vmware.com/support/pubs/nsx_pubs.html.



Использование компонентов подсистемы балансировки нагрузки NSX-T в схеме элементов

Чтобы настроить параметры компонентов компьютера vSphere в схеме элементов, на холст проекта можно добавить один или несколько компонентов подсистемы балансировки нагрузки NSX-T по требованию.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX-T. Дополнительные сведения о настройке NSX-T см. в *руководстве по администрированию NSX-T* в [документации по продукту NSX-T](#).

К пулам подсистем балансировки нагрузки и параметрам сети виртуальных IP-адресов в схеме элементов применяются следующие правила.

- При использовании профиля сети пула NAT профиль сети виртуальных IP-адресов может быть частью профиля сети NAT.
- При использовании маршрутизируемого профиля сети пула профиль сети виртуальных IP-адресов может быть только в той же маршрутизируемой или внешней сети.
- При использовании внешнего профиля сети пула профиль сети виртуальных IP-адресов может быть только таким же профилем внешней сети.

Для каждого из компонентов «Подсистема балансировки нагрузки» могут использоваться несколько виртуальных серверов, которые также называются службами подсистемы балансировки нагрузки. На каждом из виртуальных серверов в компоненте «Подсистема балансировки нагрузки» может использоваться один порт и протокол. Например, можно применить балансировку нагрузки к службе HTTP или службе HTTPS. Подсистема балансировки нагрузки может применять балансировку к нескольким службам.

Подсистема балансировки нагрузки NSX — это служба, которая содержит виртуальные серверы балансировки нагрузки.

Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Дополнительные сведения о NSX-Т конкретном развертывании и особенности топологии см. в разделе [Общие сведения о топологиях развертывания NSX-Т для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Добавление подсистемы балансировки нагрузки NSX-Т по требованию

Можно перетащить компонент подсистемы балансировки нагрузки NSX-Т по требованию на холст проекта и настроить его параметры для использования с компонентами компьютеров vSphere и компонентами контейнеров в схеме элементов.

Подсистема балансировки нагрузки NSX-Т распределяет входящие запросы служб равномерно между несколькими серверами таким образом, чтобы распределение нагрузки было прозрачным для пользователей. Балансировка нагрузки позволяет обеспечить оптимальное использование ресурсов, повысить пропускную способность до максимума, сократить время реагирования и избежать перегрузок.

Можно сопоставить виртуальный IP-адрес с набором серверов пула для балансировки нагрузки.

Подсистема балансировки нагрузки принимает запросы TCP, UDP, HTTP или HTTPS на виртуальный IP-адрес и решает, какой элемент пула использовать. Подсистема балансировки нагрузки подключается к логическому маршрутизатору первого уровня.

В зависимости от потребностей среды можно масштабировать производительность подсистемы балансировки нагрузки, увеличивая количество существующих виртуальных серверов и участников пула, чтобы справляться с высокой нагрузкой сетевого трафика.

Дополнительные сведения по созданию подсистем балансировки нагрузки NSX-T для определения поведения сетевого трафика см. в разделах *Логическая подсистема балансировки нагрузки* и *Настройка компонентов подсистемы балансировки нагрузки/руководство по администрированию NSX-T* в документации по продукту NSX-T.

Процедура

1. Определение параметров участника подсистемы балансировки нагрузки NSX-T

Можно определить компонент подсистемы балансировки нагрузки по требованию NSX-T, чтобы распределить обработку задач между подготовленными компьютерами участников vSphere или компьютерами контейнеров в сети.

2. Определение общих параметров виртуального сервера для NSX-T

Можно определить один протокол и порт виртуального сервера для подсистемы балансировки нагрузки или можно добавить дополнительные виртуальные серверы, чтобы настроить дополнительные компоненты подсистемы балансировки нагрузки NSX-T.

3. Определение параметров распределения виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** при определении виртуального сервера, можно указать сведения об участниках пула — например, порт, через который участникам поступает трафик, тип протокола, который подсистема балансировки NSX-T может использовать для обращения к этому порту, алгоритм, используемый для балансировки нагрузки, а также параметры устойчивости.

4. Определение параметров проверки работоспособности виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать, должна ли подсистема балансировки нагрузки NSX-T проверять работоспособность участников пула на виртуальном сервере и как это следует делать.

5. Определение дополнительных параметров виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно настроить компонент подсистемы балансировки нагрузки NSX-T и указать такие параметры, как количество одновременных подключений, которые может распознать один участник пула, и максимальное количество одновременных подключений, которые может обработать виртуальный сервер.

6. Определение параметров ведения журнала подсистемы балансировки нагрузки NSX-T

Можно определить типы действий по ведению журнала подсистемы балансировки нагрузки, которые записываются в ее журналах.

Определение параметров участника подсистемы балансировки нагрузки NSX-T

Можно определить компонент подсистемы балансировки нагрузки по требованию NSX-T, чтобы распределить обработку задач между подготовленными компьютерами участников vSphere или компьютерами контейнеров в сети.

При добавлении компонента подсистемы балансировки нагрузки в схему элементов на холсте проекта, можно выбрать индивидуальный вариант или вариант по умолчанию при создании или изменении определений виртуального сервера в компоненте подсистемы балансировки нагрузки. Вариант по умолчанию позволяет выбрать протокол, порт и описание виртуального сервера и использовать значения по умолчанию для всех остальных параметров. Вариант индивидуальной настройки позволяет определить дополнительные уровни детализации.

Если подсистема балансировки нагрузки подготовлена с помощью внешней сети, виртуальный IP-адрес (сеть виртуальных IP-адресов) и пул участников (сеть участников) должны находиться в одной существующей сети. Если виртуальный IP-адрес и пул участников находятся в разных внешних сетях, при попытке подготовки произойдет ошибка.

Необходимые условия

- Создайте и настройте параметры подсистемы балансировки нагрузки для NSX. См. раздел [Контрольный список для подготовки к настройке сети и системы безопасности NSX](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Создайте профиль сети. См. раздел [Создание профиля сети в vRealize Automation](#).
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.
- Убедитесь, что как минимум один компонент компьютера vSphere или компонент контейнера существует в схеме элементов.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Подсистема балансировки нагрузки по требованию NSX-T**.
3. Чтобы добавить уникальную метку для компонента на холст проекта, введите имя компонента в текстовом поле **Идентификатор**.
4. Выберите имя компонента компьютера vSphere или компонента контейнера из раскрывающегося меню **Участник**.
Это список содержит только компоненты компьютера vSphere и компоненты контейнера в активной схеме элементов.
5. В раскрывающемся меню **Сеть участников** выберите сетевой адаптер для балансировки нагрузки.
Список содержит сетевые адаптеры, которые определены для выбранного участника-компьютера vSphere.

6. Выберите доступную сеть виртуальных IP-адресов в раскрывающемся меню **Сеть виртуальных IP-адресов**. Например, выберите доступную внешнюю сеть или сеть NAT.

В схеме элементов может быть несколько подсистем балансировки нагрузки NSX и компонентов сети по требованию NSX, но все они должны быть связаны с одной сетью виртуальных IP-адресов.

7. (дополнительно) В текстовом поле **IP-адрес** укажите допустимый IP-адрес для сетевого адаптера.

По умолчанию это статический IP-адрес, который связан с сетью виртуальных VIP-адресов. Однако можно указать другой IP-адрес или диапазон IP-адресов. По умолчанию следующий доступный IP-адрес выделяется из связанной сети виртуальных IP-адресов.

Оставьте поле IP-адреса пустым, чтобы во время подготовки такой адрес мог быть выделен из связанной сети виртуальных IP-адресов.

Если указать IP-адрес для любого типа сети, то можно будет подготовить только одно развертывание. При последующих развертываниях произойдет ошибка выделения IP-адресов, так как данный IP-адрес уже будет использоваться первым развертыванием.

8. Чтобы создать определение виртуального сервера, нажмите кнопку **Создать** и ознакомьтесь с разделом [Определение общих параметров виртуального сервера для NSX-T](#).

Для каждого компонента подсистемы балансировки нагрузки требуется хотя бы один виртуальный сервер.

Чтобы указать варианты ведения журнала, см. раздел [Определение параметров ведения журнала подсистемы балансировки нагрузки NSX-T](#).

Определение общих параметров виртуального сервера для NSX-T

Можно определить один протокол и порт виртуального сервера для подсистемы балансировки нагрузки или можно добавить дополнительные виртуальные серверы, чтобы настроить дополнительные компоненты подсистемы балансировки нагрузки NSX-T.

Например, можно настроить компонент подсистемы балансировки нагрузки, чтобы определить такие параметры, как протокол и порт проверки работоспособности, алгоритм, сохранение устойчивости и прозрачность.

Необходимые условия

[Определение параметров участника подсистемы балансировки нагрузки NSX-T](#).

Процедура

1. Откройте вкладку **Общие** на странице **Виртуальный сервер**.
2. Выберите протокол сетевого трафика, который следует использовать для балансировки нагрузки виртуального сервера, в раскрывающемся меню **Протокол**.

Варианты протокола: HTTP, HTTPS, TCP и UDP.

Подсистемы балансировки нагрузки NSX-T не поддерживают транзитный режим SSL и используют вместо этого режим прерывания SSL. При выборе варианта HTTPS нужно предоставить следующую дополнительную информацию, которая уже должна быть определена в диспетчере NSX-T:

- Имя сертификата в иерархии сертификатов NSX-T. Система балансировки нагрузки представляет этот сертификат клиентам.
- Имя профиля SSL, принадлежащего клиенту.

3. В текстовом поле **Порт** введите значение порта.

Выбранный протокол определяет порт по умолчанию.

Протокол	Порт по умолчанию
HTTP	80
HTTPS	443
TCP	8080
UDP	нет по умолчанию

Для протоколов HTTP, HTTPS и TCP можно задать общий порт с UDP. Например, если служба 1 использует TCP, HTTP или HTTPS на порте 80, служба 2 может использовать UDP на том же порте. Если служба 1 использует UDP на порте 80, служба 2 не может использовать UDP на том же порте.

4. (дополнительно) Введите описание компонента виртуального сервера.

5. Щелкните вкладку **Распределение** и перейдите к разделу [Определение параметров распределения виртуального сервера для NSX-T](#), чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX-T.

Определение параметров распределения виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** при определении виртуального сервера, можно указать сведения об участниках пула — например, порт, через который участникам поступает трафик, тип протокола, который подсистема балансировки NSX-T может использовать для обращения к этому порту, алгоритм, используемый для балансировки нагрузки, а также параметры устойчивости.

Пул представляет собой кластер компьютеров с балансировкой нагрузки. Участник пула — это отдельный компьютер в данном кластере.

Параметры протокола и порта участника по умолчанию соответствуют параметрам протокола и порта на странице **Общие**.

Пул компьютеров-участников отображается в значении параметра **Участник** в пользовательском интерфейсе компонента подсистемы балансировки нагрузки схемы элементов. Запись **Участник** указывает пул или кластер компьютеров.

Необходимые условия

[Определение параметров участника подсистемы балансировки нагрузки NSX-T.](#)

Процедура

1. (дополнительно) Параметр **Протокол участника** соответствует протоколу, определенному на вкладке **Общие**. Этот параметр определяет, как участник пула должен получать сетевой трафик.
2. (дополнительно) Введите номер порта в текстовом поле **Порт участника**, чтобы указать порт, по которому участник пула должен получать сетевой трафик.

Например, если входящий запрос на виртуальный IP-адрес (VIP) подсистемы балансировки нагрузки приходит на порт 80, возможно, понадобится направить этот запрос на другой порт (например, порт 8080) для участников пула.

3. (дополнительно) Выберите алгоритм метода балансировки для этого пула.

Варианты алгоритма и его параметры для вариантов, которым они требуются, описаны в таблице ниже.

Дополнительные сведения см. в разделе *Установка серверного пула для балансировки нагрузки* в [документации по продукту NSX-T](#).

Параметр	Описание и параметры алгоритма
ROUND_ROBIN	Входящие запросы клиентов проходят циклически по списку доступных серверов, которые могут обрабатывать запрос. Вес элементов пула серверов игнорируется, даже если он настроен.
ЦИКЛИЧЕСКИЙ ПЕРЕБОР ПО ВЕСУ	Каждому серверу присваивается коэффициент нагрузки, который указывает, какое количество запросов сервер обрабатывает по сравнению с другими серверами в пуле. Значение определяет, сколько запросов клиентов отправляется на сервер по сравнению с другими серверами в пуле. Этот алгоритм подсистемы балансировки нагрузки ориентирован на относительное распределение нагрузки между доступными ресурсами сервера.
IP-HASH	Выбирает сервер на основании хэша исходного IP-адреса и общего веса всех работающих серверов.
LEASTCONN	Клиентские запросы распределяются между несколькими серверами в зависимости от количества соединений на сервере. Запросы на новые подключения отправляются на сервер с наименьшим количеством подключений. Вес элементов пула серверов игнорируется, даже если он настроен.
МИНИМАЛЬНОЕ КОЛИЧЕСТВО ПОДКЛЮЧЕНИЙ (LEASTCONN) ПО ВЕСУ	Каждому серверу присваивается коэффициент нагрузки, который указывает, какое количество запросов сервер обрабатывает по сравнению с другими серверами в пуле. Значение определяет, сколько запросов клиентов отправляется на сервер по сравнению с другими серверами в пуле. Этот алгоритм подсистемы балансировки нагрузки ориентирован на использование значений веса для относительного распределения нагрузки между доступными ресурсами сервера. По умолчанию значение веса равно 1, если это значение не настроено и включен параметр медленного запуска.

4. (дополнительно) Выберите метод сохранения устойчивости для этого пула.

Устойчивость отслеживает и сохраняет такие данные сеанса, как конкретный участник пула, который обслужил запрос клиента. Благодаря сохранению устойчивости запросы клиента направляются к одному и тому же участнику пула во время существования сеанса или в течение последующих сеансов. Дополнительные сведения о методах сохранения устойчивости см. раздел *Настройка устойчивых профилей* в [документации по продукту NSX-T](#).

- Выберите **Нет**, чтобы указать, что действия сеанса не сохраняются для последующего использования.
- Выберите **файлы Cookie**, чтобы вставить уникальный файл cookie для определения сеанса при первом входе клиента на сайт. Для сохранения подключения к соответствующему серверу в последующих запросах на этот файл cookie имеется ссылка.
- Выберите **Исходный IP-адрес**, чтобы отслеживать сеансы на основании исходных IP-адресов. Когда клиент запрашивает подключение к виртуальному серверу, поддерживающему сохранение сходства адресов источника, подсистема балансировки нагрузки проверяет, подключался ли этот клиент ранее, и, если подключался, перенаправляет клиента к тому же участнику пула.

5. При использовании параметра сохранения файлов cookie введите имя файла cookie.

6. (дополнительно) Выберите режим, при котором файл cookie вставляется из раскрывающегося меню **Режим**.

Параметр	Описание
Вставка	Создание уникального файла cookie для идентификации данного сеанса.
Префикс	Добавление к существующему файлу cookie.
Перезапись	Перезапись существующего файла cookie.

7. (дополнительно) Введите срок окончания действия сохранения для файлов cookie в секундах.

Например, для балансировки нагрузки L7 с исходным IP-адресом TCP срок действия механизма устойчивости истекает, если в указанный срок не создается ни одного нового подключения TCP, даже если существующие подключения все еще активны.

8. (дополнительно) Щелкните вкладку **Проверка работоспособности** и перейдите к разделу [Определение параметров проверки работоспособности виртуального сервера для NSX-T](#), чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX-T.

Определение параметров проверки работоспособности виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно указать, должна ли подсистема балансировки нагрузки NSX-T проверять работоспособность участников пула на виртуальном сервере и как это следует делать.

Параметры протокола и порта проверки работоспособности по умолчанию соответствуют параметрам протокола и порта на вкладке **Общие**.

Дополнительные сведения см. в [документации по продукту NSX-T](#). Обратите внимание, что в документации NSX-T участники виртуального сервера называются участниками пула.

Необходимые условия

Определение параметров распределения виртуального сервера для NSX-T.

Процедура

1. (дополнительно) Выберите протокол проверки работоспособности в раскрывающемся меню **Протокол проверки работоспособности**, чтобы указать, как осуществляется доступ к участнику пула, когда подсистема балансировки нагрузки прослушивает, чтобы определить работоспособность участника пула.

Варианты протокола: **отсутствует, HTTP, HTTPS, TCP, ICMP и UDP.**

Можно также принять протокол по умолчанию, указанный на вкладке "Общие".

2. (дополнительно) В поле **Порт проверки работоспособности** укажите номер порта, который прослушивает подсистема балансировки нагрузки для слежения за работоспособностью участника виртуального сервера или участника пула.

Обратите внимание, что в документации NSX участники виртуального сервера называются участниками пула.

Для протоколов HTTP, HTTPS и TCP можно задать общий порт с UDP. Например, если служба 1 использует TCP, HTTP или HTTPS на порте 80, служба 2 может использовать UDP на том же порте. Если служба 1 использует UDP на порте 80, служба 2 не может использовать UDP на том же порте.

3. Введите **Интервал** в секундах, по истечении которого сервер должен проверяться.
4. Введите максимальное **Время ожидания** в секундах, в течение которого должен быть получен ответ от сервера.
5. Введите **Макс. число попыток**, указывающее, сколько раз сервер должен проверяться, прежде чем он будет объявлен отключенным.
6. Если выбран протокол HTTP или HTTPS, введите **метод**, который будет использоваться для определения состояния сервера.
7. Укажите **URL-адрес** (если он задан), который следует использовать в запросе на определение состояния сервера. Это URL-адрес, который используется в параметрах методов GET и POST (по умолчанию — «/»).

8. Если заданы строки для отправки и получения, введите их в текстовых полях **Отправить** и **Получить**.

В поле **Отправить** укажите строку, которая отправляется серверу после установления соединения.

В поле **Получить** укажите строку, получение которой ожидается от сервера. Сервер будет считаться работающим, только если полученная от него строка соответствует заданной.

9. Щелкните вкладку **Дополнительные** и перейдите к разделу **Определение дополнительных параметров виртуального сервера для NSX-T**, чтобы продолжить определение виртуального сервера в компоненте подсистемы балансировки нагрузки NSX-T.

Чтобы указать варианты ведения журнала, см. раздел **Определение параметров ведения журнала подсистемы балансировки нагрузки NSX-T**.

Определение дополнительных параметров виртуального сервера для NSX-T

Выбрав пункт **Индивидуальная настройка** на вкладке **Общие**, можно настроить компонент подсистемы балансировки нагрузки NSX-T и указать такие параметры, как количество одновременных подключений, которые может распознать один участник пула, и максимальное количество одновременных подключений, которые может обработать виртуальный сервер.

Необходимые условия

Определение общих параметров виртуального сервера для NSX-T.

Процедура

1. Введите значение в текстовое поле **Ограничение подключений**, чтобы указать максимальное количество одновременных подключений в NSX-T, которые может обработать виртуальный сервер.

Этот параметр учитывает количество подключений всех участников.

Введите значение 0, чтобы указать отсутствие ограничения.

2. Введите значение в текстовое поле **Максимальная скорость подключений**, чтобы указать максимальное количество входящих запросов на подключение в NSX-T, которое может быть принято в секунду.

Этот параметр учитывает количество подключений всех участников.

Введите значение 0, чтобы указать отсутствие ограничения.

3. (дополнительно) Установите флажок **Прозрачные**, чтобы разрешить участникам пула подсистемы балансировки нагрузки просматривать IP-адреса компьютеров, которые вызывают подсистему балансировки нагрузки.

Если этот пункт не выбран, участники пула подсистемы балансировки нагрузки видят исходный IP-адрес трафика как внутренний IP-адрес подсистемы балансировки нагрузки.

4. Введите значение в текстовое поле **Максимальное количество подключений**, чтобы задать максимальное количество одновременных подключений, которые может распознать один участник пула.

Если количество входящих запросов превышает это значение, запросы ставятся в очередь, а затем обрабатываются в том порядке, в котором они были получены, по мере освобождения подключений.

Введите значение 0, чтобы указать отсутствие максимального значения.

5. Нажмите кнопку **ОК**, чтобы завершить определение виртуального сервера.
6. Чтобы задать параметры ведения журнала, см. [Определение параметров ведения журнала подсистемы балансировки нагрузки NSX-T](#). Если это не требуется, нажмите кнопку **Сохранить** или **Готово**

Определение параметров ведения журнала подсистемы балансировки нагрузки NSX-T

Можно определить типы действий по ведению журнала подсистемы балансировки нагрузки, которые записываются в ее журналах.

Для сохранения журналов регистрации трафика подсистемы балансировки нагрузки можно указать уровень ведения журнала. Уровни ведения журнала, определяемые для любого компонента подсистемы балансировки нагрузки NSX-T в схеме элементов, применяются ко всем указанным в ней подсистемам балансировки нагрузки.

Предусмотрены следующие уровни ведения журнала: отладка, информация, предупреждение, ошибка и критическая ошибка. На уровнях «Отладка» и «Информация» в журнал записываются запросы пользователей, а на уровнях «Ошибка» и «Критическая ошибка» — нет.

Дополнительную информацию о ведении журнала для подсистемы балансировки нагрузки NSX-T см. *Руководство по администрированию NSX-T* в [документации по продукту NSX-T](#).

Необходимые условия

Определение параметров участника подсистемы балансировки нагрузки NSX-T

Процедура

1. Выберите вкладку **Глобальный** в компоненте подсистемы балансировки нагрузки на холсте проекта.
2. Выберите один или несколько параметров ведения журнала в раскрывающемся меню **Уровень ведения журнала**.

Параметры ведения журнала определяются в веб-клиенте vSphere.

- Нет
- Авария
- Оповещение
- Критическая ошибка
- Ошибка
- Предупреждение
- Информация
- Отладка

3. Выберите малый, средний или большой размер системы балансировки нагрузки.
4. Нажмите **Сохранить**, затем нажмите **Готово**.

Использование компонентов безопасности NSX for vSphere в схеме элементов

Компоненты безопасности NSX for vSphere можно добавить на холст проекта, чтобы сделать их настроенные параметры доступными для одного или нескольких компонентов компьютера vSphere в схеме элементов.

В приложении NSX группы безопасности, теги и политики настраиваются за пределами vRealize Automation.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

В схеме элементов можно добавить элементы управления безопасности, настроив группы безопасности, теги и политики для вычислительного ресурса vSphere в NSX. После сбора данных конфигурации безопасности можно выбрать в vRealize Automation.

Пример стратегии безопасности NSX for vSphere см. в записи блога [vRealize and NSX](#).

Существующие группы безопасности и группы безопасности по требованию для NSX for vSphere

Группа безопасности представляет собой совокупность ресурсов или группировки объектов из иерархии vSphere, отображаемой на наборе политик безопасности, например распространяемые правила брандмауэра и сторонние службы обеспечения безопасности, такие как антивирусы и системы обнаружения вторжений. С помощью групп можно создавать пользовательские контейнеры, которым можно назначать ресурсы, такие как виртуальные машины и сетевые адаптеры, для защиты с помощью распределенного брандмауэра. После определения группы ее можно добавить в качестве источника или места назначения в правило брандмауэра для защиты.

В дополнение к группам безопасности, указанным в резервировании, в схему элементов можно добавить имеющиеся группы безопасности vSphere или группы безопасности по требованию.

Можно создать одну или несколько групп безопасности по требованию. Для группы безопасности можно выбрать и настроить одну или несколько политик безопасности.

Политика безопасности представляет собой набор служб для диагностики конечных точек, брандмауэра и сети, которые можно применить к группе безопасности. В виртуальную машину vSphere можно добавить политику безопасности с помощью группы безопасности по требованию в схеме элементов. Нельзя добавить политику безопасности непосредственно в резервирование. После сбора данных политики безопасности, определенные в NSX for vSphere для вычислительного ресурса, можно выбрать на схеме элементов.

Группы безопасности настраиваются в исходном ресурсе. Сведения об управлении группами безопасности для различных типов ресурсов см. в документации NSX for vSphere.

Примечание При включенной изоляции приложений будет создана отдельная политика безопасности. При изоляции приложений используется логический брандмауэр для блокирования всего входящего и исходящего трафика приложений в схеме элементов. Компьютеры компонентов, которые подготавливаются с использованием схем элементов, содержащих политику изоляции приложений, могут обмениваться данными друг с другом, но не могут подключаться к компьютерам за пределами брандмауэра, если другие группы безопасности не будут добавлены в схему элементов с политиками безопасности, которые разрешают доступ.

Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Существующие теги безопасности для NSX for vSphere

Можно добавить компоненты существующих тегов безопасности для NSX for vSphere. Тег безопасности является объектом или записью классификации, который можно использовать в качестве механизма группирования. Вы определяете критерии, которым должен отвечать объект, который будет добавлен в создаваемую группу безопасности. Таким образом, вы можете включить компьютеры, определив критерии фильтрации с помощью ряда параметров, которые поддерживаются, чтобы соответствовать критериям. Например, можно добавить все компьютеры с определенными тегами безопасности в группу безопасности. Добавление компонента существующей группы безопасности для NSX for vSphere

Компонент существующей группы безопасности NSX for vSphere можно добавить на холст проекта при подготовке, чтобы связать его параметры с одним или несколькими компонентами компьютера vSphere в схеме элементов.

С помощью компонента существующей группы безопасности можно добавить группу безопасности NSX на холст проекта и настроить параметры этой группы, чтобы использовать ее с компонентами компьютеров vSphere и компонентами Программное обеспечение или Все как услуга, которые принадлежат к vSphere.

При создании схемы элементов по умолчанию доступны те группы безопасности, которые применимы к текущему арендатору. В частности группы безопасности доступны в том случае, если в текущем арендаторе есть резервирование для связанной конечной точки. Для получения дополнительной информации об управлении доступом к арендаторам см. раздел [Управление доступом к объектам безопасности из арендаторов в vRealize Automation](#).

Необходимые условия

- Создайте и настройте группы безопасности для NSX. См. контрольный список конфигураций NSX в *Настройка vRealize Automation* и руководстве по администрированию NSX for vSphere в [документации по продукту NSX for vSphere](#).

- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Ознакомьтесь с основными понятиями о компоненте безопасности. См. раздел [Использование компонентов безопасности NSX for vSphere в схеме элементов](#).
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Тег безопасности**.
3. Выберите существующую группу безопасности из раскрывающегося меню **Группа безопасности**.
4. Нажмите кнопку **ОК**.
5. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Результаты

Параметры безопасности можно добавить на вкладке **Безопасность** компонента компьютера vSphere.

Добавление существующего тега безопасности для NSX for vSphere

Компонент существующего тега безопасности NSX for vSphere можно добавить на холст проекта схемы элементов при подготовке, чтобы связать его параметры с одним или несколькими компонентами vSphere в схеме элементов.

С помощью компонента тега безопасности можно добавить существующий тег безопасности vSphere на холст проекта и настроить параметры этого тега, чтобы использовать его для компонентов компьютера vSphere и компонентов Программное обеспечение, которые принадлежат к vSphere.

При создании схемы элементов по умолчанию доступны те теги безопасности, которые применимы к текущему арендатору. В частности теги безопасности доступны в том случае, если в текущем арендаторе есть резервирование для связанной конечной точки. Для получения дополнительной информации об управлении доступом к арендаторам см. раздел [Управление доступом к объектам безопасности из арендаторов в vRealize Automation](#).

На холст проекта можно добавить несколько компонентов сети и безопасности.

Дополнительные сведения см. в разделе [Использование компонентов безопасности NSX for vSphere в схеме элементов](#).

Необходимые условия

- Создайте и настройте теги безопасности для NSX. См. контрольный список конфигураций NSX в *Настройка vRealize Automation и руководстве по администрированию NSX for vSphere* в [документации по продукту NSX for vSphere](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Существующий тег безопасности**.
3. Щелкните в текстовом поле **Тег безопасности** и выберите существующий тег безопасности.
4. Нажмите кнопку **ОК**.
5. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Результаты

Параметры безопасности можно добавить на вкладке **Безопасность** компонента компьютера vSphere.

Добавление компонента группы безопасности по требованию

Компонент группы безопасности NSX по требованию можно добавить на холст проекта при подготовке, чтобы связать его параметры с одним или несколькими компонентами компьютеров vSphere или другими доступными типами компонентов в схеме элементов.

Для создания группы безопасности по требованию необходимо добавить политики безопасности. Эти политики безопасности могут быть по умолчанию доступны во всех арендаторах или скрыты. Политики доступны только в арендаторах, в которых есть резервирование для связанной конечной точки NSX.

При создании схемы элементов по умолчанию доступны те группы безопасности, которые применимы к текущему арендатору. В частности группы безопасности доступны в том случае, если в текущем арендаторе есть резервирование для связанной конечной точки. Для получения дополнительной информации об управлении доступом к арендаторам см. раздел [Управление доступом к объектам безопасности из арендаторов в vRealize Automation](#).

Необходимые условия

- Создайте и настройте политику безопасности в NSX. См. *NSXруководство администратора*.
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.

Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Ознакомьтесь с основными понятиями о компоненте безопасности. См. раздел [Использование компонентов безопасности NSX for vSphere в схеме элементов](#).
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Группа безопасности по требованию**.
3. Введите имя и, при необходимости, описание.
4. Для добавления одной или нескольких политик безопасности щелкните значок **Добавить** в области **Политики безопасности** и выберите доступные политики безопасности.
5. Нажмите кнопку **ОК**.
6. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Результаты

Параметры безопасности можно добавить на вкладке **Безопасность** компонента компьютера vSphere.

Использование компонентов безопасности NSX-T в схеме элементов

Компонент безопасности сети NSX-T можно добавить на холст проекта, чтобы сделать настроенные в нем параметры доступными для одного или нескольких связанных компонентов компьютера vSphere в схеме элементов.

Существующая группа NS в NSX-T позволяет назначать ресурсы, например виртуальные машины и сетевые адаптеры, которые должны защищаться распределенным брандмауэром.

В схеме элементов можно добавить элементы управления безопасностью, настроив группы NS для вычислительного ресурса vSphere в NSX-T. После сбора данных конфигурации безопасности можно выбрать в vRealize Automation. Компонент существующей группы NS NSX-T можно добавить в схему элементов как источник или место назначения для правила брандмауэра.

Управление группами безопасности NS NSX-T осуществляется за пределами vRealize Automation в приложении NSX-T. Дополнительные сведения об управлении группами NS см. в документации по продукту NSX-T.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

При развертывании схемы элементов, которая содержит конечную точку NSX-T, развертывание назначает тег компонентам NSX-T в развертывании. Имя тега совпадает с именем развертывания.

При включенной изоляции приложений для развертывания создается новый раздел с правилами брандмауэра. При изоляции приложений используется логический брандмауэр для блокирования всего входящего и исходящего трафика приложений в схеме элементов. Компьютеры компонентов, которые подготавливаются с использованием схем элементов, содержащих политику изоляции приложений, могут обмениваться данными друг с другом, но не могут подключаться к компьютерам за пределами брандмауэра, если другие группы NS не будут добавлены в схему элементов с политиками безопасности, которые разрешают доступ.

Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Для NSX-T изоляция приложений — это единственная группа NS, создаваемая по требованию. Она содержит набор IP-адресов, который включает в себя виртуальные IP-адреса подсистемы балансировки нагрузки и внешние IP-адреса профиля сети NAT «один ко многим».

Дополнительные сведения о NSX-T конкретном развертывании и особенности топологии см. в разделе [Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Добавление компонента группы NSGroup NSX-T

Можно добавить компонент существующей группы NS NSX-T на холст проекта и настроить его параметры для использования с компонентами компьютера vSphere и другими связанными компонентами, такими как программные и сетевые компоненты.

Группа NS NSX-T может содержать комбинацию наборов IP-адресов, наборов MAC-адресов, логических портов, логических коммутаторов и других групп NSGroup. Можно указать группы NSGroup в качестве источников и назначений в правилах брандмауэра. Дополнительные сведения о характеристиках NSGroup см. в разделе *Создание NSGroup* [руководства по администрированию NSX-T в документации по продукту NSX-T](#).

Примечание Безопасность NSGroup применяется к виртуальным машинам, которые подключены к непрозрачным сетям под управлением NSX-T. Если ВМ подключена к группе dvPortGroup vSphere, микросегментация для этой сети будет недоступна.

При создании или редактировании схемы элементов по умолчанию доступны группы NSGroup, которые применимы к текущему арендатору. Группы безопасности доступны в том случае, если в текущем арендаторе зарезервирована связанная конечная точка. Для получения дополнительной информации об управлении доступом к арендаторам см. раздел [Управление доступом к объектам безопасности из арендаторов в vRealize Automation](#).

Необходимые условия

- Создайте и настройте группу NSGroup в NSX-T. См. раздел [Контрольный список для подготовки к настройке сети и системы безопасности NSX](#).
- Убедитесь, что анализ иерархии NSX для кластера успешно выполнен.
Чтобы использовать конфигурации NSX в vRealize Automation, необходимо выполнить сбор данных.
- Ознакомьтесь с основными понятиями о компоненте безопасности. См. раздел [Использование компонентов безопасности NSX-T в схеме элементов](#).
- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **NSX-T NSGroup**.
3. Выберите нужную группу NSGroup в раскрывающемся меню.
4. При появлении запроса введите связанную конечную точку.
5. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Результаты

Параметры безопасности можно добавить на вкладке **Безопасность** компонента компьютера vSphere.
Связывание компонентов сети и системы безопасности

Компоненты сети и безопасности можно перетащить на холст проекта, чтобы их параметры стали доступны для настройки конфигурации компонентов компьютера в схеме элементов. После настройки параметров сети и безопасности для компьютера можно дополнительно связать их с настройками компонента подсистемы балансировки нагрузки.

После добавления компонента сети или безопасности NSX на холст проекта и определения доступных параметров можно открыть вкладки сети и безопасности компонента компьютера vSphere на холсте и настроить соответствующие параметры.

Можно перетащить компонент сети NAT по требованию на холст проекта и связать его с компонентом компьютера vSphere или компонентом подсистемы балансировки нагрузки NSX в схеме элементов.

Параметры компонентов сети и безопасности, добавляемые в схему элементов, наследуются от конфигурации NSX for vSphere и NSX-T. Дополнительные сведения о настройке NSX см. в *руководстве по администрированию* в [документации по продукту NSX for vSphere](#) или в [документации по продукту NSX-T](#), в зависимости от используемого приложения.

Примечание Если схема элементов содержит подсистемы балансировки нагрузки и для этой схемы включена изоляция приложений, то виртуальные IP-адреса подсистемы балансировки нагрузки будут добавлены в группу безопасности изоляции приложений как набор IP-адресов. Если в схеме элементов содержится группа безопасности по требованию, связанная с уровнем компьютеров, который также связан с подсистемой балансировки нагрузки, то группа безопасности по требованию будет включать в себя уровень компьютеров, набор IP-адресов и виртуальные IP-адреса.

Сведения об использовании правил NAT, разрешающих портам TCP и UDP сопоставлять внешний IP-адрес Edge (порта источника) с частным IP-адресом в компоненте сети NAT (портом назначения), см. в разделе [Создание и использование правил NAT для NSX for vSphere](#) или [Создание и использование правил NAT для NSX-T](#).

Дополнительные сведения о NSX-T-конкретном развертывании и особенности топологии см. в разделе [Общие сведения о топологиях развертывания NSX-T для конфигураций сетевых подключений, системы безопасности и подсистемы балансировки нагрузки](#).

Настройка схемы элементов для подготовки из файла OVF

Файл OVF можно использовать для определения свойств компьютера vSphere и параметров оборудования, которые обычно определяются на страницах настройки схемы элементов в vRealize Automation или программным путем с помощью интерфейсов REST API vRealize Automation или vRealize CloudClient.

Можно также импортировать параметры из файла OVF, чтобы определить набор значений для профиля компонента образа. В параметризованных схемах элементов используются типы профилей компонентов «Образ» и «Размер».

OVF — это стандарт с открытым исходным кодом для создания пакетов программного обеспечения для виртуальных машин и их распределения.

Подготовка файла OVF аналогична клонированию, за исключением того, что в качестве исходного компьютера используется шаблон OVF, размещенный на сервере или веб-сайте, а не шаблон виртуальной машины, размещенный в vCenter.

Файл OVF обычно используется для описания одной виртуальной машины или виртуального устройства. Он может содержать сведения о формате файла образа виртуального диска и описание виртуального оборудования, которое необходимо эмулировать для запуска ОС или приложения, содержащегося в образе диска. Файл OVA — это пакет виртуального устройства, содержащий файлы, которые используются для описания виртуальной машины, включая файл-дескриптор OVF, манифест и файлы сертификата (необязательно), а также другие связанные файлы.

При определении схемы элементов параметр подготовки ImportOvfWorkflow доступен в компоненте компьютера vSphere. Он также доступен при определении набора значений для профиль компонента образа в словаре свойств.

Параметры конфигурации схемы элементов можно добавить в файл OVF для описания следующих типов данных.

- Минимальные требования к выделению ресурсов ЦП, памяти и системы хранения.
- Настраиваемые пользователем свойства.
- Параметры профиля компонента для параметризации схемы элементов.

Файлы OVF и OVA с несколькими компьютерами не поддерживаются.

Несколько важных моментов

- Поддерживаются файлы OVF и пакеты OVA.
- Поддерживается базовая проверка подлинности по имени пользователя и паролю для HTTP-сервера, на котором размещены файлы OVA или OVF. Указанный URL-адрес проверяется в схеме элементов.
- Файлы OVF и OVA не собираются данные из vCenter Server.
- Поддерживаются подписки EBS.
- Настраиваемые свойства можно определить при импорте параметров OVF, настраиваемых пользователем, в схеме элементов.
- Можно добавлять, изменять или удалять параметры, полученные из импорта файла OVF, когда запрашивается подготовка компьютера vSphere.
- Во время перенастройки компьютера можно добавлять, изменять или удалять параметры.

Определение параметров схемы элементов для компонента vSphere с помощью файла OVF

Из файла OVF можно импортировать параметры, чтобы упростить процесс настройки параметров компонента для компьютера vSphere в схеме элементов vRealize Automation.

Данная процедура предполагает, что вы в общих чертах знакомы с процессом создания схемы элементов vRealize Automation.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Обеспечьте выполнение остальных предварительных требований, описанных в разделе [Настройка схемы элементов компьютера](#).

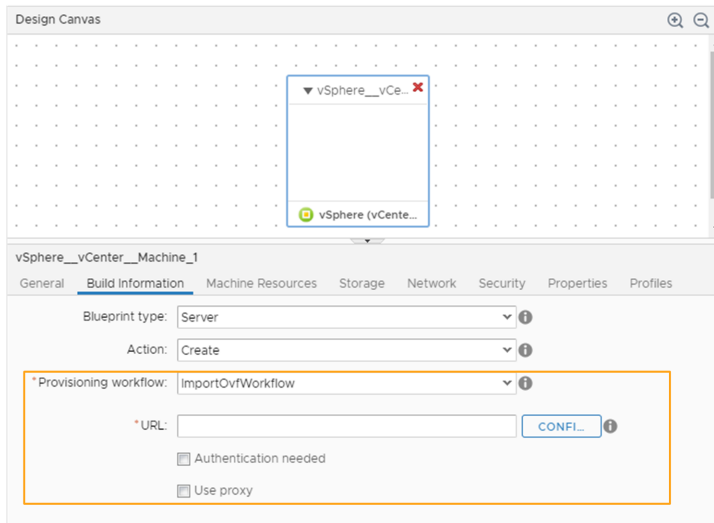
Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Выберите значок **Создать (+)**.
3. Введите имя и описание схемы элементов и нажмите **ОК**.
4. В области «Категории» щелкните **Типы компьютеров** и перетащите компонент **Компьютер vSphere (vCenter)** на холст проекта.

5. Откройте вкладку **Сведения о сборке** и задайте следующие параметры.

- **Тип схемы элементов:** сервер
- **Действие:** создать
- **Рабочий процесс подготовки:** ImportOvfWorkflow

При наличии параметра ImportOvfWorkflow становится доступным параметр **URL-адрес**.



6. Укажите расположение файла OVF.

- Введите путь к URL-адресу файла OVF в формате `https://сервер/папка/имя.ovf` или `имя.ova`.

При включении проверки подлинности на сервере, на котором размещен файл OVF, введите учетные данные для проверки подлинности пользователя.

- Если файл OVF размещен на веб-сайте, и создана конечная точка прокси-сервера для использования при доступе к веб-сайту, выберите **Использовать прокси-сервер** и укажите доступную конечную точку прокси-сервера.

7. Щелкните элемент **Настроить**.

Примечание Если появилось сообщение об ошибке проверки подлинности, значит, на сервере, на котором расположен файл OVF, требуется ввод учетных данных для проверки подлинности. Если такое сообщение появилось, установите флажок **Требуется проверка подлинности**, введите учетные данные (**Имя пользователя** и **Пароль**), которые необходимы для прохождения проверки подлинности на HTTP-сервере, где расположен файл OVF, после чего снова щелкните **Настроить**.

При выборе параметра «Настроить» открывается мастер и отображает все настраиваемые пользователем свойства и значения для импорта из файла OVF в качестве настраиваемых свойств. Если настраиваемые свойства для импорта отсутствуют, панель будет пустой.

- а) Используя данный мастер, либо примите значения по умолчанию, которые будут импортированы, либо измените эти значения для схемы элементов перед началом импорта.
- б) Нажмите кнопку **ОК**, чтобы импортировать свойства и значения.

Все настраиваемые пользователем свойства в шаблоне OVF импортируются в схему элементов как редактируемые настраиваемые свойства vRealize Automation, начиная со свойства VMware.Ovf, в то время как другие свойства импортируются как скрытые свойства, не предназначенные для редактирования после импорта.

8. Откройте вкладку **Ресурсы компьютера**, чтобы отобразить результаты импорта файла OVF, которые представлены записями с минимальными значениями для параметров **Процессоры**, **Память (МБ)** и **Хранилище (ГБ)**.

Любое из этих значений можно изменить после импорта.

9. Откройте вкладку **Хранилище**, чтобы отобразить результаты импорта файла OVF.
10. Последовательно откройте вкладки **Свойства > Настраиваемые свойства**, чтобы отобразить результаты импорта файла OVF.
11. Нажмите кнопку **Сохранить**.

Следующие шаги

Продолжите определение параметров схемы элементов либо нажмите кнопку **Готово**.

Определение набора значений образа для профиля компонента с помощью файла OVF

Можно импортировать параметры из файла OVF, чтобы создать один или несколько наборов значений для профиля компонентов образа, который будет использоваться в параметризованной схеме элементов vRealize Automation.

После импорта определений набора значений для профиля компонента **Image** можно добавить один набор значений или несколько таких наборов в профиль компонента для компьютера vSphere в схеме элементов. При запросе элемента каталога пользователи могут выбрать доступный **Image** и развертывание с использованием параметров, которые определены в наборе значений образа.

При импорте файла OVF настраиваемые пользователем свойства и значения в файле OVF не импортируются как настраиваемые свойства в набор значений. Если нужно использовать новые настраиваемые свойства из импортированного файла OVF для набора значений образа, необходимо вручную определить новые настраиваемые свойства в компоненте компьютера vSphere или всей схеме элементов. Настраиваемые свойства, созданные в параметризованной схеме элементов, должны применяться к набору значений для каждого образа профиля компонента.

Примечание Настраиваемые свойства OVF для vRealize Automation не применимы к настраиваемым свойствам OVF для vSphere. Рекомендуется создать один набор значений образа для vRealize Automation и один набор для vSphere.

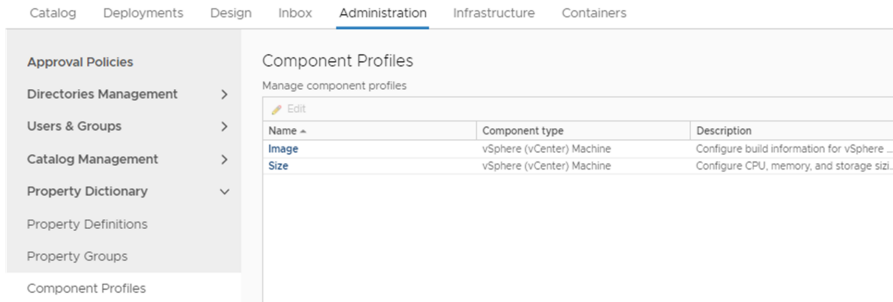
Дополнительные сведения об использовании профилей компонентов для параметризации схемы элементов см. в разделе [Общие сведения о параметризации схем элементов и ее использование](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве администратора с правами доступа **администратора арендатора и администратора инфраструктуры как услуги**.

Процедура

1. Выберите **Администрирование > Словарь свойств > Профили компонентов**.



2. Выберите **Image** в столбце «Имя».

Появится информация о свойстве компонента Image.

3. Перейдите на вкладку **Наборы значений**.

4. Чтобы определить новый набор значений, нажмите кнопку **Создать** и настройте параметры Image.

- а) Введите значение в поле **Отображаемое имя**, которое будет добавлено к разделителю ValueSet, например **ProdOVF**.
- б) Оставьте значение по умолчанию в текстовом поле **Имя** или введите настраиваемое имя.
- в) Введите описание, например **Параметры сборки для сценария клонирования А**, в текстовое поле **Описание**.
- г) В раскрывающемся меню **Состояние** выберите **Активно** или **Неактивно**.

При выборе варианта **Активно** набор значений будет отображаться в форме запроса на подготовку каталога.

- д) Выберите действие со сборкой **Создать**.
- е) В качестве типа схемы элементов выберите **Серверная** или **Настольная**.
- ж) Выберите рабочий процесс подготовки **ImportOvfWorkflow**.
- з) Введите путь к URL-адресу файла OVF в формате `https://сервер/папка/имя.ovf` или `имя.ova`.

- и) При включении проверки подлинности на сервере, на котором размещен файл OVF, введите учетные данные для проверки подлинности пользователя.
- к) Если файл OVF размещен на веб-сайте, и создана конечная точка прокси-сервера для использования при доступе к веб-сайту, выберите **Использовать прокси-сервер** и укажите доступную конечную точку прокси-сервера.

5. Нажмите кнопку **Сохранить**.

6. Закончив настройку параметров, нажмите кнопку **Готово**.

Следующие шаги

После создания образа и импорта файла OVF, чтобы определить набор значений образа, можно добавить образ в компонент компьютера vSphere в схеме элементов.

Использование компонентов контейнера в схемах элементов

Компоненты контейнера можно настроить и использовать в схеме элементов.

После того как администратор контейнера создал определения контейнера в Контейнеры для vRealize Automation, архитектор контейнера может добавлять и настраивать компоненты контейнера для схем элементов vRealize Automation на холсте проекта.

Настройки компонентов контейнера

Настройки и параметры схемы элементов для компонента контейнера Контейнеры для vRealize Automation можно задать на холсте проекта vRealize Automation.

Вкладка **Общие**

Настройте общие параметры для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-33. Настройки вкладки **Общие**

Параметр	Описание
Имя	Введите имя компонента контейнера в схеме элементов.
Описание	Составьте сводку по компоненту контейнера, чтобы ею было удобно пользоваться другим разработчикам архитектуры.
Образ	Введите полное имя образа в управляемом реестре (в частном реестре или реестре Docker Hub), например registry.hub.docker.com/library/python.
Команды	Введите команду, которая применяется к указанному образу, например python app.py. Команда выполняется при запуске процесса подготовки контейнера.
Ссылки	Ссылки — это еще один способ подключить контейнеры на одном узле или на нескольких узлах. Введите одну или несколько служб, с которыми этот контейнер должен быть связан, например redis или datadog.

Вкладка **Сеть**

Настройте параметры сети для компонента контейнера в схеме элементов на холсте проекта.

Контейнер можно подключить к сети. Сеть представлена как компонент сети контейнера на холсте проекта. Сведения о доступных сетях приведены на странице «Сеть» для формы компонента контейнера.

Таблица 3-34. Настройки вкладки **Сеть**

Параметр	Описание
Сети	Укажите существующие сети, которые определены для выбранного образа. Можно также создать новую сеть. Когда компонент контейнера сети добавляется в форму проекта, сети, которые указываются здесь, перечисляются как доступные для выбора варианты.
Привязки портов	Укажите привязки портов для выбранной сети. Привязки точек состоят из узла протокола, порта узла и порта контейнера.
Публиковать все порты	Установите флажок, чтобы сделать порты, которые используются в образе контейнера, доступными для всех пользователей.
Имя узла	Укажите имя узла контейнера. Если имя не указано, по умолчанию устанавливается имя компонента контейнера в схеме элементов.
Режим сети	Укажите сетевой стек контейнера. Если значение не указано, контейнер настраивается в режиме сети «Мост».

Вкладка **Хранилище**

Настройте параметры хранилища для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-35. Настройки вкладки **Хранилище**

Параметры	Описание
Тома	Укажите тома хранилищ, сопоставляемые из узла, который будет использоваться контейнером.
Тома из	Укажите тома хранилищ, которые будут унаследованы из другого контейнера.
Рабочий каталог	Укажите каталог, из которого будут выполняться команды.

Вкладка **Политика**

Настройте параметры политики, например политику развертывания и ограничения сходства, для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-36. Настройки вкладки **Политика**

Параметры	Описание
Политика развертывания	<p>Укажите политику развертывания, чтобы задать предпочтительные параметры относительно того, какой набор узлов будет использоваться для развертывания этого контейнера. Политики развертывания можно связать с узлами, политиками и определениями контейнера, чтобы задать предпочтительные узлы, политики и квоты при развертывании контейнера.</p> <p>Политику развертывания можно добавить на вкладке Контейнеры в vRealize Automation.</p>
Размер кластера	Укажите количество экземпляров, которые следует создать в качестве кластера из этого контейнера.
Политика перезапуска	Укажите политику перезапуска, регламентирующую порядок перезапуска контейнера при выходе.
Макс. запуск	Если в качестве политики перезапуска выбрано осуществление этого действия при сбое, можно указать максимальное количество перезапусков.
Доли ЦП	Укажите количество долей ЦП, выделенных для подготовленного ресурса.
Ограничение памяти	Укажите число от 0 до объема памяти, который доступен в зоне размещения. Это общий объем памяти, доступный для ресурсов в этом размещении. 0 означает отсутствие ограничений.
Подкачка памяти	Ограничение на суммарный объем памяти.
Ограничения сходства	<p>Определяет правила для подготовки контейнеров на одном и том же или разных узлах.</p> <ul style="list-style-type: none"> ■ Тип сходства <p>При отсутствии сходства контейнеры размещаются на разных узлах, в противном случае они размещаются на одном и том же узле.</p> ■ Служба <p>Имя службы, доступное в раскрывающемся меню, соответствует имени компонента контейнера, указанному в поле Имя на вкладке Общие.</p> ■ Ограничение <p>Жесткое ограничение указывает на то, что если ограничение не удовлетворяется, подготовка завершается сбоем. Гибкое ограничение указывает на то, что если ограничение не удовлетворяется, подготовка продолжается.</p>

Вкладка **Среда**

Настройте параметры среды, например привязки свойств, для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-37. Настройки вкладки **Среда**

Параметр	Описание
Имя	Имя переменной.
Привязка	Привяжите переменную к другому свойству, входящему в шаблон. При выборе привязки значение необходимо вводить, используя синтаксис <code>_resource~TemplateComponent~TemplateComponentProperty</code> .
Значение	Значение переменной среды или, если выбрана привязка, значение свойства, которое нужно привязать.

Вкладка «Свойства»

Настройте индивидуальные настраиваемые свойства или группы свойств для компонента контейнера в схеме элементов на холсте проекта.

Если открыть вкладку **Группы свойств** и щелкнуть **Добавить**, будут доступны следующие параметры.

- Свойства узла контейнера с проверкой подлинности при помощи сертификата
- Свойства узла контейнера с проверкой подлинности при помощи имени пользователя и пароля

Если определены дополнительные группы свойств, они также перечисляются.

Если открыть вкладку **Настраиваемые свойства** и щелкнуть **Добавить**, к компоненту контейнера можно будет добавить индивидуальные настраиваемые свойства.

Таблица 3-38. Настройки вкладки **Свойства** для настраиваемых свойств

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Как правило, это другой архитектор. Но если установить параметр «Показывать в запросе», бизнес-пользователи смогут просматривать и изменять значения свойств при выполнении запроса на элемент каталога.
Показывать в запросе	Если необходимо отображать имя свойства и его значение для конечных пользователей, можно выбрать отображение свойства в форме запроса во время запроса на подготовку компьютера. Если необходимо, чтобы пользователи указывали значение, нужно выбрать параметр Допускает переопределение .

Вкладка **Конфигурация работоспособности**

Укажите режим конфигурации работоспособности для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-39. Настройки вкладки **Конфигурация работоспособности**

Настройка режима	Описание
Нет	По умолчанию. Проверки работоспособности не настроены.
HTTP	<p>Если выбран параметр HTTP, необходимо указать API-интерфейс для доступа, а также используемые метод и версию HTTP. Интерфейс API относителен, поэтому не нужно вводить адрес контейнера. Кроме того, можно задать период времени ожидания для операции и установить пороговые значения работоспособности.</p> <p>Например, пороговое значение работоспособности 2 означает, что для того, чтобы контейнер считался работоспособным и имел состояние ЗАПУЩЕН, должно быть два последовательных успешных вызова. Пороговое значение неработоспособности 2 означает, что для того, чтобы контейнер считался неработоспособным и имел состояние ОШИБКА, должно быть два неуспешных вызова. В случае всех условий между пороговыми значениями работоспособности и неработоспособности контейнер имеет состояние СНИЖЕНИЕ ПРОИЗВОДИТЕЛЬНОСТИ.</p>
TCP-соединение	<p>Если выбран параметр TCP-соединение, необходимо ввести только порт для контейнера. При проверке работоспособности будет предпринята попытка установить TCP-соединение с контейнером в указанном порту. Кроме того, можно задать значение времени ожидания для операции и установить пороговые значения работоспособности и неработоспособности, как в случае с HTTP.</p>
Команда	<p>Если выбран параметр Команда, необходимо ввести команду, которая будет выполняться в контейнере. Успех проверки работоспособности определяется состоянием выхода команды.</p>
Пропускать проверку работоспособности при подготовке	<p>Снимите этот флажок, чтобы выполнять принудительную проверку работоспособности при подготовке. Если включена эта функция, контейнер не считается подготовленным до тех пор, пока он не пройдет хотя бы одну проверку работоспособности.</p>
Автоматическое развертывание	<p>Автоматическое повторное развертывание контейнеров, находящихся в состоянии ОШИБКИ.</p>

Вкладка **Конфигурация ведения журнала**

Укажите режим ведения журнала (и дополнительные параметры ведения журнала) для компонента контейнера в схеме элементов на холсте проекта.

Таблица 3-40. Настройки вкладки **Конфигурация ведения журнала**

Параметр	Описание
Драйвер	Выберите формат ведения журнала в раскрывающемся меню.
Параметры	Введите параметры драйвера, используя формат имени и значения, который отвечает формату ведения журнала.

Использование свойств и групп свойств контейнера в схеме элементов

Можно добавить предварительно определенные группы свойств в компонент контейнера схемы элементов vRealize Automation. Если компьютеры подготавливаются с использованием схемы элементов, которая содержит эти свойства, подготовленный компьютер регистрируется как хост-компьютер контейнера докера.

Контейнеры для vRealize Automation предоставляет следующие две группы настраиваемых свойств, связанных с контейнерами. При добавлении компонента контейнера в схему элементов можно добавить эти группы свойств в контейнер, чтобы зарегистрировать подготовленные машины как узлы контейнеров.

- Свойства узла контейнера с проверкой подлинности при помощи сертификата
- Свойства узла контейнера с проверкой подлинности при помощи имени пользователя и пароля

Чтобы просмотреть эти группы свойств в vRealize Automation, выберите элементы **Администрирование > Словарь свойств > Группы свойств**.

Поскольку группы свойств являются общими для всех арендаторов, если вы работаете в среде коллективной аренды, рекомендуется клонировать и настраивать свойства соответственно вашим требованиям. Давая уникальные имена группам свойств и свойствам в группах, вы сможете редактировать их, чтобы задавать собственные значения для использования в отдельных арендаторах.

Наиболее часто используемые свойства — `Container.Auth.PublicKey` и `Container.Auth.PrivateKey`. В них администраторы контейнеров используют сертификат клиента для проверки подлинности узла контейнеров.

Таблица 3-41. Настраиваемые свойства Containers

Свойство	Описание
<code>containers.ipam.driver</code>	Только для использования с контейнерами. Определяет, какой драйвер управления IP-адресами будет использоваться при добавлении компонента сети Containers в схему элементов. Набор поддерживаемых значений зависит от того, какие драйверы установлены в среде узла контейнера, в которой используются эти значения. Например, может использоваться поддерживаемое значение <code>infoblox</code> или <code>calico</code> в зависимости от того, какие подключаемые модули управления IP-адресами установлены на узле контейнера.
<code>containers.network.driver</code>	Только для использования с контейнерами. Определяет, какой сетевой драйвер будет использоваться при добавлении компонента сети Containers в схему элементов. Набор поддерживаемых значений зависит от того, какие драйверы установлены в среде узла контейнера, в которой используются эти значения. По умолчанию сетевые драйверы Docker включают <code>bridge</code> , <code>overlay</code> и <code>macvlan</code> , а сетевые драйверы Virtual Container Host (VCH) включают драйвер <code>bridge</code> . Также могут быть доступны сетевые драйверы от сторонних разработчиков, например <code>weave</code> и <code>calico</code> , в зависимости от того, какие подключаемые модули сети установлены на узле контейнера.
<code>Container</code>	Только для использования с контейнерами. Значение по умолчанию — <code>App.Docker</code> (обязательное значение). Не изменяйте это свойство.
<code>Container.Auth.User</code>	Только для использования с контейнерами. Указывает имя пользователя для подключения к узлу Containers.
<code>Container.Auth.Password</code>	Только для использования с контейнерами. Определяет, какой будет использоваться пароль: пароль для имени пользователя либо пароль открытого или закрытого ключа. Поддерживается зашифрованное значение свойства.
<code>Container.Auth.PublicKey</code>	Только для использования с контейнерами. Указывает открытый ключ для подключения к узлу Containers.
<code>Container.Auth.PrivateKey</code>	Только для использования с контейнерами. Указывает закрытый ключ для подключения к узлу Containers. Поддерживается зашифрованное значение свойства.
<code>Container.Connection.Protocol</code>	Только для использования с контейнерами. Указывает протокол связи. Значение по умолчанию — <code>API</code> (обязательное значение). Не изменяйте это свойство.
<code>Container.Connection.Scheme</code>	Только для использования с контейнерами. Указывает схему связи. Значение по умолчанию — <code>https</code> .
<code>Container.Connection.Port</code>	Только для использования с контейнерами. Указывает порт подключения Containers. Значение по умолчанию — <code>2376</code> .

Таблица 3-41. Настраиваемые свойства Containers (продолжение)

Свойство	Описание
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.MachineActivated	Только для использования с контейнерами. Указывает свойство брокера событий для отображения всех свойств Containers и используется для регистрации подготовленного узла. Значение по умолчанию — Container* (обязательное значение). Не изменяйте это свойство.
Extensibility.Lifecycle.Properties.VMPSMasterWorkf low32.Disposing	Только для использования с контейнерами. Указывает свойство брокера событий для отображения всех перечисленных выше свойств Containers и используется для отмены регистрации подготовленного узла. Значение по умолчанию — Container* (обязательное значение). Не изменяйте это свойство.

Использование компонентов сети Containers на холсте проекта

На холст проекта можно добавить один или несколько компонентов сети Containers и настроить их параметры для компонентов компьютера vSphere в схеме элементов.

Можно добавить `containers.ipam.driver` и `containers.network.driver` в компонент при его добавлении в схему элементов.

Добавление компонента «Сеть контейнера»

Можно добавить информацию о сети контейнера в схему элементов vRealize Automation, содержащую компоненты контейнера.

Контейнеры можно настроить в Контейнеры для vRealize Automation на вкладке **Контейнеры** vRealize Automation. Чтобы добавить эти контейнеры и их параметры сети как компоненты в схему элементов, используйте вкладку **Проектирование** в vRealize Automation.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор контейнеров**.
- Откройте новую или существующую схему элементов в холсте проекта с помощью вкладки **Проектирование**.

Процедура

1. Чтобы отобразить список доступных компонентов сети и безопасности, щелкните **Сеть и безопасность** в разделе «Категории» (Categories).
2. Перетащите на холст проекта компонент **Сеть контейнера**.
3. Чтобы добавить уникальную метку для компонента на холсте проекта, введите имя в текстовом поле **Имя**.
4. (дополнительно) В текстовом поле **Описание** введите описание компонента.
5. (дополнительно) Если не нужно задавать параметры для внешнего поставщика услуг управления IP-адресами, установите флажок **Внешний**.

После установки флажка **Внешний** исчезнет вкладка **Настройка управления IP-адресами**.

6. Выберите вкладку **Настройка управления IP-адресами**, чтобы задать новую или изменить существующую подсеть, диапазон IP-адресов и шлюз для сети, указанной в компоненте контейнера в схеме элементов.

Настройки управления IP-адресами применяются к новым сетям, которые создаются программой vRealize Automation, и не применяются к тем сетям, которые были ранее созданы в Docker или другом поддерживаемом приложении контейнера. Если эти настройки перекрываются с настройками других сетей, то они не проходят проверку и подготовка не выполняется. Например, в рамках одного узла контейнера должны использоваться уникальные подсеть и шлюз.

7. Выберите вкладку **Свойства**, чтобы задать настраиваемые свойства компонента.

Если открыть вкладку **Группы свойств** и щелкнуть **Добавить**, будут доступны следующие параметры.

- Свойства узла контейнера с проверкой подлинности при помощи сертификата
- Свойства узла контейнера с проверкой подлинности при помощи имени пользователя и пароля

Если определены дополнительные группы свойств, они также перечисляются.

Если открыть вкладку **Настраиваемые свойства** и щелкнуть **Добавить**, к компоненту контейнера можно будет добавить индивидуальные настраиваемые свойства.

Таблица 3-42. Настройки вкладки **Свойства** для настраиваемых свойств

Параметр	Описание
Имя	Введите имя настраиваемого свойства или выберите доступное настраиваемое свойство в раскрывающемся меню.
Значение	Введите или измените значение, которое нужно связать с именем настраиваемого свойства.
Зашифровано	При необходимости можно зашифровать значение свойства, например если значение — это пароль.
Допускает переопределение	Можно настроить возможность переопределения значения свойства следующим пользователем или последующими пользователями, которые будут использовать свойство. Как правило, это другой архитектор. Но если установить параметр «Показывать в запросе», бизнес-пользователи смогут просматривать и изменять значения свойств при выполнении запроса на элемент каталога.
Показывать в запросе	Если необходимо отображать имя свойства и его значение для конечных пользователей, можно выбрать отображение свойства в форме запроса во время запроса на подготовку компьютера. Если необходимо, чтобы пользователи указывали значение, нужно выбрать параметр Допускает переопределение .

8. Чтобы сохранить схему элементов как черновик или продолжить настройку схемы элементов, нажмите **Сохранить** или **Готово**.

Следующие шаги

Параметры сети контейнера можно добавить на вкладке **Сеть** компонента контейнера.

Отправка шаблонов контейнеров для использования в схемах элементов

Шаблон контейнера можно сделать доступным для использования в схеме элемента vRealize Automation.

Шаблон контейнера может включать несколько контейнеров. При отправке шаблона с несколькими контейнерами в vRealize Automation шаблон создается как многокомпонентная схема элементов в vRealize Automation.

Свойства отдельных контейнеров, которые добавляются в шаблон контейнера, распознаются в схеме элементов vRealize Automation. См. раздел [Использование свойств и групп свойств контейнера в схеме элементов](#).

При запросе на подготовку схемы элементов, опубликованной в каталоге vRealize Automation, подготавливается приложение исходного контейнера для этой схемы элементов.

В схему элементов vRealize Automation можно добавить и другие компоненты, в том числе компоненты таких типов:

- типы компьютеров;
- компоненты программного обеспечения;
- другие схемы элементов;
- компоненты сети NSX и безопасности;
- компоненты Все как услуга;
- настраиваемые компоненты.

Можно отправить шаблон из Containers в vRealize Automation. Изменения схемы элементов vRealize Automation не влияют на шаблон Containers.

Впоследствии можно внести изменения в шаблон Containers и снова отправить его, чтобы перезаписать схему элементов в vRealize Automation. В результате отправки шаблона в vRealize Automation схема элементов перезаписывается, а любые изменения схемы элементов в vRealize Automation, внесенные между отправками, будут потеряны. Чтобы не допустить потери изменений схемы элементов, используйте vRealize CloudClient для клонирования новой схемы элементов или экспорта схемы элементов.

Подготовка контейнера или узла Docker на основе схемы элементов

Схемы элементов vRealize Automation можно создавать и использовать для подготовки компьютеров в качестве зарегистрированных узлов контейнера Docker.

Чтобы подготовленный компьютер можно было зарегистрировать как узел контейнера, он должен соответствовать следующим требованиям:

- Подготовка компьютера осуществляется с помощью схемы элементов, содержащей настраиваемые свойства, которые характерны для Containers.

Необходимые настраиваемые свойства, зависящие от конкретного контейнера, предоставляются в виде двух групп свойств. См. раздел [Использование свойств и групп свойств контейнера в схеме элементов](#).

Дополнительные сведения об использовании настраиваемых свойств и групп свойств в vRealize Automation см. в разделе *Справочник по настраиваемым свойствам*.

- Компьютер доступен в сети.

К примеру, у компьютера должен быть действительный IP-адрес и он должен быть включен.

Можно определить схему элементов vRealize Automation, в которой будут содержаться конкретные настраиваемые свойства, позволяющие назначить компьютер в качестве узла контейнера при подготовке с помощью схемы элементов.

После успешной подготовки компьютера с необходимыми свойствами схемы элементов он регистрируется в Containers и принимает события и действия из vRealize Automation.

Создание схем элементов Microsoft Azure и включение действий ресурсов

Администратор облака или структуры может создавать схемы элементов виртуальной машины Microsoft Azure, которые администраторы бизнес-группы будут использовать в качестве структурных блоков, чтобы создавать настраиваемые подготовленные компьютеры для потребителей. Администраторы DevOps могут также создавать схемы элементов компьютера Azure либо использовать существующие схемы элементов компьютера Azure при создании составных схем элементов.

- [Создание схемы элементов для Microsoft Azure](#)

Можно создать схему элементов виртуальной машины Microsoft Azure для доступа к ресурсам виртуальной машины Azure.

- [Создание настраиваемых действий ресурсов Azure](#)

Для управления виртуальными машинами Azure можно создать и использовать настраиваемые действия ресурсов.

Создание схемы элементов для Microsoft Azure

Можно создать схему элементов виртуальной машины Microsoft Azure для доступа к ресурсам виртуальной машины Azure.

Шаблон виртуальной машины Azure по умолчанию отобразится в категории **Типы компьютеров** на странице редактирования схем элементов vRealize Automation. Этот шаблон виртуальной машины можно использовать как основу для схемы элементов Azure, как описано в процедуре ниже. После создания схемы элементов Azure ее можно опубликовать и развернуть в соответствии с проектом или ее можно использовать в сочетании с настраиваемыми ресурсами Azure либо с другими схемами элементов, чтобы создать составную схему элементов.

После создания и публикации схемы элементов пользователи с соответствующими правами могут запросить и подготовить экземпляр Azure с помощью vRealize Automation каталога служб.

Обратите внимание, что схемы элементов Azure определяют требования виртуальных машин. vRealize Automation использует эти требования для выбора наиболее подходящего резервирования для развертывания.

Для получения сведений о вкладке «Настройки и свойства NSX» в диалоговом окне «Новая схема элементов» см. раздел *Настройка vRealize Automation*.

Если необходимо одновременно создать две виртуальные машины из одного развертывания, нужно создать два имени сетевых интерфейсов и два имени виртуальных машин.

Примечание Не допускайте подготовки развертывания и Azure, и vSphere с помощью одного префикса именования, так как это может привести к повторяющимся именам в Azure и vSphere. В результате у некоторых пользователей могут возникнуть проблемы.

Необходимые условия

- Получите действительный идентификатор подписки Azure и связанные с ним сведения (группу ресурсов, учетную запись хранилища и сведения о виртуальной сети, которые могут понадобиться для создания схемы элементов).
- Настройте конечную точку Azure, чтобы создать подключение к Azure для использования с развертыванием vRealize Automation.
- Настройка резервирования Azure в соответствии с потребностями бизнес-групп.

Процедура

1. Выберите **Проектирование > Схемы элементов**.

2. Выберите значок **Создать (+)**.

3. В текстовом поле **Имя** введите имя схемы элементов.

Введенное имя также появится в текстовом поле **Идентификатор**. В большинстве случаев можно игнорировать вкладки **Настройки NSX** и **Свойства**.

4. Нажмите кнопку **ОК**.

5. Выберите пункт **Типы компьютеров** в меню «Категории».

6. Перетащите шаблон виртуальной машины **Компьютер Azure** на холст проекта.

Если настраиваемый ресурс Azure создан для использования в качестве основы для схемы элементов, этот ресурс можно выбрать из назначенной категории в списке «Категории».

7. Введите необходимые сведения о виртуальной машине Azure в текстовых полях на помеченных страницах, расположенных в нижней половине холста проекта, который отображается при перетаскивании шаблона виртуальной машины Azure на холст проекта.

Доступные для выбора варианты текстовых полей и прочих параметров на всех этих вкладках в основном зависят от конечной точки Azure, настроенной в качестве основы для схем элементов.

Для большинства параметров при щелчке на текстовом поле рядом с именем параметра с левой стороны страницы откроется новая панель. На этой панели можно ввести значения параметров в текстовом поле **Значение** и указать **обязательные** ли они. Обратите внимание, что в некоторых случаях необходимо также указать **Минимальное значение** и **Максимальное значение**. Нажмите кнопку **Применить** на правой панели, чтобы заполнить первоначальное текстовое поле.

Рис. 3-1. Меню с правой стороны схемы элементов Azure

Azure_Machine_1

General Build Information **Machine Resources** Storage Network Properties

Resource Group

● Resource Group: ☐ Create New ☒ Use Existing

● Resource Group Name: RG1-vAficionado

Availability Set

● Availability Set: ☒ None ☐ Create New ☐ Use Existing

Required: No

Value: RG1-vAficionado

Помимо этого, для большинства параметров существует кнопка **Дополнительные параметры**. Она позволяет задавать длину параметров и даже скрывать параметры от конечных пользователей.

Примечание Чтобы перейти к настройке схемы элементов, необходимо задать обязательные параметры на каждой вкладке. Чтобы оставить поле пустым, вернитесь назад и удалите запись перед сохранением.

Вкладка	Описание	Важные параметры
Общие	Выберите основные данные о подключении для виртуальной машины Azure, например конечную точку, которая будет использоваться.	<p>Идентификатор — определяет создаваемую виртуальную машину Azure. При изменении этого имени образ виртуальной машины Azure на холсте проекта также обновляется автоматически.</p> <p>Описание — определяет создаваемую виртуальную машину и указывает, обязательная ли она.</p> <p>Экземпляры — этот выбор позволяет создавать масштабируемую виртуальную машину. Используйте поля Минимум и Максимум, чтобы указать количество экземпляров Azure, которые можно создать с этой виртуальной машины.</p> <p>Проверка подлинности с помощью пароля: выберите «Да», чтобы выполнять проверку подлинности с помощью пароля, либо «Нет», чтобы использовать SSH.</p> <p>Имя пользователя администратора — оставьте это поле пустым, чтобы пользователь, выполняющий подготовку компьютера, мог сам назначить имя.</p> <p>Пароль администратора — оставьте это поле пустым, чтобы человек, выполняющий подготовку компьютера, мог задать необходимый пароль.</p>
Сведения о сборке	Позволяет указать сведения о создаваемой виртуальной машине.	<p>Расположение — выберите географическое расположение развертывания этой виртуальной машины.</p> <p>Префикс компьютера — выберите соответствующий переключатель, чтобы указать, следует ли использовать префикс компьютера из связанной бизнес-группы или создать настраиваемый префикс. Чтобы использовать настраиваемый префикс, введите его в текстовом поле Настраиваемый префикс компьютера.</p> <p>Тип образа виртуальной машины — выберите соответствующий переключатель для настраиваемого или резервного образа виртуальной машины. Настраиваемая виртуальная машина создается из классического развертывания Azure и предоставляет больше вариантов конфигурации для облачных служб, учетных записей хранилища и наборов доступности.</p> <p>Образ виртуальной машины — определяет образ виртуальной машины Azure, которая будет использоваться как основа для схемы элементов.</p> <ul style="list-style-type: none"> ■ Для резервного образа виртуальной машины его URN должен иметь такой формат: (издатель):(предложение):(sku):(версия). ■ Для управляемого диска URN образа машины должен соответствовать следующему формату: (ИмяГруппыРесурса):(ИмяНастраиваемогоОбраза) ■ Для настраиваемого образа виртуальной машины его URN должен иметь такой формат: <code>https://storageaccount.blob.core.windows.net/container/image.vhd</code> <p>Также для настраиваемого образа необходимо заполнить текстовое поле «Тип образа ОС (Windows или Linux)».</p> <p>Администратор — введите имя пользователя, назначенного в качестве администратора, которое настроено для виртуальных машин на основе этой схемы элементов. Либо можно оставить это поле пустым и заполнить его по запросу.</p>

Вкладка	Описание	Важные параметры
		<p>Проверка подлинности — выберите соответствующий переключатель, чтобы указать, требуется ли для виртуальной машины на основе этой схемы элементов проверка подлинности с помощью пароля или SSH.</p> <p>Пароль администратора — пароль администратора для экземпляра виртуальной машины.</p> <p>Серия — определяет общий размер экземпляра виртуальной машины. Сведения о серии см. в документации Azure на веб-странице https://azure.microsoft.com/ru-ru/documentation/articles/virtual-machines-windows-sizes/.</p> <p>Размер — определяет размер отдельного экземпляра виртуальной машины в серии. Размер относится к выбранной серии. При наличии допустимого подключения к экземпляру Azure доступные размеры заполняются динамически на основании подписки, а также выбранного расположения и серии. Сведения о размере см. в документации Azure.</p> <p>Сведения о размере экземпляра — дополнительные сведения о серии и размере экземпляра виртуальной машины.</p>

Вкладка	Описание	Важные параметры
Ресурсы компьютера	<p>Объедините ресурсы виртуальной машины в блоки. Группа ресурсов — это организационная структура, объединяющая ресурсы виртуальной машины, такие как веб-сайты, учетные записи, базы данных и сети.</p> <p>Набор доступности — это механизм управления двумя или более виртуальными машинами для обеспечения избыточности. Для получения дополнительной информации о наборах доступности Azure см. раздел https://azure.microsoft.com/en-us/documentation/articles/virtual-machines-windows-manage-availability/.</p> <hr/> <p>Примечание Если настраивается схема элементов, для параметра максимального количества экземпляров Azure которой установлено число больше 1, тогда следует использовать уже существующие группу ресурсов и набор доступности вместо того, чтобы создавать их. Использование новых групп ресурсов или наборов доступности в сразу в нескольких экземплярах в одном развертывании приведет к возникновению ошибок и других проблем, в случае связи с подсистемами балансировки нагрузки.</p>	<p>Создание или повторное использование группы ресурсов: выберите соответствующий переключатель, чтобы указать, следует ли использовать существующую группу ресурсов Azure или создать новую. Имя существующей группы ресурсов можно найти на странице «Группы ресурсов» на портале Azure. При создании новой группы ресурсов соответствующее имя новой группы автоматически отобразится в текстовом поле Группа ресурсов.</p> <p>Создание или повторное использование набора доступности: выберите соответствующий переключатель в зависимости от желаемого действия. При создании нового набора доступности соответствующие сведения о новом наборе доступности отобразятся в текстовом поле.</p>

Вкладка	Описание	Важные параметры
Хранилище	Позволяет выбрать для данной схемы элементов либо диск под управлением Azure, либо учетную запись хранения. В отношении управляемого диска Azure выполняет основные задачи по настройке конфигурации хранилища и его обслуживанию. Учетная запись хранения обеспечивает доступ к различным типам хранилищ Azure, например Azure Blob, таблица очереди и хранилище файлов. Для большинства схем элементов можно использовать значения по умолчанию.	<p>Тип хранилища — выберите, будет ли необходимо предоставить управляемый диск или учетную запись хранилища, управляемого вручную.</p> <ul style="list-style-type: none"> ■ При выборе управляемого диска нужно также в поле Тип диска ВМ выбрать, следует ли использовать диск класса премиум или стандартный диск. Остальные поля выбора можно игнорировать. ■ При выборе учетной записи хранения нужно в поле Учетная запись ОС для дискового хранилища ввести имя учетной записи хранилища для данной виртуальной машины. Диск с операционной системой виртуальной машины Azure разворачивается в этой учетной записи хранения. Информацию о группе хранения можно найти на портале Azure. Можно использовать одну или несколько учетных записей хранения. <p>Примечание Использование в именах учетных записей хранения символа подчеркивания и других специальных символов может привести к возникновению ошибок.</p> <p>Включить диагностику при загрузке — установите этот флажок, если в экземпляре Azure используются диагностические данные.</p> <p>Количество дисков с данными — укажите соответствующее количество дисковых накопителей для хранения данных, которые используются виртуальной машиной. Можно указать до четырех дисков. Эти диски используются в дополнение к диску с операционной системой, как указано в текстовом поле Учетная запись хранения.</p> <p>Номер дискового накопителя</p> <ul style="list-style-type: none"> ■ Имя диска — определяющее имя, назначенное диску. ■ Тип диска — тип накопителя. ■ Размер диска — размер накопителя. ■ Репликация — метод резервирования, используемый для создания резервной копии данных на диске. ■ Кэширование узла — указывает, следует ли кэшировать операции чтения/записи для увеличения производительности.

Вкладка	Описание	Важные параметры
Сеть	<p>Позволяет выбрать сеть для схемы элементов виртуальной машины. Для большинства схем элементов можно использовать значения по умолчанию, а потребитель сможет ввести соответствующие сведения о сети во время развертывания.</p> <p>Примечание Можно создать только одну виртуальную машину на интерфейс, но каждая виртуальная машина может использовать до четырех интерфейсов.</p>	<p>Щелкните таблицу, чтобы открыть справа диалоговое окно с другой редактируемой таблицей, которая содержит указанные ниже поля.</p> <ul style="list-style-type: none"> ■ Имя подсистемы балансировки нагрузки — подсистема балансировки нагрузки, которая используется экземпляром Azure. ■ Количество сетевых интерфейсов — укажите количество сетевых интерфейсов, которые используются экземпляром Azure. Количество сетевых интерфейсов должно поддерживаться размером виртуальной машины, как указано на вкладке «Хранилище». ■ Сетевой интерфейс — выберите соответствующий сетевой интерфейс для схемы элементов виртуальной машины. Если указать существующую сеть, то все остальные вкладки сети можно игнорировать. Если ввести имя несуществующего сетевого интерфейса, будет создан новый сетевой интерфейс с таким именем, который можно будет настроить с помощью прочих вкладок сети. ■ Префикс имени сетевого адаптера — префикс для сетевого адаптера. ■ Тип IP-адреса — указывает, какой тип IP-адреса используется виртуальной машиной: статический или динамический. ■ Конфигурация сети — укажите соответствующую конфигурацию сети. Поддерживаются профили сети. Есть два варианта: Указать сети Azure или Использовать профиль сети. Последующие поля зависят от выбора одного из этих вариантов . <ul style="list-style-type: none"> ■ Далее описаны параметры, доступные в случае выбора варианта Указать сети Azure. Если оставить эти текстовые поля незаполненными, будут использоваться сетевые структуры по умолчанию в зависимости от сведений, указанных в применимом резервировании. <ul style="list-style-type: none"> ■ Имя виртуальной сети — имя виртуальной сети. ■ Имя подсети — доменное имя подсети Azure. <p>Примечание Задать публичный IP-адрес для Azure можно в рамках операций дня 2.</p> <ul style="list-style-type: none"> ■ Если выбрать вариант Использовать профиль сети, конфигурация сети отделяется от базовых структур Azure и объединяется с профилем сети vRealize Automation. <ul style="list-style-type: none"> ■ Если оставить текстовое поле Профиль сети пустым, пара виртуальной сети и подсети Azure по умолчанию обрабатывается на основе применимых резервирований, в которых указан профиль сети. ■ Если указать профиль сети, виртуальная сеть и подсеть Azure обрабатываются на основе совпадающих резервирований.
Свойства	<p>Позволяет добавлять настраиваемые свойства в схему элементов. Применяемые здесь настраиваемые свойства можно переопределить</p>	<p>Есть два варианта добавления настраиваемых свойств, они представлены двумя вкладками в диалоговом окне «Свойства».</p>

Вкладка	Описание	Важные параметры
	свойствами, назначенными позже в цепочке приоритетов. Дополнительные сведения о порядке приоритетов настраиваемых свойств см. в разделе <i>Справочник по настраиваемым свойствам</i> .	<ul style="list-style-type: none"> ■ Группы свойств: это многоуровневые группы, которые упрощают процесс добавления настраиваемых свойств. Существуют четыре параметра для выбора групп свойств. <ul style="list-style-type: none"> ■ Добавить — позволяет добавить доступную группу свойств в схему элементов. ■ Переместить вверх или вниз — позволяет управлять приоритетом групп свойств. Первая группа в списке имеет наивысший приоритет, а ее настраиваемые свойства наиболее приоритетны. ■ Просмотр свойств — позволяет просмотреть настраиваемые свойства в выбранной группе. ■ Просмотр объединенных свойств — если настраиваемое свойство входит в несколько групп свойств, более высокий приоритет имеет значение, которое входит в группу свойств с наивысшим приоритетом. Просмотр таких объединенных свойств помогает в определении приоритетов групп свойств. ■ Настраиваемые свойства: эта вкладка используется для добавления отдельных настраиваемых свойств. <ul style="list-style-type: none"> ■ Создать — позволяет добавить отдельное настраиваемое свойство в схему элементов. ■ Имя — введите имя для определения свойства. Список настраиваемых свойств и их определения см. в разделе <i>Справочник по настраиваемым свойствам</i>. ■ Значение — введите значение для настраиваемого свойства. ■ Зашифровано — это свойство можно зашифровать. ■ Допускает переопределение — можно указать, что значение свойства может быть переопределено следующим или последующим пользователем. Как правило, это другой архитектор. Но если установить параметр «Показывать в запросе», бизнес-пользователи смогут просматривать и изменять значения свойств при выполнении запроса на элемент каталога. ■ Показывать в запросе. Если необходимо отображать имя свойства и его значение для конечных пользователей, можно выбрать отображение свойства в форме запроса во время запроса на подготовку компьютера. Если необходимо, чтобы пользователи указывали значение, нужно выбрать параметр «Допускает переопределение».

8. Нажмите кнопку **Готово**, чтобы сохранить конфигурацию схемы элементов и вернуться на главную страницу «Схемы элементов».

Следующие шаги

Если в резервировании Azure заданы настраиваемые свойства для поддержки туннеля VPN, можно добавить компоненты программного обеспечения в схемы элементов Azure.

1. В меню «Категории» выберите **Компоненты программного обеспечения**. В области ниже появятся компоненты программного обеспечения, настроенные в схемах элементов Azure.

2. В раскрывающемся списке значений контейнера выберите виртуальную машину Azure.
3. Выберите нужный компонент программного обеспечения и перетащите его в виртуальную машину Azure на холст проекта.
4. Если для компонента программного обеспечения требуются какие-либо свойства, введите их в соответствующие текстовые поля параметров под холстом проекта.
5. Нажмите кнопку **Сохранить**.

Чтобы опубликовать схему элементов, выберите ее на главной странице «Схемы элементов» и нажмите кнопку **Опубликовать**. Опубликованная схема элементов будет доступна на странице «Элементы каталога». Также, диспетчер бизнес-групп или пользователь с эквивалентными правами может использовать опубликованную схему элементов как основу для составной схемы элементов.

Создание настраиваемых действий ресурсов Azure

Для управления виртуальными машинами Azure можно создать и использовать настраиваемые действия ресурсов.

Реализация vRealize Automation Azure предоставляется с двумя настраиваемыми действиями ресурсов по умолчанию:

- Запуск виртуальной машины
- Остановка виртуальной машины

Кроме того, настраиваемые действия ресурсов можно создать с помощью рабочих процессов, доступных через библиотеку vRealize Orchestrator в интерфейсе vRealize Automation.

С действиями ресурсов Azure можно работать так же, как и с другими действиями ресурсов «Все как услуга» в vRealize Automation. Подробнее о действиях ресурсов см. в разделах *Создание схем элементов и действий ресурсов «Все как услуга»* и *Интеграция vRealize Orchestrator в vRealize Automation* в *Настройка vRealize Automation*.

Необходимые условия

Настройте допустимую конечную точку Azure для своего развертывания vRealize Automation.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Нажмите кнопку **Создать**.
3. Перейдите к **Orchestrator > Библиотека > Azure** в библиотеке рабочих процессов vRealize Orchestrator.
4. Выберите необходимую папку и рабочий процесс.
5. Настройте необходимое для себя действие, как любое другое действие ресурсов «Все как услуга».

Добавление возможности управления конфигурацией в схемы элементов vSphere

Можно добавить в схемы элементов vSphere специальные компоненты для поддержки управления конфигурацией виртуальных машин vSphere.

vRealize Automation поддерживает добавление в схемы элементов vSphere функций Puppet и Ansible для управления конфигурацией.

Средства управления конфигурацией на основе Puppet для определения и контроля конфигураций программного обеспечения обычно используют роли и среды на основе приложения Puppet Enterprise. Следует помнить, что значения роли и среды в среде Puppet отличаются от значений, общепринятых в ИТ-отрасли.

Управление конфигурацией Ansible основано на шаблонах заданий, определяемых в реализации Ansible Tower. Можно выбрать несколько шаблонов и изменить их порядок. Эти шаблоны можно запустить после развертывания компьютера, но до его удаления из vRealize Automation.

Конечная точка устанавливает соединение с существующим корпоративным развертыванием Puppet или Ansible. После создания конечной точки vRealize Automation получает соответствующую информацию из указанных развертываний. При настройке Puppet или Ansible с поддержкой схемы элементов виртуальной машины можно указать режим ранней или поздней привязки.

Примечание Компоненты Puppet и Ansible в настоящее время поддерживаются только в схемах элементов и виртуальных машинах vSphere.

Добавление компонента Puppet в схему элементов vSphere

Можно добавить компонент управления конфигурацией Puppet в схему элементов vSphere, чтобы упростить принудительное управление виртуальными машинами vSphere с помощью главного узла Puppet.

При добавлении компонента Puppet в схему элементов vSphere агент Puppet добавляется на виртуальные машины, созданные на основе этой схемы элементов.

При создании схем элементов vSphere с поддержкой Puppet необходимо указать, следует ли создавать конфигурацию с ранним или поздним связыванием.

Если используется раннее связывание, пользователь определяет роль компонента Puppet и настройки среды для всех виртуальных машин, созданных на основе конкретной схемы элементов в момент добавления компонента Puppet в эту схему элементов. Эти настройки не изменяются на протяжении всего жизненного цикла схемы элементов. Выполнить позднюю привязку можно несколькими способами.

- Оставьте текстовые поля **Среда Puppet** и **Роль Puppet** пустыми в схеме элементов, и пользователи настроят эти параметры во время оформления запроса.
- Задайте параметр **Среда Puppet**, а поле **Роль Puppet** оставьте пустым. Пользователи зададут роль во время оформления запроса.

Необходимые условия

Создайте соответствующую схему элементов vSphere. Дополнительные сведения см. в разделе [Настройки компонентов компьютера vSphere в vRealize Automation](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Выберите **Управление конфигурацией** в меню «Категории» на странице проекта схемы элементов.
3. Выберите компонент Puppet и перетащите его в компонент vSphere на холсте проекта.
4. На вкладке «Общие» в нижней части страницы укажите **Идентификатор** и **Описание** для компонента Puppet.

Идентификатор и описание указываются в произвольной форме.

5. Откройте вкладку «Сервер».
6. Щелкните раскрывающееся меню и выберите соответствующий главный узел Puppet для схемы элементов.
7. Выберите соответствующую **среду Puppet** и **роль Puppet**, чтобы использовать для этого компонента раннее связывание.

Чтобы настроить раннее связывание, выберите среду и роль Puppet. Чтобы создать компонент с поздним связыванием, выберите элемент **Среда Puppet** или оставьте текстовые поля **Среда Puppet** и **Роль Puppet** пустыми и установите флажки **Задать в форме запроса**.

Примечание Флажки **Задать в форме запроса** связаны друг с другом. Если один из этих флажков устанавливается вручную, второй устанавливается автоматически.

8. Нажмите кнопку **Готово**, чтобы сохранить конфигурацию компонента Puppet и вернуться на главную страницу проекта схемы элементов.

Добавление компонента Ansible к схеме элементов vSphere

Можно добавить в схему элементов vSphere компонент управления конфигурацией Ansible, чтобы упростить принудительное управление виртуальными машинами vSphere с помощью средства Ansible Tower.

Добавление компонента Ansible в схему элементов vSphere позволяет средству Ansible Tower устанавливать связь с развернутыми ресурсами и выполнять на них различные команды.

Необходимые условия

Создайте соответствующую схему элементов vSphere. Дополнительные сведения см. в разделе [Настройки компонентов компьютера vSphere в vRealize Automation](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Выберите **Управление конфигурацией** в меню «Категории» на странице проекта схемы элементов.
3. Выберите компонент Ansible и перетащите его в компонент vSphere на холсте проекта.

4. На вкладке «Общие» в нижней части страницы укажите **Идентификатор** и **Описание** для компонента Ansible.

Идентификатор и описание указываются в произвольной форме.

5. Перейдите на вкладку сведений и введите необходимую информацию об Ansible Tower, проекте и шаблоне.

- а) Выберите нужный элемент **Ansible Tower** и **организацию**, которая будет использовать этот компонент.
- б) Настройте для компонента Ansible раннюю или позднюю привязку.
 - Если нужно использовать для этого компонента раннюю привязку, выберите соответствующий **проект** и **шаблон задания**. В текстовом поле **Шаблон задания удаления** выберите шаблон, который нужно запустить при уничтожении компьютера. Не устанавливайте флажки **Задать в форме запроса**. Также выберите нужную среду и роль Ansible.
 - Если нужно создать компонент с поздней привязкой, можно установить флажки **Задать в форме запроса** и не задавать значения для полей **Проект**, **Шаблон задания** и **Шаблон задания удаления**.

Примечание Флажки **Задать в форме запроса** связаны друг с другом. При выборе одного флажка остальные выбираются автоматически. Это происходит потому, что поле **Проект** работает как фильтр для шаблонов заданий. При выборе проекта список шаблонов заданий автоматически фильтруется по указанному проекту. Поэтому, если выбрать для проекта режим **Задать в форме запроса**, следующие два поля выбираются автоматически.

6. Нажмите кнопку **Готово**, чтобы сохранить конфигурацию компонента Ansible и вернуться на главную страницу проекта схемы элементов.

Добавление поддержки подключения к удаленному рабочему столу (RDP) к схемам элементов компьютера Windows

Чтобы разрешить администраторам каталога назначать пользователям права на действие «Подключиться с помощью RDP» для схем элементов Windows, необходимо добавить настраиваемые свойства RDP в схему элементов и создать ссылку на файл RDP, подготовленный администратором системы.

Примечание Если администратор структуры создает группу свойств, которая содержит требуемые настраиваемые свойства, а вы добавляете эту группу в схему элементов, вам не нужно отдельно добавлять настраиваемые свойства в схему элементов.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора арендатора** или **диспетчера бизнес-групп**.
- Получите имя настраиваемого RDP-файла, созданного системным администратором. См. раздел [Создание настраиваемого RDP-файла для поддержки подключений RDP для подготовленных компьютеров](#).

- Создайте по крайней мере одну схему элементов компьютера Windows.

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Наведите указатель мыши на схему элементов, которую нужно обновить, и нажмите кнопку **Изменить**.
3. На холсте выберите компонент компьютера, чтобы изменить сведения.
4. Перейдите на вкладку **Свойства**.
5. Перейдите на вкладку **Настраиваемые свойства**.
6. Настройте параметры RDP.
 - а) Щелкните **Новое свойство**.
 - б) Введите имена настраиваемых свойств RDP в текстовом поле **Имя** и соответствующие значения в текстовом поле **Значение**.

Параметр	Описание и значение
VirtualMachine.Rdp.File	Указывает RDP-файл, из которого нужно получить параметры, например <code>My_RDP_Settings.rdp</code> . Файл должен находиться в подкаталоге <code>Website\Rdp</code> каталога установки vRealize Automation.
VirtualMachine.Rdp.SettingN	Указывает параметры RDP, которые нужно использовать при открытии ссылки RDP на компьютер. <i>N</i> — это уникальный номер, который используется для отличия одного параметра RDP от другого. Например, чтобы указать уровень проверки подлинности RDP, не указывая отдельные требования к проверке подлинности, задайте настраиваемое свойство <code>VirtualMachine.Rdp.Setting1</code> и укажите значение <code>authentication level:i:3</code> . Дополнительные сведения о доступных настройках RDP и об их корректном синтаксисе см. в документации Microsoft Windows по RDP, например Настройки RDP для служб удаленного рабочего стола на сервере Windows .
VirtualMachine.Admin.NameCompletion	Указывает имя домена, которое нужно включить в полное доменное имя компьютера, которое создают RDP- или SSH-файлы при действии параметра Подключиться с помощью RDP или Подключиться с помощью SSH . Например, задайте значение для переменной <code>myCompany.com</code> , чтобы создать полное доменное имя <code>my-machine-name.myCompany.com</code> в RDP- или SSH-файле.

- в) Нажмите кнопку **Сохранить**.
7. Выберите строку схемы элементов и нажмите кнопку **Опубликовать**.

Результаты

Администраторы каталога могут предоставлять пользователям право на действие **«Подключиться с помощью RDP»** для компьютеров, подготовленных с помощью вашей схемы элементов. Если пользователи не имеют права на это действие, они не могут подключаться с помощью RDP.

Добавление средства очистки Active Directory в схему элементов CentOS

Разработчики архитектуры инфраструктуры как услуги могут настроить vRealize Automation для очистки среды Active Directory после удаления подготовленных компьютеров из гипервизоров. Для настройки подключаемого модуля очистки Active Directory вносятся изменения в схему.

При использовании подключаемого модуля очистки Active Directory можно задать следующие действия с учетной записью Active Directory, которые производятся при удалении компьютера из гипервизора.

- Удалить учетную запись AD
- Деактивировать учетную запись AD
- Переименовать учетную запись AD
- Переместить учетную запись AD в другую организационную единицу (OU) AD

Необходимые условия

Примечание Эта информация не распространяется на Amazon Web Services.

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Соберите следующую информацию о среде Active Directory.
 - имя пользователя учетной записи и пароль Active Directory с правами на удаление, деактивацию, переименование или перемещение учетных записей Active Directory; имя пользователя необходимо указывать в формате domain\username;
 - (необязательно) имя подразделения, куда перемещаются удаленные компьютеры;
 - (необязательно) префикс, добавляемый к имени удаленного компьютера.
- Создайте схему элементов компьютера. См. раздел [Настройка схемы элементов компьютера](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Наведите указатель мыши на схему элементов и нажмите **Изменить**.
3. Выберите на холсте компонент компьютера, чтобы отобразилась вкладка «Сведения».
4. Перейдите на вкладку **Свойства**.
5. Нажмите вкладку **Настраиваемые свойства** для настройки подключаемого модуля очистки Active Directory.
 - а) Щелкните **Новое свойство**.
 - б) В текстовом поле **Имя** введите Plugin.AdMachineCleanup.Execute.
 - в) В текстовом поле **Значение** введите **true**.
 - г) Щелкните значок **Сохранить** (✔).

6. Настройка подключаемого модуля очистки Active Directory путем добавления настраиваемых свойств.

Параметр	Описание и значение
Plugin.AdMachineCleanup.UserName	Введите имя пользователя учетной записи Active Directory в текстовом поле Значение . У этого пользователя должны быть права на удаление, деактивацию, перемещение и переименование учетных записей Active Directory. Имя пользователя необходимо указывать в формате domain\username.
Plugin.AdMachineCleanup.Password	Введите пароль для учетной записи Active Directory в текстовом поле Значение .
Plugin.AdMachineCleanup.Delete	Задайте значение «Истина», чтобы не отключать учетные записи уничтоженных компьютеров, а удалить их.
Plugin.AdMachineCleanup.MoveToOu	Перемещает учетную запись уничтоженных компьютеров в новую организационную единицу Active Directory. Это значение — это организационная единица, в которую перемещается учетная запись. Запись должна быть в формате <i>ou=OU, dc=dc</i> , например <i>ou=trash,cn=computers,dc=lab,dc=local</i> .
Plugin.AdMachineCleanup.RenamePrefix	Переименовывает учетные записи уничтоженных компьютеров путем добавления префикса. Значение — это строка префикса, которую нужно поставить в начало, например <i>destroyed_</i> .

7. Нажмите кнопку **ОК**.

Результаты

Всякий раз, когда компьютеры, подготовленные с помощью схемы элементов, будут удаляться из гипервизора, среда Active Directory будет обновляться.

Предоставление запросившим сторонам возможности указывать имя узла компьютера

Как разработчик архитектуры схемы элементов вы хотите предоставить пользователям возможность выбора имен компьютеров, когда они запрашивают схемы элементов. Для этого необходимо изменить схему: добавить настраиваемое свойство «Имя узла» и настроить его так, чтобы пользователям предлагалось ввести значение при обработке их запросов.

Примечание Если администратор структуры создает группу свойств, которая содержит требуемые настраиваемые свойства, а вы добавляете эту группу в схему элементов, вам не нужно отдельно добавлять настраиваемые свойства в схему элементов.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Создайте схему элементов компьютера. См. раздел [Настройка схемы элементов компьютера](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Наведите указатель мыши на схему элементов и нажмите **Изменить**.
3. Выберите на холсте компонент компьютера, чтобы отобразилась вкладка «Сведения».

4. Перейдите на вкладку **Свойства**.
5. Щелкните **Новое свойство**.
6. Введите **Имя узла** в текстовом поле **Имя**.
7. Оставьте текстовое поле **Значение** пустым.
8. Настройте vRealize Automation так, чтобы пользователям предлагалось ввести значение при обработке запроса.
 - а) Установите флажок **Допускает переопределение**.
 - б) Выберите **Показывать в запросе**.

Так как имена узлов должны быть уникальными, пользователи могут запрашивать из этой схемы элементов только один компьютер в конкретный момент времени.

9. Щелкните значок **Сохранить** (✓).
10. Нажмите кнопку **ОК**.

Результаты

Пользователи, запрашивающие компьютеры из вашей схемы элементов, должны указать имя узла для своего компьютера. vRealize Automation проверяет, что указанное имя узла является уникальным.

Предоставление пользователям возможности выбирать расположение центра обработки данных при развертываниях в нескольких регионах

Если разработчику схемы элементов требуется предоставить пользователям две инфраструктуры для подготовки компьютеров на выбор — бостонскую или лондонскую, — необходимо изменить схему, чтобы включить функцию определения расположения.



При наличии центра обработки данных в Лондоне и Бостоне нельзя, чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Лондона и наоборот. Чтобы пользователи в Бостоне подготавливали компьютеры в инфраструктуре Бостона, а пользователи Лондона — в инфраструктуре Лондона, необходимо разрешить пользователям выбирать соответствующее расположение для подготовки при запросе компьютеров.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.

- Определите расположение центров обработки данных, используя права системного администратора. См. раздел [Сценарий: добавление данных о расположении центра обработки данных при развертываниях в нескольких регионах](#).
- Примените соответствующие расположения к вычислительным ресурсам в качестве администратора структуры. См. раздел [Сценарий: применение размещения к вычислительному ресурсу при развертываниях в нескольких регионах](#).
- Создайте схему элементов компьютера. См. раздел [Настройка схемы элементов компьютера](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Наведите указатель мыши на схему элементов и нажмите **Изменить**.
3. Чтобы открыть вкладку **Общие сведения**, на холсте выберите компонент компьютера.
4. Установите флажок **Отобразить расположение по запросу**.
5. Щелкните элемент **Готово**.
6. Наведите указатель мыши на схему элементов и нажмите **Опубликовать**.

Результаты

Теперь, когда пользователи бизнес-групп запрашивают подготовку компьютера на основе схемы элементов, отображается запрос на выбор расположения центра обработки данных.

Проектирование компонентов Программное обеспечение

Программный архитектор может создавать повторно используемые программные компоненты, стандартизируя свойства конфигурации и используя сценарии действий для точного указания того, как компоненты устанавливаются, настраиваются, удаляются или обновляются при масштабировании развертывания. Можно переписывать эти сценарии действий в любое время и сразу публиковать их для внедрения изменений в подготовленные программные компоненты.

Можно проектировать сценарии действий так, чтобы они были универсальными и допускали повторное использование, определяя и используя пары имен и значений, называемые программными свойствами, и передавая их в качестве параметров в сценарии действий. Если у программных свойств есть неизвестные значения или значения, которые будут определены в будущем, можно сделать предоставление этих значений обязательным требованием или возможностью для других архитекторов схем элементов или конечных пользователей. Если в схеме элементов требуется значение из другого компонента, например IP-адрес компьютера, можно привязать программное свойство к IP-адресу этого компьютера. Использование программных свойств для параметризации сценариев действий делает их универсальными и доступными для повторного использования, поэтому можно развертывать программные компоненты в различных средах без изменения сценариев.

Таблица 3-43. Действия жизненного цикла

Действия жизненного цикла	Описание
Установка	Установка программного обеспечения. Например, можно скачать установочный файл сервера Tomcat и установить службу Tomcat. Сценарии, написанные для действий жизненного цикла, запускаются при первой подготовке программного обеспечения (во время первоначального запроса на развертывание или в ходе увеличения масштаба).
Настройка	Настройка программного обеспечения. Для примера Tomcat можно задать сценарии JAVA_OPTS и CATALINA_OPTS. Сценарии настройки запускаются после завершения действий установки.
Запуск	Запуск программного обеспечения. Например, можно запустить службу Tomcat с помощью команды запуска на сервере Tomcat. Сценарии запуска запускаются после завершения действий настройки.
Обновление	Если проектируется программный компонент для поддержки масштабируемых схем элементов, обрабатывайте все обновления, необходимые после операции увеличения или уменьшения масштаба. Например, можно изменить размер кластера для масштабируемого развертывания и управлять узлами кластера с помощью подсистемы балансировки нагрузки. Проектируйте сценарии обновления для многократного запуска (без изменений) и обрабатывайте оба случая масштабирования (увеличение и уменьшение масштаба). После выполнения операции масштабирования сценарии обновления запускаются на всех зависимых программных компонентах.
Удаление	Удаление программного обеспечения. Например, можно выполнять особые действия в приложении перед удалением развертывания. Сценарии удаления запускаются каждый раз при удалении компонентов.

На портале VMware Solution Exchange можно загрузить предварительно настроенные компоненты Программное обеспечение для разнообразных служб и приложений промежуточного слоя. С помощью интерфейса REST API vRealize CloudClient или vRealize Automation можно программно импортировать предварительно настроенные компоненты Программное обеспечение в экземпляр vRealize Automation.

- Сведения о посещении портала VMware Solution Exchange см. в разделе https://solutionexchange.vmware.com/store/category_groups/cloud-management.
- Сведения об интерфейсе REST API vRealize Automation см. в документах *Руководство по программированию* и *API-интерфейс службы содержимого vRealize Automation* на сайте <https://code.vmware.com>.
- Сведения о vRealize CloudClient см. в разделе <https://developercenter.vmware.com/tool/cloudclient>.

Типы свойств и параметры настройки

Можно проектировать сценарии действий так, чтобы они были универсальными и допускали повторное использование, определяя и используя пары имен и значений, называемые программными свойствами, и передавая их в качестве параметров в сценарии действий. Можно создавать программные свойства, которые ожидают значения типа «строка», «массив», «содержимое», «логическое» или «целое число». Можно указывать значение самостоятельно, запрашивать кого-либо предоставить значение или получать значение от другого компонента схемы элементов путем создания привязки.

Параметры свойств

Чтобы вычислить значение любого свойства строкового типа, установите флажок «Вычисляемое». Чтобы сделать любое свойство зашифрованным, обязательным или допускающим переопределение, установите соответствующие флажки во время настройки свойств Программное обеспечение. Укажите для этих параметров значения в зависимости от цели. Например, вам необходимо потребовать от архитекторов схем элементов предоставить значение для пароля и зашифровать это значение, когда они используют ваш программный компонент в схеме элементов. Создайте свойство пароля, но оставьте текстовое поле пустым. Выберите «Допускает переопределение», «Обязательно» и «Зашифровано». Если ожидаемый пароль принадлежит конечному пользователю, архитектор схем элементов может выбрать параметр **Показывать в запросе**, чтобы требовать от пользователей ввода пароля при заполнении формы запроса.

Параметр	Описание
Зашифровано	Пометьте свойства как зашифрованные, чтобы скрыть значение. Оно будет отображаться в виде звездочек в vRealize Automation. Если изменить пометку свойства с «Зашифрованное» на «Незашифрованное», vRealize Automation сбросит значение свойства. Из соображений безопасности для свойства нужно задать новое значение.
Допускает переопределение	Если выбрать этот параметр, архитекторы смогут изменять значение этого свойства при сборке схемы элементов приложения. Если ввести значение, оно отобразится в качестве значения по умолчанию.
Обязательно	Если выбрать этот параметр, архитекторам потребуется указать значение этого свойства или принять предоставляемое значение по умолчанию.
Вычисляемое	Значения вычисляемых свойств назначаются сценариями жизненного цикла INSTALL, CONFIGURE, START или UPDATE. Назначенное значение распространяется на последующие доступные этапы жизненного цикла и компоненты, которые связаны с этими свойствами в схеме элементов. Если выбрать для нестрокового свойства тип «Вычисляемое», тип свойства станет строковым.

При выборе параметра свойства «Вычисляемое» нужно оставить поле значения для настраиваемого свойства пустым. Создайте сценарии для вычисленных значений.

Таблица 3-44. Примеры сценариев для параметра вычисляемого свойства

Образец строкового свойства	Синтаксис сценария	Пример использования
my_unique_id = ""	Bash — \$my_unique_id	export my_unique_id="0123456789"
	Windows CMD — %my_unique_id%	set my_unique_id=0123456789
	Windows PowerShell — \$my_unique_id	\$my_unique_id = "0123456789"

Свойство типа «строка»

Строковые свойства ожидают получить строковые значения. Можно указывать строковое значение самостоятельно, требовать от кого-либо предоставить значение или получать значение от другого компонента схемы элементов путем создания привязки к другому строковому свойству. Строковые значения могут содержать любые символы ASCII. Для создания привязки к свойству используйте вкладку **Свойства** на холсте схемы элементов, чтобы выбрать соответствующее свойство для привязки. Затем значение свойства передается в сценарии действий в виде необработанных строковых данных. Когда выполняется привязка к строковому свойству схемы элементов, убедитесь, что компонент схемы элементов, к которому выполняется привязка, не относится к кластеру. Если компонент относится к кластеру, строковое значение становится массивом и получается неожиданное значение.

Образец строкового свойства	Синтаксис сценария	Пример использования
admin_email = "admin@email987.com"	Bash — \$admin_email	echo \$admin_email
	Windows CMD — %admin_email%	echo %admin_email%
	Windows PowerShell — \$admin_email	write-output \$admin_email

Свойство типа «массив»

Свойства типа «массив» ожидает массив строк, целых чисел, десятичных чисел или логических значений, определенных как *[value1, value2, value3...]*. Можно указывать значения самостоятельно, требовать от кого-либо предоставить значения или получать значения от другого компонента схемы элементов путем создания привязки к свойству.

При создании программного свойства типа «массив» с целочисленными или десятичными данными необходимо использовать точку с запятой для разделения элементов массива, независимо от языка. Не используйте запятую (,) или точку (.). В некоторых языках можно использовать запятую (,) как разделитель десятичных знаков. Пример:

- Допустимый массив для французского языка: [1,11;2,22;3,33]

- Допустимый массив для английского языка: [1.11,2.22,3.33]

При передаче больших чисел в массив не используйте формат группировки. Например, не используйте **4444 444.000** (французский), **4.444.444,000** (итальянский) или **4,444,444.000** (английский), поскольку в файлах с данными, содержащих форматы тех или иных языков, могут возникнуть ошибки при передаче на компьютер с другим языком. Формат группировки недопустим, поскольку такое число, как **4,444,444.000**, будет воспринято как три отдельных числа. Введите его в формате **4444444.000**.

При определении значений для свойства типа «массив» необходимо заключить массив в квадратные скобки. Для массива строк значение в элементах массива может содержать любые символы ASCII. Чтобы должным образом закодировать символ обратной косой черты в значении свойства типа «Массив», добавьте дополнительную обратную косую черту, например `["c:\\test1\\test2"]`. Для привязанного свойства используйте вкладку **Свойства** на холсте проекта, чтобы выбрать соответствующее свойство для привязки. В случае привязки к массиву необходимо спроектировать программные компоненты таким образом, чтобы не учитывался порядок значений в массиве.

Например, рассмотрим виртуальную машину подсистемы балансировки нагрузки, которая балансирует нагрузку кластера виртуальных машин сервера приложений. В таком случае для подсистемы балансировки нагрузки определяется свойство типа «массив», которому присваивается массив IP-адресов виртуальных машин сервера приложений.

В приведенных ниже сценариях настройки подсистемы балансировки нагрузки свойство типа «массив» используется для настройки соответствующей схемы балансировки нагрузки в операционных системах Red Hat, Windows и Ubuntu.

Образец свойства типа «массив»	Синтаксис сценария	Пример использования
operating_systems = ["Red Hat","Windows","Ubuntu"]	Bash — <code>\${operating_systems[@]}</code> для всего массива строк <code>\${operating_systems[N]}</code> для отдельного элемента массива	<pre>for ((i = 0 ; i < \$ {#operating_systems[@]}; i++)); do echo \${operating_systems[i]} done</pre>
	Windows CMD — <code>%operating_systems_%</code> где <i>N</i> соответствует позиции элемента в массиве	<pre>for /F "delims== tokens=2" %A in ('set operating_systems_') do (echo %A)</pre>
	Windows PowerShell — <code>\$operating_systems</code> для всего массива строк <code>\$operating_systems[N]</code> для отдельного элемента массива	<pre>foreach (\$os in \$operating_systems){ write-output \$os }</pre>

Свойство типа «содержимое»

Значением свойства типа «Содержимое» выступает URL-адрес, по которому можно загрузить файл с содержимым. Агент Программное обеспечение загружает содержимое с URL-адреса на виртуальную машину и передает расположение локального файла в сценарий.

Свойства типа «содержимое» должны быть определены в виде действующего URL-адреса по протоколу HTTP или HTTPS. Например, компонент Программное обеспечение сервера приложений JBOSS в примере приложения Dukes Bank указывает свойство содержимого `cheetah_tgz_url`. Артефакты размещены на устройстве Программное обеспечение и URL-адрес указывает на их расположение. Агент Программное обеспечение загружает артефакты из указанного расположения на развернутую виртуальную машину.

Сведения о параметрах `software.http.proxy`, которые используются для свойств содержимого, см. в *Справочник по настраиваемым свойствам*.

Образец строкового свойства	Синтаксис сценария	Пример использования
<code>cheetah_tgz_url = "http:// app_content_server_ip:port/artifacts/ software/jboss/cheetah-2.4.4.tar.gz"</code>	Bash — <code>\$cheetah_tgz_url</code>	<code>tar -zxvf \$cheetah_tgz_url</code>
	Windows CMD — <code>%cheetah_tgz_url%</code>	<code>start /wait c:\unzip.exe %cheetah_tgz_url%</code>
	Windows PowerShell — <code>\$cheetah_tgz_url</code>	<code>& c:\unzip.exe \$cheetah_tgz_url</code>

Свойство типа «Логическое»

Используйте свойства типа «логическое» для предоставления в раскрывающемся меню «Значение» вариантов «Истина» и «Ложь».

Свойство «Целое число»

Используйте свойство целочисленного типа для нулевых, положительных и отрицательных целых значений.

Свойство «Десятичное число»

Используйте свойство типа «десятичное число» для значений, представляющих собой неперiodические десятичные дроби.

Когда для компонента Программное обеспечение требуется информация из другого компонента

В нескольких сценариях развертывания для настройки одного компонента требуется значение свойства другого компонента. Это можно сделать с помощью vRealize Automation путем привязки свойств. Можно создать сценарии действий Программное обеспечение для привязки свойств, но окончательная настройка привязок выполняется архитектором, разрабатывающим схему элементов.

Помимо установки жестко заданных значений свойств, программный архитектор, архитектор инфраструктуры как услуги или разработчик архитектуры приложений могут привязать свойства компонента Программное обеспечение к другим свойствам в схеме элементов, например к IP-адресу или месту установки. При использовании привязки свойства Программное обеспечение к другому свойству можно настроить сценарий на основе значения свойства другого компонента или свойства виртуальной машины. Например, для компонента WAR может потребоваться место установки сервера Apache

Tomcat. В созданных сценариях для компонента WAR можно настроить установку значения `install_path` сервера Apache Tomcat для свойства `server_home`. Если архитектор, выполняющий сборку схемы элементов, привязал свойство `server_home` к свойству `install_path` сервера Apache Tomcat, значение `server_home` установлено правильно.

В сценариях действий можно использовать только те свойства, которые определены в этих сценариях, а в привязках можно использовать только свойства со значениями типа «строка» или «массив». Массивы свойств схемы элементов не возвращаются в каком-либо заданном порядке, поэтому значения, получаемые в результате привязки к группируемым или масштабируемым компонентам, могут быть неожиданными. Например, программному компоненту необходим идентификатор каждого компьютера в кластере и пользователям разрешено запрашивать кластер из диапазона 1–10 и масштабировать развертывание в диапазоне 1–10 компьютеров. Если настроить программное свойство строкового типа, вы получите один случайно выбранный идентификатор компьютера из кластера. Если настроить программное свойство типа «массив», вы получите массив всех идентификаторов компьютеров в кластере, но их порядок будет неизвестен. Если пользователи будут масштабировать развертывание, порядок значений может быть разным для каждой операции. Чтобы гарантировать отсутствие потери значений для компонентов кластера, можно использовать тип «массив» для всех программных свойств. Однако необходимо спроектировать программные компоненты без учета порядка значений в массиве.

Во время привязки к различным типам свойств см. примеры значений свойства строкового типа в таблице «Примеры привязок свойств строкового типа».

Таблица 3-45. Примеры привязок свойств строкового типа

Образец типа свойства	Тип свойства для привязки	Результат привязки (А привязывается к В)
Строка (свойство А)	Строка (свойство В="Hi")	A="Hi"
Строка (свойство А)	Содержимое (свойство В="http://my.com/content")	A="http://my.com/content"
Строка (свойство А)	Массив (свойство В=["1", "2"])	A=["1", "2"]
Строка (свойство А)	Вычисляемое (свойство В="Hello")	A="Hello"

Во время привязки к различным типам свойств см. примеры значений свойства типа «массив» в таблице «Примеры привязок свойства типа "массив"».

Таблица 3-46. Примеры привязок свойств типа «массив»

Образец типа свойства	Тип свойства для привязки	Результат привязки (А привязывается к В)
Массив (свойство А)	Строка (свойство В="Hi")	A="Hi"
Массив (свойство А)	Содержимое (свойство В="http://my.com/content")	A="http://my.com/content"
Массив (свойство А)	Вычисляемое (свойство В="Hello")	A="Hello"

Подробное объяснение поддерживаемых типов свойств см. в разделе [Типы свойств и параметры настройки](#).

Передача значений свойств между этапами жизненного цикла

С помощью сценариев действий можно изменять и передавать значения свойств между этапами жизненного цикла.

Для вычисляемого свойства можно изменить значение свойства и передать значение следующему этапу жизненного цикла в сценарии действий. Например, если для значения свойства `progress_status` компонента А определено значение `staged`, для этапов жизненного цикла `INSTALL` и `CONFIGURE` необходимо изменить значение на `progress_status=installed` в соответствующих сценариях действий. Если компонент В привязан к компоненту А, значения свойства `progress_status` этапов жизненного цикла сценария действий соответствуют значениям компонента А.

Укажите в программном компоненте, что компонент В зависит от компонента А. Эта зависимость определяет передачу правильных значений свойств между компонентами независимо от того, находятся они на одном узле или на разных.

Например, можно обновить значение свойства в сценарии действия путем использования поддерживаемых сценариев.

- Bash `progress_status="completed"`
- Windows CMD `set progress_status=completed`
- Windows PowerShell `$progress_status="completed"`

Примечание Свойства типа «содержимое» и «массив» не поддерживают передачу измененных значений свойств между сценариями действий этапов жизненного цикла.

Практические рекомендации по разработке компонентов

Для ознакомления с практическими рекомендациями по определению свойств и сценариев действий загрузите и импортируйте компоненты Программное обеспечение и схемы элементов приложения с портала VMware Solution Exchange.

Следуйте нижеприведенным практическим рекомендациям при разработке компонентов Программное обеспечение.

- Для выполнения сценария без каких-либо прерываний возвращаемое значение должно быть установлено равным нулю (0). Это дает агенту возможность получать все свойства и передавать их на сервер Программное обеспечение.
- Некоторым программам установки может понадобиться доступ к консоли `tty`. Перенаправьте ввод из `/dev/console`. Например, в сценарии установки компонент `RabbitMQ` Программное обеспечение может использовать команду `./rabbitmq_rhel.py --setup-rabbitmq < /dev/console`.
- Если компонент использует несколько этапов жизненного цикла, значение свойства может быть изменено на этапе `INSTALL`. Новое значение передается на следующий этап жизненного цикла. Сценарии действий могут вычислять значение свойства в ходе развертывания для передачи значения другим зависимым сценариям. Например, в образце приложения `Clustered Dukes Bank` служба `JBossAppServer` вычисляет свойство `JVM_ROUTE` на этапе жизненного цикла `INSTALL` (установка). Это свойство используется службой `JBossAppServer` для настройки жизненного цикла.

Затем служба балансировки нагрузки Apache привязывает свое свойство JVM_ROUTE к свойству all(appserver:JbossAppServer:JVM_ROUTE) для получения окончательного вычисленного значения node0 и node1. Если компоненту требуется значение свойства из другого компонента для успешного завершения развертывания приложения, необходимо задать явные зависимости в схеме элементов приложения.

Примечание Нельзя изменить значение свойства содержимого для компонента, который использует несколько этапов жизненного цикла.

Создание компонента Программное обеспечение

После настройки и публикации компонента Программное обеспечение его смогут использовать другие программные архитекторы, архитекторы инфраструктуры как услуги и разработчики архитектуры приложений для создания схем элементов приложений.

Необходимые условия

Войдите в службу vRealize Automation как **программный архитектор**.

Процедура

1. Выберите **Проектирование > Компоненты программного обеспечения**.
2. Щелкните значок **Добавить** (+).
3. Введите имя и, при необходимости, описание.

На основе имени, указанного для компонента Программное обеспечение, vRealize Automation создает идентификатор для компонента Программное обеспечение, который является уникальным в пределах арендатора. Сейчас это поле можно изменить, но после сохранения схемы элементов изменить его будет невозможно. Поскольку идентификаторы в арендаторе постоянны и уникальны, их можно использовать для программного взаимодействия со схемами элементов и создания привязок свойств.

4. (дополнительно) Если требуется управлять добавлением компонента Программное обеспечение в схемы элементов, в раскрывающемся меню **Контейнер** выберите тип контейнера.

Параметр	Описание
Компьютеры	Компонент Программное обеспечение необходимо разместить непосредственно на компьютере.
Один из опубликованных компонентов Программное обеспечение	Если проектируемый компонент Программное обеспечение предназначен для установки поверх другого созданного компонента Программное обеспечение, выберите этот компонент Программное обеспечение в списке. Например, для проектируемого компонента EAR, который будет устанавливаться поверх компонента JBOSS, созданного ранее, выберите в списке компонент JBOSS.
Компоненты программного обеспечения	Если необходимо спроектировать компонент Программное обеспечение, который не предназначен для непосредственной установки на компьютере, но может быть установлен в нескольких различных компонентах Программное обеспечение, выберите параметр «Компоненты программного обеспечения». Например, если при проектировании компонента WAR необходимо, чтобы его можно было установить в компоненте Программное обеспечение сервера Tomcat и Программное обеспечение Tcserver, выберите компоненты программного обеспечения контейнерного типа.

5. Нажмите кнопку **Далее**.
6. Определите свойства, которые планируется использовать в сценариях действий.

- Щелкните значок **Добавить** (+).
- Введите имя свойства.
- Введите описание свойства.

Это описание отображается для архитекторов, которые использовали этот компонент Программное обеспечение в схемах элементов.

- г) Выберите необходимый тип для значения свойства.
- д) Определите значение свойства.

Параметр	Описание
Использовать текущее указанное значение	<ul style="list-style-type: none"> ■ Введите значение. ■ Снимите флажок Допускает переопределение. ■ Установите флажок Обязательно.
Обязательно указывать значение (для архитекторов)	<ul style="list-style-type: none"> ■ Введите значение, чтобы предоставить значение по умолчанию для этого параметра. ■ Установите флажок Допускает переопределение. ■ Установите флажок Обязательно.
Разрешить архитекторам указывать значения при необходимости	<ul style="list-style-type: none"> ■ Введите значение, чтобы предоставить значение по умолчанию для этого параметра. ■ Установите флажок Допускает переопределение. ■ Снимите флажок Обязательно.

Архитекторы могут настроить свойства Программное обеспечение таким образом, чтобы они отображались в форме запроса для пользователей. Архитекторы могут использовать параметр «Показать в запросе», который позволяет отображать запрос на указание значений свойств, помеченных как допускающие переопределение.

7. Чтобы указать сценарий по крайней мере для одного из действий жизненного цикла программного обеспечения, работайте с запросами.

Таблица 3-47. Действия жизненного цикла

Действия жизненного цикла	Описание
Установка	Установка программного обеспечения. Например, можно скачать установочный файл сервера Tomcat и установить службу Tomcat. Сценарии, написанные для действий жизненного цикла, запускаются при первой подготовке программного обеспечения (во время первоначального запроса на развертывание или в ходе увеличения масштаба).
Настройка	Настройка программного обеспечения. Для примера Tomcat можно задать сценарии JAVA_OPTS и CATALINA_OPTS. Сценарии настройки запускаются после завершения действий установки.
Запуск	Запуск программного обеспечения. Например, можно запустить службу Tomcat с помощью команды запуска на сервере Tomcat. Сценарии запуска запускаются после завершения действий настройки.

Таблица 3-47. Действия жизненного цикла (продолжение)

Действия жизненного цикла	Описание
Обновление	Если проектируется программный компонент для поддержки масштабируемых схем элементов, обрабатывайте все обновления, необходимые после операции увеличения или уменьшения масштаба. Например, можно изменить размер кластера для масштабируемого развертывания и управлять узлами кластера с помощью подсистемы балансировки нагрузки. Проектируйте сценарии обновления для многократного запуска (без изменений) и обрабатывайте оба случая масштабирования (увеличение и уменьшение масштаба). После выполнения операции масштабирования сценарии обновления запускаются на всех зависимых программных компонентах.
Удаление	Удаление программного обеспечения. Например, можно выполнять особые действия в приложении перед удалением развертывания. Сценарии удаления запускаются каждый раз при удалении компонентов.

Включите в свои сценарии действий коды выхода и состояния. Каждому типу сценариев соответствуют уникальные коды выхода и состояния.

Тип сценария	Успешное состояние	Ошибочное состояние	Неподдерживаемые команды
Bash	■ return 0 ■ exit 0	■ return non-zero ■ exit non-zero	Нет
Windows CMD	exit /b 0	exit /b non-zero	Не используйте коды exit 0 и exit non-zero.
PowerShell	exit 0	exit non-zero;	Не используйте вызовы warning, verbose, debug и host.

- Установите флажок **Перезагрузить** для каждого сценария, при котором требуется перезагрузка компьютера.

После запуска сценария и перед запуском следующего сценария жизненного цикла произойдет перезагрузка компьютера.

- Щелкните элемент **Готово**.

- Выберите компонент Программное обеспечение и нажмите кнопку **Опубликовать**.

Результаты

Теперь компонент Программное обеспечение настроен и опубликован. Другие программные архитектуры, архитектуры инфраструктуры как услуги и разработчики архитектуры приложений могут использовать этот компонент Программное обеспечение для добавления программного обеспечения в схему элементов приложения.

Следующие шаги

Добавьте опубликованный компонент Программное обеспечение в схему элементов приложения. См. раздел [Сборка составных схем элементов](#).

Параметры компонента Программное обеспечение

Настройте общие параметры, создайте свойства и сценарии настраиваемых действий, чтобы установить, настроить, обновить или удалить компонент Программное обеспечение на подготовленных компьютерах.

Войдите в качестве программного архитектора, выберите элементы **Проектирование > Компоненты программного обеспечения**, затем — значок **Добавить**, чтобы создать компонент Программное обеспечение.

Общие параметры нового компонента Программное обеспечение

Примените общие параметры к компоненту Программное обеспечение.

Таблица 3-48. Общие параметры нового компонента Программное обеспечение

Параметр	Описание
Имя	Введите имя своего компонента Программное обеспечение.
Идентификатор	На основе имени, указанного для компонента Программное обеспечение, vRealize Automation создает идентификатор для компонента Программное обеспечение, который является уникальным в пределах арендатора. Сейчас это поле можно изменить, но после сохранения схемы элементов изменить его будет невозможно. Поскольку идентификаторы в арендаторе постоянны и уникальны, их можно использовать для программного взаимодействия со схемами элементов и создания привязок свойств.
Описание	Составьте сводку по компоненту Программное обеспечение, чтобы ею было удобно пользоваться другим разработчикам архитектуры.
Контейнер	<p>На холсте проекта архитекторы схем элементов могут помещать ваш компонент Программное обеспечение только внутри контейнера с выбранным вами типом.</p> <ul style="list-style-type: none"> ■ Выберите Компьютеры, чтобы от архитекторов требовалось размещать компонент Программное обеспечение непосредственно на компонент компьютера на холсте проекта. ■ Выберите Компоненты программного обеспечения, если проектируется компонент Программное обеспечение, который никогда не следует размещать непосредственно на компоненте компьютера, но можно вкладывать в один из нескольких различных компонентов Программное обеспечение. ■ Выберите конкретный опубликованный компонент Программное обеспечение, если проектируете компонент Программное обеспечение специально для вложения в другой созданный вами компонент Программное обеспечение. ■ Выберите Виртуальная машина Azure, если проектируется компонент Программное обеспечение специально для схемы элементов Azure.

Новые свойства Программное обеспечение

Свойства Программное обеспечение используются для параметризации сценариев, что позволяет передавать определенные свойства в качестве переменных среды в сценарии, выполняемые на виртуальной машине. Перед выполнением сценариев агент Программное обеспечение, установленный на подготовленном компьютере, обменивается данными с vRealize Automation для сопоставления свойств. Затем агент создает на основе этих свойств переменные, соответствующие определенным сценариям, и передает их в сценарии.

Таблица 3-49. Новые свойства Программное обеспечение

Параметр	Описание
Имя	Введите имя своего свойства Программное обеспечение. В именах свойств учитывается регистр и они могут содержать только буквы, цифры, символы дефиса (-) и подчеркивания (_).
Описание	Составьте сводку по свойствам и любым требованиям к значению, которая окажет содействие другим пользователям.
Тип	Программное обеспечение поддерживает типы «строка», «массив», «содержимое», «логическое» и «целое число». Подробное объяснение поддерживаемых типов свойств см. в разделе Типы свойств и параметры настройки . Сведения о привязке свойств см. в разделе Когда для компонента Программное обеспечение требуется информация из другого компонента и Создание привязки свойств между компонентами схемы элементов .
Значение	<ul style="list-style-type: none"> ■ Порядок использования указанного значения. <ul style="list-style-type: none"> ■ Введите значение в поле Значение. ■ Установите флажок Обязательно. ■ Снимите флажок Допускает переопределение. ■ Порядок действий, необходимых для того, чтобы потребовать от архитекторов предоставить значение. <ul style="list-style-type: none"> ■ (Необязательно.) В поле Значение введите значение, которое будет использоваться по умолчанию. ■ Установите флажок Допускает переопределение. ■ Установите флажок Обязательно. ■ Разрешите архитекторам предоставлять значение или оставлять значение пустым. <ul style="list-style-type: none"> ■ (Необязательно.) В поле Значение введите значение, которое будет использоваться по умолчанию. ■ Установите флажок Допускает переопределение. ■ Снимите флажок Обязательно.

Таблица 3-49. Новые свойства Программное обеспечение (продолжение)

Параметр	Описание
Зашифровано	<p>Пометьте свойства как зашифрованные, чтобы скрыть значение. Оно будет отображаться в виде звездочек в vRealize Automation. Если изменить пометку свойства с «Зашифрованное» на «Незашифрованное», vRealize Automation сбросит значение свойства. Из соображений безопасности для свойства нужно задать новое значение.</p> <p>Важно! При печати защищенных свойств в сценарии с помощью команды <code>echo</code> и других подобных команд такие значения отображаются обычным текстом в файлах журнала. Значения в файлах журнала не маскируются.</p>
Допускает переопределение	Если выбрать этот параметр, архитекторы смогут изменять значение этого свойства при сборке схемы элементов приложения. Если ввести значение, оно отобразится в качестве значения по умолчанию.
Обязательно	Если выбрать этот параметр, архитекторам потребуется указать значение этого свойства или принять предоставляемое значение по умолчанию.
Вычисляемое	Значения вычисляемых свойств назначаются сценариями жизненного цикла <code>INSTALL</code> , <code>CONFIGURE</code> , <code>START</code> или <code>UPDATE</code> . Назначенное значение распространяется на последующие доступные этапы жизненного цикла и компоненты, которые связаны с этими свойствами в схеме элементов. Если выбрать для нестрокового свойства тип «Вычисляемое», тип свойства станет строковым.

Действия нового компонента «Программное обеспечение»

Создавайте сценарии действий Bash, Windows CMD или PowerShell для указания того, как именно устанавливаются, настраиваются, удаляются или обновляются компоненты во время операций масштабирования развертывания.

Таблица 3-50. Действия жизненного цикла

Действия жизненного цикла	Описание
Установка	Установка программного обеспечения. Например, можно скачать установочный файл сервера Tomcat и установить службу Tomcat. Сценарии, написанные для действий жизненного цикла, запускаются при первой подготовке программного обеспечения (во время первоначального запроса на развертывание или в ходе увеличения масштаба).
Настройка	Настройка программного обеспечения. Для примера Tomcat можно задать сценарии <code>JAVA_OPTS</code> и <code>CATALINA_OPTS</code> . Сценарии настройки запускаются после завершения действий установки.
Запуск	Запуск программного обеспечения. Например, можно запустить службу Tomcat с помощью команды запуска на сервере Tomcat. Сценарии запуска запускаются после завершения действий настройки.

Таблица 3-50. Действия жизненного цикла (продолжение)

Действия жизненного цикла	Описание
Обновление	Если проектируется программный компонент для поддержки масштабируемых схем элементов, обрабатывайте все обновления, необходимые после операции увеличения или уменьшения масштаба. Например, можно изменить размер кластера для масштабируемого развертывания и управлять узлами кластера с помощью подсистемы балансировки нагрузки. Проектируйте сценарии обновления для многократного запуска (без изменений) и обрабатывайте оба случая масштабирования (увеличение и уменьшение масштаба). После выполнения операции масштабирования сценарии обновления запускаются на всех зависимых программных компонентах.
Удаление	Удаление программного обеспечения. Например, можно выполнять особые действия в приложении перед удалением развертывания. Сценарии удаления запускаются каждый раз при удалении компонентов.

Установите флажок **Перезагрузить** для каждого сценария, при котором требуется перезагрузка компьютера. После запуска сценария и перед запуском следующего сценария жизненного цикла произойдет перезагрузка компьютера. При выполнении сценария действий убедитесь в отсутствии процессов, запрашивающих действия пользователя. Прерывания приостанавливают сценарий, что приводит к его простоя в течение неопределенного времени и впоследствии к сбою. Кроме того, ваши сценарии должны содержать надлежащие коды выхода, которые применимы к развертыванию приложений. Если в сценарии отсутствуют коды выхода и возврата, состоянием выхода становится последняя команда, которая выполнялась в сценарии. Коды выхода и возврата зависят от поддерживаемых типов сценариев (Bash, Windows CMD, PowerShell).

Тип сценария	Успешное состояние	Ошибочное состояние	Неподдерживаемые команды
Bash	<ul style="list-style-type: none"> ■ return 0 ■ exit 0 	<ul style="list-style-type: none"> ■ return non-zero ■ exit non-zero 	Нет
Windows CMD	exit /b 0	exit /b non-zero	Не используйте коды exit 0 и exit non-zero.
PowerShell	exit 0	exit non-zero;	Не используйте вызовы warning, verbose, debug и host.

Проектирование схем элементов и действий ресурсов Все как услуга

Схемы элементов Все как услуга можно публиковать в качестве элементов каталогов или использовать на холсте проекта схем элементов. Действия ресурсов — это действия, выполняемые с развернутыми элементами.

В Все как услуга для запуска рабочих процессов подготовки элементов или выполнения действий используется vRealize Orchestrator. Например, можно настроить рабочие процессы для создания виртуальных машин vSphere, пользователей Active Directory в группах или выполнения сценариев PowerShell. При создании настраиваемого рабочего процесса vRealize Orchestrator можно указать его в качестве элемента в каталоге служб. Это позволит запускать соответствующий рабочий процесс уполномоченным пользователям.

Можно использовать схему элементов Все как услуга как компонент в схеме элементов, созданной на холсте проекта, либо опубликовать ее непосредственно в каталоге служб.

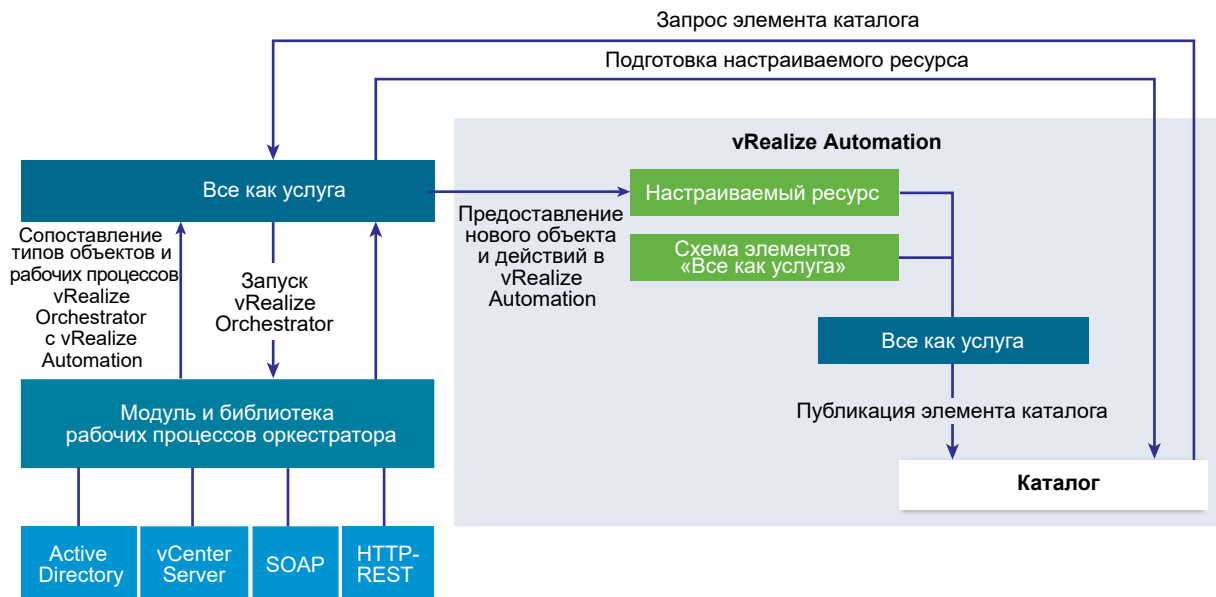
Если схема элементов используется в качестве компонента другой схемы элементов, можно задать, чтобы при уменьшении или увеличении масштаба развернутой схемы элементов происходило соответствующее масштабирование данной схемы.

Интеграция vRealize Orchestrator в vRealize Automation

vRealize Orchestrator является ядром рабочих процессов, интегрированным в vRealize Automation.

Сервер vRealize Orchestrator распространяется с предварительно настроенным vRealize Automation, поэтому, когда системный администратор развернет устройство vRealize Automation, сервер vRealize Orchestrator будет готов к работе.

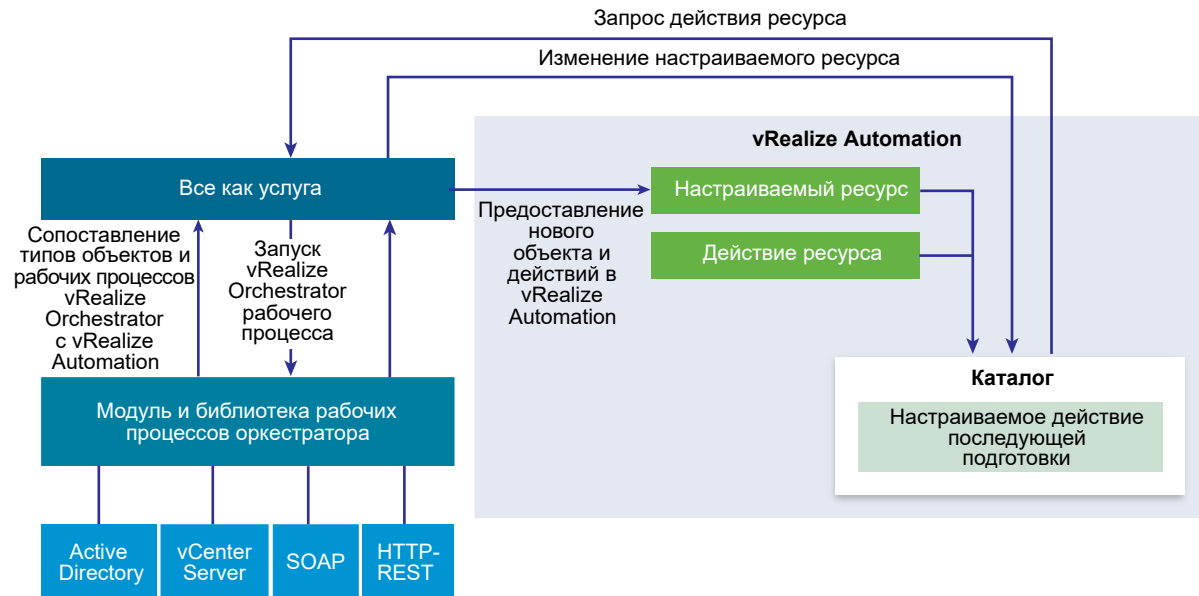
Рис. 3-2. Создание и запрос элементов каталога входит в состав Все как услуга для подготовки пользовательского ресурса



Разработчики архитектуры Все как услуга добавляют настраиваемые ресурсы, относящиеся к поддерживаемым конечным точкам и предоставляемым рабочим процессам, а затем создают схемы элементов Все как услуга и действия, основанные на этих ресурсах. Администраторы арендатора и менеджеры бизнес-группы могут добавлять схемы элементов Все как услуга и действия в каталог служб. Схему элементов Все как услуга также можно использовать в конструкторе схем элементов.

Когда пользователь каталога служб запрашивает элемент, vRealize Automation запускает рабочий процесс vRealize Orchestrator для подготовки настраиваемого ресурса.

Рис. 3-3. Создание и запрос действий настраиваемых ресурсов для изменения настраиваемого ресурса



Разработчики Все как услуга также могут добавить рабочие процессы vRealize Orchestrator в качестве действий ресурсов для расширения возможностей vRealize Automation. После подготовки пользователями каталога служб настраиваемого ресурса они могут запускать действия, выполняемые после подготовки ресурсов. Таким образом, клиенты запускают рабочий процесс vRealize Orchestrator и изменяют подготовленный настраиваемый ресурс.

Когда пользователь каталога служб запрашивает схему элементов Все как услуга или действие ресурса в качестве элемента каталога, служба Все как услуга запускает соответствующий рабочий процесс vRealize Orchestrator, передавая ему в качестве глобальных параметров следующие данные.

Таблица 3-51. Глобальные параметры Все как услуга

Параметр	Описание
__asd_tenantRef	Арендатор пользователя, запрашивающего рабочий процесс.
__asd_subtenantRef	Бизнес-группа пользователя, запрашивающего рабочий процесс.
__asd_catalogRequestId	Идентификатор запроса из каталога для запуска этого рабочего процесса.
__asd_requestedFor	Целевой пользователь запроса. Если запрос выполняется от имени пользователя, то это пользователь, от имени которого запрошен рабочий процесс, в остальных случаях это пользователь, запрашивающий рабочий процесс.
__asd_requestedBy	Пользователь, запрашивающий рабочий процесс.

Если схема элементов Все как услуга или действие ресурса использует рабочий процесс vRealize Orchestrator, который содержит элемент схемы взаимодействия с пользователем, то при запросе пользователем службы рабочий процесс приостанавливает выполнение и ожидает от пользователя предоставления необходимых данных. Чтобы ответить на ожидание взаимодействия, пользователь должен перейти к **Входящие > Действие пользователя, выполняемое вручную**.

Иерархия сервера vRealize Orchestrator по умолчанию является общей для всех арендаторов и не может быть использована отдельно для каждого арендатора. Например, если разработчик архитектуры служб создает схему элементов службы для создания кластера вычислительных ресурсов, клиентам из разных арендаторов придется просматривать элементы иерархии всех экземпляров vCenter Server, хотя они могут относиться к другому арендатору.

Системные администраторы могут установить vRealize Orchestrator или отдельно развернуть vRealize Orchestrator Appliance, чтобы настроить внешний экземпляр vRealize Orchestrator и сконфигурировать vRealize Automation для работы с таким внешним экземпляром vRealize Orchestrator.

Системные администраторы также могут настраивать категории рабочих процессов vRealize Orchestrator отдельно для каждого арендатора и определять, какие рабочие процессы доступны для каждого арендатора.

Кроме того, администраторы арендаторов могут также настроить внешний экземпляр vRealize Orchestrator, но только для своих арендаторов.

Для получения информации о настройке внешнего экземпляра vRealize Orchestrator и категорий рабочих процессов vRealize Orchestrator см. *Настройка vCenter Orchestrator и подключаемых модулей*.

Список подключаемых модулей vRealize Orchestrator

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

Среди подключаемых модулей, с помощью которых пользователи могут получать доступ к различным сторонним решениям, могут быть средства управления виртуализацией, почтовые платформы, базы данных, службы каталогов и интерфейсы удаленного управления.

Стандартный набор подключаемых модулей vRealize Orchestrator позволяет использовать в рабочих процессах такие преимущества внешних решений, как интерфейс API и почтовые возможности vCenter Server. Кроме того, открытая архитектура подключаемых модулей для vRealize Orchestrator дает возможность разрабатывать подключаемые модули для доступа к другим приложениям.

Таблица 3-52. Подключаемые модули по умолчанию в vRealize Orchestrator

Подключаемый модуль	Цель
vCenter Server	Обеспечивает доступ к интерфейсу API vCenter Server, позволяя использовать все объекты и функции vCenter Server в процессах управления, автоматизируемых с помощью vRealize Orchestrator.
Конфигурация	Предоставляет рабочие процессы для настройки проверки подлинности, подключения к базе данных и сертификатов SSL для vRealize Orchestrator.
Библиотека vCO	Предоставляет рабочие процессы, которые работают в качестве основных элементов настройки и автоматизации клиентских процессов. Библиотека рабочих процессов включает в себя шаблоны для управления жизненным циклом, подготовкой, аварийным восстановлением, горячим резервным копированием и другими стандартными процессами. Шаблоны можно копировать и изменять в соответствии с потребностями.
SQL	Предоставляет интерфейс JDBC API. Это стандартный интерфейс в отрасли, который позволяет подключать приложения, написанные на языке Java, к базам данных независимо от их платформ. К таким базам данных относятся базы данных SQL и другие табличные источники данных, например электронные таблицы и неструктурированные файлы. Интерфейс JDBC API предоставляет API для вызовов, позволяющий получать доступ к базам данных SQL с помощью рабочих процессов.
SSH	Обеспечивает реализацию протокола SSH-2. Позволяет использовать в рабочих процессах сеансы удаленной командной строки и передачи файлов с использованием проверки подлинности на основе пароля и открытого ключа. Поддерживает интерактивную проверку подлинности с использованием клавиатуры. Подключаемый модуль SSH также может обеспечивать удаленный просмотр файловой системы непосредственно в иерархии клиента vRealize Orchestrator.
XML	Полнофункциональное средство анализа XML модели DOM, которое можно использовать в рабочих процессах. Кроме того, в интерфейсе JavaScript API vRealize Orchestrator можно реализовывать ECMAScript для XML (E4X).
Почта	Использует протокол SMTP для отправки сообщений электронной почты из рабочих процессов.
Сеть	Предусматривает использование библиотеки Jakarta Apache Commons Net Library. Реализовывает протоколы Telnet, FTP, POP3 и IMAP. Протоколы POP3 и IMAP используются для чтения электронной почты. Вместе с почтовым подключаемым модулем сетевой подключаемый модуль обеспечивает возможности отправки и получения электронной почты в рабочих процессах.
Перечисление	Предоставляет общие типы перечислений, которые можно использовать в рабочих процессах других подключаемых модулей.
Документация по рабочим процессам	Позволяет использовать рабочие процессы, с помощью которых можно создавать информацию о рабочем процессе или категории рабочих процессов в формате PDF.
HTTP-REST	Позволяет управлять веб-службами REST, обеспечивая взаимодействие между vCenter Orchestrator и узлами REST.
SOAP	Позволяет управлять веб-службами SOAP, обеспечивая взаимодействие между vCenter Orchestrator и узлами SOAP.

Таблица 3-52. Подключаемые модули по умолчанию в vRealize Orchestrator (продолжение)

Подключаемый модуль	Цель
AMQP	Обеспечивает взаимодействие с серверами, которые используют протокол AMQP, также известными как брокеры.
SNMP	Позволяет vCenter Orchestrator устанавливать подключение к системам и устройствам, которые поддерживают протокол SNMP, и получать из них информацию.
Active Directory	Обеспечивает взаимодействие между vCenter Orchestrator и Microsoft Active Directory.
vCO WebOperator	Веб-представление, которое позволяет получать доступ к рабочим процессам в библиотеке vRealize Orchestrator и работать в сети с помощью веб-браузера.
Динамические типы	Позволяет определить динамические типы, а также создавать и использовать объекты этих типов.
PowerShell	Позволяет управлять узлами и выполнять настраиваемые процессы PowerShell.
Несколько узлов	Содержит рабочие процессы для иерархической оркестрации, управления экземплярами Orchestrator и увеличения масштаба действий Orchestrator.
vRealize Automation	Позволяет создавать и запускать рабочие процессы для взаимодействия между vRealize Orchestrator и vRealize Automation.

Дополнительные сведения о подключаемых модулях vRealize Orchestrator, проектируемых и предоставляемых VMware, см. на начальной странице документации по VMware vRealize™ Orchestrator™.

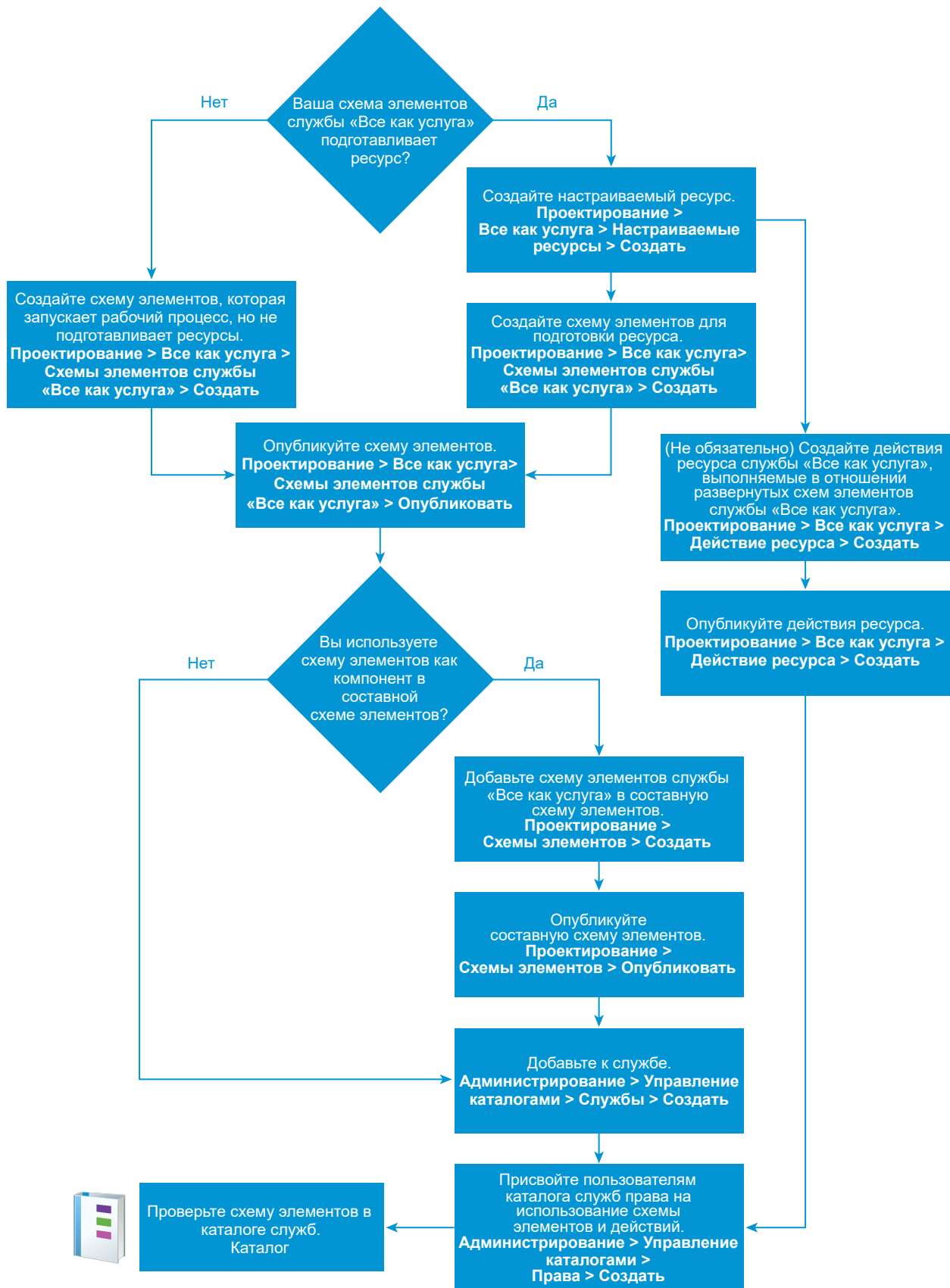
Создание схем элементов и действий ресурсов Все как услуга

Права на схемы элементов Все как услуга могут быть предоставлены пользователям как права на элементы каталога, либо их можно собрать в виде составных схем элементов с помощью холста проекта. Действия ресурса выполняются с подготовленными элементами для управления этими элементами после их подготовки.

Например, схему элементов Все как услуга можно использовать для создания пользователей Active Directory в группе. Затем можно использовать действие ресурса, чтобы потребовать от пользователя изменения пароля.

Рабочий процесс по созданию схемы элементов Все как услуга

Рабочий процесс, выполняемый для создания схемы элементов Все как услуга, и все дополнительные действия ресурса зависят от того, каким образом пользователь собирается использовать данную схему элементов. Описанный ниже рабочий процесс содержит основные этапы данной операции.



Терминология схемы элементов Все как услуга

Схемы элементов Все как услуга являются рабочими процессами vRealize Orchestrator, которые могут подготавливать ресурсы, вносить изменения в подготовленные ресурсы или вести себя как служба, которая выполняет задачу в данной среде. Схемы элементов и действия ресурса имеют несколько нюансов, которые необходимо принимать во внимание при проектировании схем элементов для пользователей каталога служб.

Следующие определения помогут вам понять терминологию, используемую при работе со схемами элементов Все как услуга.

Настраиваемый ресурс

Тип объекта vRealize Orchestrator, который предоставляется в качестве ресурса через API подключаемого модуля vRealize Orchestrator. Вы можете создать настраиваемый ресурс, чтобы определить выходной параметр схемы элементов подготовки Все как услуга и входной параметр действия ресурса.

Компонент схемы элементов Все как услуга

Схема элементов подготовки или схема элементов операций, не относящихся к подготовке, которую можно использовать на холсте проекта схемы элементов. Эта схема элементов также может быть самостоятельной схемой элементов Все как услуга.

Самостоятельная схема элементов Все как услуга

Схема элементов подготовки или схема элементов операций, не относящихся к подготовке, опубликованная непосредственно для каталога служб и имеющая соответствующие права.

Схема элементов подготовки

Схема элементов подготовки, которая запускает рабочий процесс vRealize Orchestrator для подготовки ресурсов на целевой конечной точке с помощью API подключаемого модуля vRealize Orchestrator для этой конечной точки. Например, добавляет виртуальные сетевые адаптеры к сетевому устройству в vSphere. Для создания схемы элементов подготовки необходимо иметь настраиваемый ресурс, который определяет тип ресурса vRealize Orchestrator.

Когда пользователь каталога служб запрашивает этот тип элементов каталога, рабочий процесс подготавливает его и развернутый элемент сохраняется на вкладке **Развертывания**. Для этого типа подготовленных ресурсов можно определять операции последующей подготовки. Можно также делать схемы элементов масштабируемыми, добавляя или удаляя экземпляр при необходимости.

Схема элементов операций, не относящихся к подготовке

Схема элементов операций, не относящихся к подготовке, запускает рабочий процесс vRealize Orchestrator для выполнения задачи, которая не требует от API внесения изменений в конечную точку. Например, выполняемый рабочий процесс создает отчет, а затем отправляет его по электронной почте или направляет в целевую коммуникационную систему.

Когда пользователь каталога служб запрашивает такой тип элемента каталога, рабочий процесс запускается, чтобы выполнить включенную в сценарий задачу, но этот элемент не добавляется на вкладку **Развертывания**. Для этого типа схемы элементов нельзя выполнять операции последующей

подготовки. Схемы элементов операций, не относящихся к подготовке, можно использовать в качестве поддерживающих рабочих процессов в масштабируемых схемах элементов. Например, можно создать схему элементов для обновления подсистемы балансировки нагрузки высокой доступности.

Составная схема элементов

Схема элементов, созданная с помощью холста проекта. В составной схеме элементов используется один или несколько компонентов. Например, компонент компьютера, программного обеспечения или компонент Все как услуга. Если такая схема добавляется к службе, она указывается как развертывание. Если такая схема добавляется к разрешениям, чтобы сделать ее доступной для пользователей каталога служб, она указывается как составная схема элементов. Составная схема элементов может иметь один компонент схемы элементов или включать в себя полное приложение с несколькими компьютерами, программным обеспечением и сетью.

Действие ресурса

Рабочий процесс, который можно запустить на развернутой схеме элементов подготовки. Развернутая схема элементов может быть схемой элементов Все как услуга или компонентом схемы элементов. Она также может быть типом компьютера, сопоставленного с типом ресурса vRealize Orchestrator.

Вопросы по проектированию схемы элементов Все как услуга

Прежде чем создать схему элементов Все как услуга, необходимо определить ее предназначение. Это позволит создать схему элементов, которая правильно подготовит ресурсы.

Схемы элементов Все как услуга можно создавать и использовать в качестве компонента схемы элементов на холсте проекта или как самостоятельную схему элементов. Схема элементов может представлять собой схему элементов подготовки или обычную схему элементов (не относящуюся к подготовке).

Таблица 3-53. Типы и результаты схемы элементов Все как услуга

Тип схемы элементов Все как услуга	Требуется ли настраиваемый ресурс?	Масштабируется ли схема элементов в развертывании?	Можно ли выполнить действие ресурса на развернутой схеме элементов?
Компонент схемы элементов, который подготавливает ресурсы	Да	Да. Если для схемы настроено масштабирование, ее масштаб будет меняться при изменении масштаба развертывания.	Да. Ее масштаб изменится при изменении масштаба развертывания, а пользователь может выполнить другие действия ресурса с развернутым компонентом. Компонент схемы элементов появится на вкладке «Развертывания».
Компонент схемы элементов, который выполняет рабочий процесс, но не подготавливает ресурсы	Нет. Схема элементов использует конфигурацию сервера vRealize Orchestrator, но ей не требуется настраиваемый ресурс Все как услуга.	Нет. Она не подготавливает ресурсы, но может выполняться как часть операции масштабирования. Например, обновление подсистемы балансировки нагрузки с новой конфигурацией, основанной на операции масштабирования.	Нет. Невозможно выполнить действие ресурса с компонентом, который не относится к подготовке.
Самостоятельная схема элементов, которая подготавливает ресурсы	Да	Нет. Необходимо создать действия ресурса, чтобы добавить или удалить экземпляры.	Да. Можно выполнять действия ресурса с развернутым ресурсом, включая все действия, созданные для поддержки масштабирования. Схема элементов появляется на вкладке «Развертывания».
Самостоятельная схема элементов, которая запускает рабочий процесс, но не подготавливает ресурсы	Нет. Схема элементов использует конфигурацию сервера vRealize Orchestrator, но ей не требуется настраиваемый ресурс Все как услуга.	Нет. Она не подготавливает ресурсы, но может выполняться как часть действия ресурса.	Нет. Невозможно выполнить действие ресурса с компонентом, который не относится к подготовке.

Добавление настраиваемого ресурса Все как услуга

Чтобы определить элемент Все как услуга для подготовки, можно создать настраиваемый ресурс. Для того чтобы можно было создать схему элементов Все как услуга или действие, в распоряжении должен быть настраиваемый ресурс, совместимый с типом объекта схемы элементов или рабочего процесса действия.

Создание настраиваемого ресурса предусматривает сопоставление типа объекта, который предоставляется через интерфейс API подключаемого модуля vRealize Orchestrator, в качестве ресурса. Настраиваемый ресурс определяет выходной параметр схемы элементов Все как услуга для подготовки и входной параметр действия ресурса.

Если рабочий процесс схемы элементов или действия ресурса не подготавливает ресурс или выполняется в отношении развернутой схемы элементов, настраиваемый ресурс создавать не нужно. К примеру, нет необходимости в настраиваемом ресурсе, если рабочий процесс обновляет значение базы данных или отправляет сообщение электронной почты после операции подготовки.

Создавая настраиваемый ресурс, можно указать поля формы только для чтения в представлении сведений подготовленного элемента. См. раздел [Проектирование настраиваемой формы ресурсов](#).

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Сведения о расширенных параметрах помогут в настройке настраиваемого ресурса. См. раздел [Параметры мастера настраиваемого ресурса Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Выберите значок **Создать** (+).
3. Настройте значения на вкладке **Тип ресурса**.
 - а) Введите или выберите тип объекта vRealize Orchestrator в текстовом поле **Тип оркестратора**.
К примеру, можно ввести значение **V**, чтобы отобразить типы, содержащие букву «V». Для просмотра всех типов введите пробел.
 - б) Введите имя и, при необходимости, описание.
 - в) Введите версию.
Поддерживаемый формат расширен и имеет вид основной номер.промежуточный номер.номер микровыпуска-номер редакции.
 - г) Нажмите кнопку **Далее**.
4. Внесите необходимые изменения на вкладке **Форма сведений**.
Чтобы изменить настраиваемый ресурс, удалите, измените или переставьте местами элементы. Кроме того, можно добавить форму и страницы формы, а также перетащить элементы в новую форму и на страницу формы.
5. Щелкните элемент **Готово**.

Результаты

Теперь настраиваемый ресурс создан и отображен на странице «Настраиваемые ресурсы». Теперь на основе этого настраиваемого ресурса можно создавать схемы элементов или действия Все как услуга.

Следующие шаги

- Создайте схему элементов Все как услуга. См. раздел [Добавление схемы элементов Все как услуга](#).
- Создайте действия ресурса Все как услуга. См. раздел [Создание действия ресурса Все как услуга](#).

Параметры мастера настраиваемого ресурса Все как услуга

Эти параметры настраиваемого ресурса используются для создания или изменения настраиваемого ресурса, что позволяет запускать схему элементов Все как услуга и рабочие процессы действия ресурса, которые подготавливают ресурсы или изменяют подготовленные ресурсы.

Можно создать только один настраиваемый ресурс для одного типа объекта. Настраиваемый ресурс можно использовать для нескольких схем элементов и действий ресурса.

Чтобы создать действие настраиваемого ресурса, последовательно выберите **Проект > Все как услуга > Настраиваемые ресурсы**

Тип ресурса

Список возможных типов объекта, который появляется на вкладке **Тип ресурса**, основан на установленных подключаемых модулях в настроенном экземпляре vRealize Orchestrator. vRealize Automation получает значения от настроенного экземпляра vRealize Orchestrator.

Таблица 3-54. Варианты типов ресурса

Параметр	Описание
Тип оркестратора	Введите или выберите тип, совместимый с рабочим процессом, который используется для подготовки. Название типа состоит из имени подключаемого модуля, указанного в API сценария, например VC для vCenter, и типа объекта, например VirtualMachine. В этом примере в API используется значение VC:VirtualMachine. Этот тип может быть выходным параметром рабочего процесса схемы элементов или входным параметром рабочего процесса действия ресурса.
Имя	Введите информативное имя для настраиваемого ресурса, позволяющее определить его при создании схем элементов Все как услуга или действий ресурса.
Описание	Введите подробное описание.
Версия	Поддерживаемая форма расширена и имеет такой вид: основной номер.промежуточный номер.номер микровыпуска-номер редакции.

Форма сведений

Эти поля формы появляются как значения только для чтения, когда пользователи каталога служб подготавливают элемент, для которого используется этот настраиваемый ресурс. Можно изменять существующие поля и добавлять новые, определенные во внешнем источнике.

Дополнительные сведения о настройке форм см. в разделе [Проектирование настраиваемой формы ресурсов](#).

Назначение

Поскольку можно создать только один настраиваемый ресурс для одного типа объекта, используйте эту страницу мастера, чтобы понять, как используется настраиваемый ресурс.

Эта вкладка доступна для сохраненных настраиваемых ресурсов и не доступна во время создания ресурса.

Таблица 3-55. Параметры назначения

Параметр	Описание
Схемы элементов «Все как услуга»	<p>Список схем элементов, которые настроены для использования этого настраиваемого ресурса.</p> <p>На этой странице можно выполнить следующие действия.</p> <ul style="list-style-type: none"> ■ Изменить. Открывается схема элементов, настройки которой можно просмотреть или изменить. ■ Опубликовать/отменить публикацию. Измените состояние схемы элементов, разрешив использовать ее в составной схеме элементов или добавлять к службе. В случае отмены публикации схемы элементов можно потенциально сделать ее недоступной для использования в составных схемах элементов и для добавления к службе, а также недоступной в каталоге служб. ■ Удалить. Схема элементов удаляется из системы.
Действия ресурса	<p>Список действий ресурса, для которых настроено использование этого настраиваемого ресурса.</p> <p>На этой странице можно выполнить следующие действия.</p> <ul style="list-style-type: none"> ■ Изменить. Открывается действие ресурса, настройки которого можно просмотреть или изменить. ■ Опубликовать/отменить публикацию. Измените состояние действия ресурса, добавив его к разрешениям. Отменив публикацию действия ресурса, можно потенциально сделать его недоступным для добавления к службе или для запуска в развернутых схемах элементов. ■ Удалить. Действие ресурса удаляется из системы.

Создание схемы элементов Все как услуга

Схема элементов Все как услуга может быть схемой элементов подготовки или обычной схемой элементов. К числу выполняемых рабочих процессов подготовки vRealize Orchestrator, среди прочего, относятся: создание виртуальных машин, добавление пользователей в Active Directory, создание моментальных снимков виртуальных машин. Примеры обычных рабочих процессов (не связанных с подготовкой), которые можно создавать: обновление средства балансировки нагрузки или составление отчета и его отправка получателям.

Вы можете создавать схемы элементов Все как услуга на основе рабочих процессов, представленных в vRealize Orchestrator, а можете использовать созданные вами рабочие процессы для выполнения конкретных задач в своей среде.

Процедура

1. Добавление схемы элементов Все как услуга

Схема элементов Все как услуга — это спецификация, определяющая способ выполнения рабочего процесса vRealize Orchestrator, который вносит изменение в целевую систему в вашей среде. Помимо самого рабочего процесса, схема элементов может также включать входные параметры, формы для отправки и формы только для чтения, последовательность действий, операции подготовки или другие операции.

2. Добавление схемы элементов Все как услуга к составной схеме элементов

Схема элементов Все как услуга добавляется как компонент к составной схеме элементов так же, как компоненты схемы элементов добавляются на холст проекта.

Добавление схемы элементов Все как услуга

Схема элементов Все как услуга — это спецификация, определяющая способ выполнения рабочего процесса vRealize Orchestrator, который вносит изменение в целевую систему в вашей среде. Помимо самого рабочего процесса, схема элементов может также включать входные параметры, формы для отправки и формы только для чтения, последовательность действий, операции подготовки или другие операции.

Схему элементов Все как услуга можно создать одним или несколькими способами, описанными ниже.

- Создание схемы элементов Все как услуга как компонента. Компонент схемы элементов — это схема элементов подготовки или схема элементов операций, не относящихся к подготовке, которую можно использовать на холсте проекта схемы элементов как часть составной схемы элементов. При использовании схемы как компонента необходимо настроить параметры жизненного цикла этого компонента так, чтобы для него поддерживались операции уменьшения и увеличения масштаба в развернутой составной схеме элементов.

Схема элементов такого типа также может быть опубликована как самостоятельная.

- Создание самостоятельной схемы элементов Все как услуга. Самостоятельная схема элементов — это схема элементов подготовки или схема элементов операций, не относящихся к подготовке, которая публикуется и получает необходимые права непосредственно в каталоге служб.

Пример создания пользователей Active Directory с помощью схемы элементов Все как услуга см. в разделе [Создание схемы элементов Все как услуга и действия для создания и изменения пользователя](#).

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Если с помощью схемы элементов необходимо подготавливать ресурсы, создайте настраиваемый ресурс, соответствующий выходному параметру схемы элементов службы. См. раздел [Добавление настраиваемого ресурса Все как услуга](#). Если API подключаемого модуля vRealize Orchestrator не используется, то необходимости в настраиваемом ресурсе нет.

- При создании схемы элементов Все как услуга рабочий процесс vRealize Orchestrator публикуется как возможный элемент каталога или компонент схемы элементов. В схеме элементов содержится форма, которая может быть изменена. См. раздел [Проектирование формы схемы элементов Все как услуга](#).
- Для настройки схемы элементов используйте подробные сведения о параметрах. См. раздел [Параметры мастера схемы элементов Все как услуга «Создать» или «Редактировать»](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Выберите значок **Создать** (+).
3. На вкладке **Рабочий процесс** выберите рабочий процесс, который выполняется при подготовке ресурса с помощью схемы элементов.

Эта вкладка недоступна при внесении изменений в схему элементов.

- а) Перейдите в библиотеку рабочих процессов vRealize Orchestrator и выберите рабочий процесс, соответствующий настраиваемому ресурсу.
 - б) Убедитесь, что входные и выходные параметры позволяют вам позже внести правильные значения.
 - в) Нажмите кнопку **Далее**.
4. На вкладке **Общие** настройте параметры и нажмите кнопку **Далее**.
 - а) В текстовом поле **Имя** введите имя, которое позволит отличить данную схему элементов от похожих схем.
 - б) Если вы не хотите использовать эту схему элементов как компонент в составной схеме элементов, снимите флажок **Сделать доступным в качестве компонента на холсте проекта**.
 5. На вкладке **Форма схемы элементов** внесите необходимые изменения в форму и нажмите кнопку **Далее**.
 6. На странице **Подготовленный ресурс** выберите значение и нажмите кнопку **Далее**.

Параметр	Описание
Подготовка отсутствует	Если рабочий процесс не используется для подготовки ресурсов, можно выбрать этот параметр или оставить поле пустым.
<Настраиваемый ресурс, созданный ранее>	Выберите настраиваемый ресурс, совместимый с данным рабочим процессом подготовки.

7. На вкладке **Жизненный цикл компонента** определите поведение этой схемы элементов при увеличении и уменьшении масштаба, а также при операции уничтожения.

Такие рабочие процессы выполняются на основе развернутой составной схемы элементов, в которой данная схема элементов является одним из компонентов. Доступность различных параметров зависит от схемы элементов. Не для всех рабочих процессов схемы элементов поддерживаются или требуются те или иные параметры.

8. Щелкните элемент **Готово**.

9. Выберите строку вашей схемы элементов и щелкните кнопку **Опубликовать**.

Результаты

Схема элементов Все как услуга создана и опубликована.

Следующие шаги

- Чтобы добавить эту схему элементов как самостоятельную схему непосредственно в каталог служб, добавьте службу, затем добавьте в нее схему элементов. См. раздел [Добавление служб](#).
- Сведения об использовании данной схемы элементов как компонента в составной схеме элементов см. в разделе [Добавление схемы элементов Все как услуга к составной схеме элементов](#).

Параметры мастера схемы элементов Все как услуга «Создать» или «Редактировать»

Эти параметры используются для создания схемы элементов Все как услуга, которая запускает рабочий процесс vRealize Orchestrator при развертывании схемы элементов. Рабочий процесс изменяет целевую систему в среде.

Сведения о действиях, которые необходимо выполнить для создания схемы элементов, см. в разделе [Добавление схемы элементов Все как услуга](#).

Чтобы использовать этот мастер, последовательно выберите **Проект > Все как услуга > Схемы элементов «Все как услуга»**.

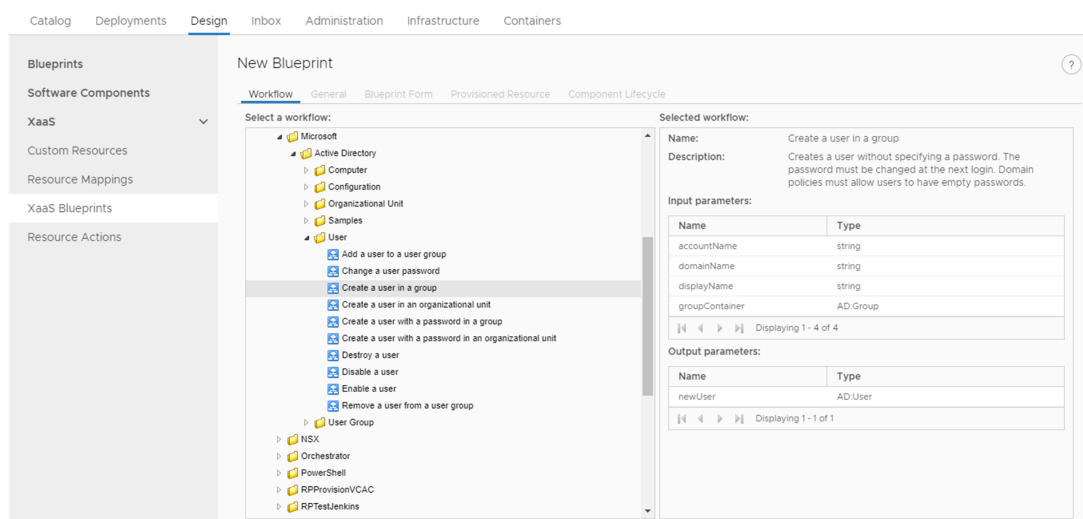
Вкладка «Рабочий процесс»

Выберите рабочий процесс, который выполняется, когда схема элементов подготавливает ресурс.

Эта вкладка недоступна при внесении изменений в схему элементов.

На изображении ниже дерево рабочего процесса расположено слева, а параметры — справа.

Рис. 3-4. Вкладка «Рабочий процесс» в мастере схемы элементов Все как услуга



Проверьте входные и выходные параметры, чтобы убедиться, что вы и ваши пользователи каталога служб сможете указывать правильные значения в следующих обстоятельствах.

- При настройке формы схемы элементов в данном мастере или на холсте проекта схемы элементов.
- Если оставить все входные параметры пустыми, пользователи каталога служб смогут задавать значения.

Вкладка «Общие»

Настройте метаданные о схеме элементов и ее поведение.

Таблица 3-56. Настройки вкладки «Общие»

Параметр	Описание
Имя	<p>Имя схемы элементов, как оно должно отображаться в следующих расположениях:</p> <ul style="list-style-type: none"> ■ холст проекта. При выборе параметра «Сделать доступным в качестве компонента на холсте проекта» это значение является именем, которое появляется в списке категорий. ■ Службы. При использовании данной схемы элементов как самостоятельной это значение является именем, которое отображается при добавлении элементов каталога к службе. ■ Права. Если схема элементов получает права как индивидуальный элемент, это значение является именем, которое отображается в списке «Добавить элементы».
Описание	<p>Подробное описание, которое помогает различать похожие элементы.</p>
Скрыть страницу со сведениями о запросе в каталог	<p>Установите этот флажок, если нет необходимости требовать от пользователей каталога служб предоставлять описание и причину при запросе элемента. Флажок установлен по умолчанию.</p>
Версия	<p>Поддерживаемый формат расширен и имеет вид основной номер.промежуточный номер.номер микровыпуска-номер редакции.</p>
Сделать доступным в качестве компонента на холсте проекта	<p>Если планируется использовать эту схему элементов в качестве компонента в схеме элементов холста проекта, выберите этот параметр.</p> <p>После публикации схема элементов доступна в категории, выбранной при настройке настраиваемого ресурса.</p> <p>Если этот параметр не будет выбран, схема элементов не появится на холсте проекта. Однако ее по-прежнему можно будет добавить к службе и разрешить пользователям развертывать ее в качестве самостоятельной схемы элементов.</p>

Вкладка «Форма схемы элементов»

Поля, появляющиеся на этой странице мастера, являются входными параметрами рабочего процесса. Можно внести одно или несколько из описанных ниже изменений.

- Добавить поля в форму.

- Изменить существующие поля, удалив их или поменяв местами.
- Предоставить значения по умолчанию в качестве входных параметров.

Все изменения влияют на форму, которая представляется следующим адресатам.

- Архитектору приложения, работающему на холсте проекта, если эта схема элементов Все как услуга используется в качестве компонента схемы элементов.
- Пользователю каталога служб, если эта схема элементов опубликована как самостоятельная схема элементов.

Дополнительные сведения о настройке форм см. в разделе [Проектирование формы схемы элементов Все как услуга](#).

Подготовленный ресурс

Подготовленный ресурс связывает схему элементов с соответствующим настраиваемым ресурсом Все как услуга, настроенным на странице «Настраиваемый ресурс» в разделе **Проект > Все как услуга > Настраиваемый ресурс**.

Таблица 3-57. Параметры подготовленного ресурса

Параметр	Описание
Настраиваемый ресурс, созданный ранее	<p>Выберите настраиваемый ресурс, который определяет тип ресурса vRealize Orchestrator, необходимый для запуска схемы элементов подготовки.</p> <p>Схема элементов подготовки запускает рабочий процесс vRealize Orchestrator для подготовки ресурсов на целевой конечной точке с помощью API подключаемого модуля vRealize Orchestrator для этой конечной точки. Например, добавляет виртуальные сетевые адаптеры к сетевому устройству в vSphere.</p> <p>Для этого типа подготовленных ресурсов можно определять операции последующей подготовки. Можно делать схему элементов масштабируемой, добавляя или удаляя экземпляры при необходимости.</p> <p>Результаты</p> <ul style="list-style-type: none"> ■ Эту схему элементов можно масштабировать. ■ Схема элементов появляется на холсте проекта в категории, указанной для выбранного настраиваемого ресурса. ■ Схема элементов отображается на вкладке Развертывания при развертывании схемы элементов, которая ее включает. Вы можете выполнять любые действия с этим элементом после развертывания.
Подготовка отсутствует	<p>Схема элементов операций, не относящихся к подготовке, запускает рабочий процесс vRealize Orchestrator для выполнения задачи, которая не требует от API внесения изменений в конечную точку. Например, создает отчет и отправляет его по электронной почте или публикует его в целевой коммуникационной системе.</p> <p>Результаты</p> <ul style="list-style-type: none"> ■ Эту схему элементов нельзя масштабировать. Схемы элементов операций, не относящихся к подготовке, можно использовать в качестве поддерживающих рабочих процессов в масштабируемых схемах элементов. Например, можно создать схему элементов для обновления подсистемы балансировки нагрузки высокой доступности. ■ Схема элементов появляется в категории Все как услуга на холсте проекта. ■ Эта схема элементов не отображается на вкладке Развертывания при развертывании схемы элементов, которая ее включает. Вы не можете выполнять никаких действий с элементом после развертывания.

Вкладка «Жизненный цикл компонента»

Вкладка «Жизненный цикл компонента» доступна, если на вкладке **Общие** выбран параметр **Сделать доступным в качестве компонента на холсте проекта**.

Эти параметры используются для определения поведения данной схемы элементов после развертывания во время операций увеличения и уменьшения масштаба, когда она используется в качестве компонента в составной схеме элементов.

Доступность различных параметров зависит от схемы элементов. Не для всех рабочих процессов схемы элементов поддерживаются или требуются те или иные параметры. Так как схема Все как услуга может быть использована в составной схеме элементов, необходимо настроить параметры обновления и удаления, а также выделения и освобождения, если они доступны для схемы элементов, чтобы масштаб схемы элементов изменялся правильно.

Таблица 3-58. Параметры жизненного цикла компонента

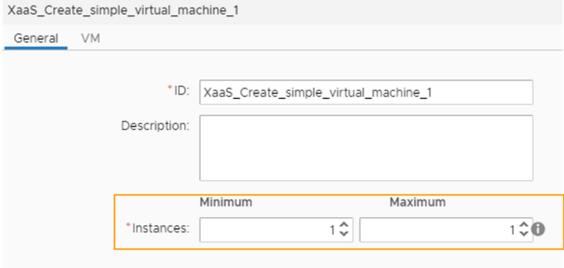
Параметр	Описание
Масштабируемая	<p>Выберите этот параметр, чтобы разрешить пользователю каталога служб изменять количество экземпляров компонента этой схемы элементов после ее развертывания в рамках операции уменьшения или увеличения масштаба.</p> <p>Этот параметр доступен, если на вкладке «Подготовленный ресурс» выбран настраиваемый ресурс, и не доступен, если выбран параметр «Подготовка отсутствует».</p> <p>Если эта схема элементов сделана масштабируемой, параметр «Экземпляры» добавляется на вкладку «Общие» на холсте проекта. См. пример внизу. Если параметр «Масштабируемая» не выбран, параметра «Экземпляры» не будет на холсте проекта.</p> 
Рабочий процесс подготовки	<p>Рабочий процесс, выполняемый во время операции подготовки или увеличения масштаба. Этот рабочий процесс был выбран при создании данной схемы элементов, и это значение нельзя изменить.</p>
Рабочий процесс выделения	<p>Выберите рабочий процесс, выполняемый перед любой начальной операцией подготовки или увеличения масштаба.</p> <p>Этот тип рабочего процесса жизненного цикла доступен для выделений Azure. Если вы создадите рабочий процесс выделения для операции масштабирования, он должен включать следующие значения.</p> <ul style="list-style-type: none"> ■ Входные параметры <ul style="list-style-type: none"> ■ Имя параметра — requestData, тип параметра — Properties. ■ Имя параметра — subtenant, тип параметра — Properties. ■ reservations, тип параметра — Arrays/Properties. ■ Выходной параметр <ul style="list-style-type: none"> ■ Должен включать параметр, в котором тип параметра — Properties.

Таблица 3-58. Параметры жизненного цикла компонента (продолжение)

Параметр	Описание
Рабочий процесс обновления	<p>Выберите рабочий процесс, запускаемый во время операций обновления (включая увеличение или уменьшение масштаба), в котором компонент не является масштабируемым, но может быть обновлен.</p> <p>Например, подсистема балансировки нагрузки обновляется на основе новой конфигурации, созданной с помощью операции увеличения или уменьшения масштаба для любого из компонентов в составной схеме элементов.</p> <p>Рабочий процесс обновления можно применить к компоненту, который привязан к масштабируемому компоненту, но который сам по себе не является масштабируемым. Этот рабочий процесс обновления может изменять немасштабируемый компонент на основании операции обновления.</p> <p>Если вы создаете рабочий процесс обновления для операции масштабирования, он должен включать следующие значения.</p> <ul style="list-style-type: none"> ■ Входные параметры <ul style="list-style-type: none"> ■ Должен быть задан параметр (независимо от его имени), который соответствует типу выходного параметра рабочего процесса подготовки. ■ Имя параметра — <code>data</code>, тип параметра — <code>Properties</code>.
Рабочий процесс удаления	<p>Выберите рабочий процесс, выполняемый во время операции увеличения масштаба или удаления.</p> <p>Если вы создаете рабочий процесс удаления для операции масштабирования, он должен включать следующее значение.</p> <ul style="list-style-type: none"> ■ Входной параметр <ul style="list-style-type: none"> ■ Должен быть задан параметр (независимо от его имени), который соответствует типу выходного параметра рабочего процесса подготовки. <p>Например, если рабочий процесс «Создание» для подготовки простой виртуальной машины включает в себя выходной параметр <code>VC: VirtualMachine</code>, то рабочий процесс удаления должен включать входной параметр, где типом является <code>VC:VirtualMachine</code>.</p>

Таблица 3-58. Параметры жизненного цикла компонента (продолжение)

Параметр	Описание
Рабочий процесс освобождения	<p>Выберите рабочий процесс, выполняемый после любой операции удаления или увеличения масштаба. Если происходит сбой освобождения во время операции, рабочий процесс удаления продолжает работать надлежащим образом.</p> <p>Освобождение — это финальный процесс, когда вы увеличиваете масштаб составной схемы элементов или удаляете ее. Он запускается после операции удаления, освобождая ресурсы.</p> <p>Этот тип рабочего процесса жизненного цикла доступен для выделений Azure. Если вы создаете рабочий процесс освобождения для операции масштабирования, он должен включать следующее значение.</p> <ul style="list-style-type: none"> ■ Входной параметр <ul style="list-style-type: none"> ■ Имя параметра — <code>data</code>, тип параметра — <code>Properties</code>.
Категория	<p>Чтобы указать, где схема элементов Все как услуга появляется на холсте проекта, выберите значение в раскрывающемся меню Категория холста проекта.</p> <p>Если вы не выберете категорию, схема элементов будет добавлена к категории Все как услуга после публикации.</p>

Добавление схемы элементов Все как услуга к составной схеме элементов

Схема элементов Все как услуга добавляется как компонент к составной схеме элементов так же, как компоненты схемы элементов добавляются на холст проекта.

Используйте этот метод для добавления компонента Все как услуга к составной схеме элементов. Эта схема элементов может быть единственным компонентом схемы элементов или же одним из нескольких компонентов в составе схемы элементов приложения.

Если схема элементов Все как услуга — это все, что нужно предоставить пользователям, можно добавить ее в службу и предоставить пользователям разрешение на ее использование, не добавляя эту схему в составную схему элементов.

При увеличении или уменьшении масштаба для развернутой схемы элементов приложения масштаб схемы элементов Все как услуга изменяется в зависимости от ее настроек жизненного цикла.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Создайте и опубликуйте схему элементов Все как услуга. См. раздел [Создание схемы элементов Все как услуга](#). При создании схемы элементов вы указали категорию, к которой она отнесена на холсте проекта.
- Просмотрите способы настройки форм схемы элементов Все как услуга в составной схеме элементов. См. раздел [Проектирование форм для схем элементов Все как услуга и действий](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.

2. Выберите имя схемы элементов, к которой добавляется Все как услуга.

Появится холст проекта. Он содержит текущие схемы элементов компонентов приложений и другие компоненты.

3. В списке «Категории» найдите схему элементов.
4. Перетащите на холст свою схему элементов.
5. Настройте используемые по умолчанию значения на вкладках «Общие» и «Создание».

Эти значения по умолчанию появляются в форме каталога служб, когда пользователь запрашивает элемент.

6. Щелкните элемент **Готово**.
7. Выберите схему элементов и нажмите кнопку **Опубликовать**.

Результаты

Теперь схема элементов Все как услуга входит в составную схему элементов.

Следующие шаги

Добавьте составную схему элементов к службе. См. раздел [Управление каталогом служб](#).

Создание действия ресурса Все как услуга

Действие ресурса позволяет управлять подготовленными элементами с использованием рабочих процессов vRealize Orchestrator.

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Убедитесь в наличии настраиваемого ресурса, который поддерживает это действие. См. раздел [Добавление настраиваемого ресурса Все как услуга](#).
- При создании действий, которые будут выполняться с элементами, неподготовленными в качестве элементов каталога Все как услуга, следует убедиться, что целевые ресурсы сопоставлены. См. раздел [Сопоставление других ресурсов для работы с действиями ресурсов Все как услуга](#).

Процедура

1. Создание действия ресурса

Действие ресурса представляет собой рабочий процесс Все как услуга, который пользователи каталога служб могут выполнять в подготовленных элементах каталога. Разработчик архитектуры Все как услуга может создавать действия ресурсов и с их помощью определять операции, которые потребители могут выполнять с подготовленными элементами.

2. Публикация действия ресурса

Созданное действие ресурса, которое находится в состоянии черновика, необходимо опубликовать.

3. Назначение значка действию ресурса Все как услуга

После создания и публикации действия ресурса можно изменить это действие и назначить ему значок.

Создание действия ресурса

Действие ресурса представляет собой рабочий процесс Все как услуга, который пользователи каталога служб могут выполнять в подготовленных элементах каталога. Разработчик архитектуры Все как услуга может создавать действия ресурсов и с их помощью определять операции, которые потребители могут выполнять с подготовленными элементами.

При создании действия ресурса рабочий цикл vRealize Orchestrator связывается с ним как операция последующей подготовки. Во время этого процесса можно изменять формы отправки и формы только для чтения по умолчанию. См. раздел [Проектирование формы действия ресурса](#).

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Создайте настраиваемый ресурс, который соответствует входному параметру действия ресурса.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите значок **Создать (+)**.
3. Перейдите в библиотеку рабочих процессов vRealize Orchestrator и выберите рабочий процесс, соответствующий настраиваемому ресурсу.

При этом можно просмотреть название и описание выбранного рабочего процесса, а также входные и выходные параметры, определенные в vRealize Orchestrator.

4. Нажмите кнопку **Далее**.
5. Выберите созданный ранее настраиваемый ресурс в раскрывающемся меню **Тип ресурса**.
6. Выберите входной параметр для действия ресурса в раскрывающемся меню **Входной параметр**.
7. Нажмите кнопку **Далее**.
8. Введите имя и, при необходимости, описание.

В текстовые поля **Имя** и **Описание** автоматически подставляются имя и описание рабочего процесса, заданные в vRealize Orchestrator.

9. (дополнительно) Если не нужно требовать, чтобы потребители вводили описание и причину запроса этого действия ресурса, установите флажок **Скрыть страницу со сведениями о запросе в каталог**.
10. Введите версию.

Поддерживаемый формат расширен и имеет вид основной номер.промежуточный номер.номер микровыпуска-номер редакции.

11. (дополнительно) Выберите тип действия.



Параметр	Описание
Списание	Входной параметр рабочего процесса действия с ресурсом удаляется, и элемент удаляется с вкладки Развертывания . Например, действием ресурса может быть удаление подготовленного компьютера.
Подготовка	<p>Действие ресурса — подготовка. Например, действием ресурса может быть копирование элемента каталога.</p> <p>В раскрывающемся меню выберите выходной параметр. При этом можно выбрать настраиваемый ресурс, созданный ранее. В результате, когда клиенты запрашивают это действие с ресурсом, подготовленные элементы добавляются на вкладку Развертывания. Если единственный доступный вариант — Подготовка отсутствует, это свидетельствует о том, что либо действие ресурса отличается от подготовки, либо для выходного параметра не создан надлежащий настраиваемый ресурс, что не позволяет продолжать процедуру.</p>
Подготовить как дочерний ресурс	Можно подготовить ресурс как дочерний по отношению к родительскому ресурсу. При удалении родительского ресурса и масштабировании необходимо сначала решить вопрос с дочерними ресурсами.

В зависимости от рабочего процесса действий можно выбрать один вариант, оба варианта или ни один из вариантов.

12. Выберите условия, при которых действие ресурса доступно пользователям, и нажмите кнопку **Далее**.13. (дополнительно) Измените форму действия ресурса на вкладке **Форма**.

Форма действия ресурса сопоставляется с представлением рабочего процесса vRealize Orchestrator. Чтобы изменить форму, удалите, измените или переставьте местами элементы. Кроме того, можно добавить новую форму и страницы формы, а также перетащить необходимые элементы в новую форму и на страницу формы.

Параметр	Действие
Добавление формы	Щелкните значок Новая форма (+) рядом с именем формы, укажите необходимую информацию и нажмите кнопку Отправить .
Изменение формы	Щелкните значок Изменить (✎) рядом с именем формы, чтобы внести необходимые изменения, и нажмите кнопку Отправить .
Пересоздание представления рабочего процесса	Щелкните значок Пересоздать (↺) рядом с именем формы и нажмите кнопку ОК .
Удаление формы	Щелкните значок Удалить (✖) рядом с именем формы и нажмите кнопку ОК в диалоговом окне подтверждения.
Добавление страницы формы	Щелкните значок Новая страница (+) рядом с именем страницы формы, укажите необходимую информацию и нажмите кнопку Отправить .
Изменение страницы формы	Щелкните значок Изменить (✎) рядом с именем страницы формы, чтобы внести необходимые изменения, и нажмите кнопку Отправить .
Удаление страницы формы	Щелкните значок Удалить (✖) рядом с именем формы и нажмите кнопку ОК в диалоговом окне подтверждения.

Параметр	Действие
Добавление элемента на страницу формы	Перетащите элемент из области «Новые поля» слева в область справа. Затем можно предоставить необходимую информацию и нажать кнопку Отправить .
Редактирование элемента	Щелкните значок Изменить () рядом с элементом, который необходимо изменить, чтобы внести необходимые изменения, и нажмите кнопку Отправить .
Удаление элемента	Щелкните значок Удалить () рядом с элементом, который необходимо удалить, и нажмите кнопку ОК в диалоговом окне подтверждения.

14. Щелкните элемент **Готово**.

Результаты

Вы создали действие ресурса. Теперь оно отображается в списке на странице «Действия ресурсов».

Следующие шаги

Опубликуйте действие ресурса. См. раздел [Публикация действия ресурса](#).

Публикация действия ресурса

Созданное действие ресурса, которое находится в состоянии черновика, необходимо опубликовать.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите строку действия ресурса, которое нужно опубликовать, и нажмите кнопку **Опубликовать**.

Результаты

Состояние действия ресурса изменится на «Опубликовано».

Следующие шаги

Назначьте значок действию ресурса. См. [Назначение значка действию ресурса Все как услуга](#). Диспетчеры бизнес-групп и администраторы арендаторов могут использовать действие при назначении прав.

Назначение значка действию ресурса Все как услуга

После создания и публикации действия ресурса можно изменить это действие и назначить ему значок.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Администрирование > Управление каталогом > Действия**.
2. Выберите созданное действие ресурса.
3. Щелкните элемент **Настроить**.

4. Нажмите кнопку **Обзор** и выберите значок, который необходимо добавить.
5. Нажмите кнопку **Открыть**.
6. Щелкните **Обновить**.

Результаты

Действию ресурса назначен значок. Диспетчеры бизнес-групп и администраторы арендатора могут добавить действие ресурса в качестве права.

Сопоставление других ресурсов для работы с действиями ресурсов Все как услуга

Сопоставление элементов, которые не подготовлены с использованием Все как услуга, позволяет выполнять для них действия ресурсов.

Действия и рабочие процессы сценария сопоставления ресурсов

Можно использовать предоставленные сопоставления ресурсов для виртуальных машин vSphere, vCloud Director или vCloud Air либо создать настраиваемые действия или рабочие процессы сценария vRealize Orchestrator для сопоставления других типов ресурса каталога vRealize Automation с типами иерархии vRealize Orchestrator.

Сопоставления ресурсов, предоставленных с помощью vRealize Automation

vRealize Automation включает в себя сопоставления ресурсов для виртуальных машин инфраструктуры как услуги vSphere, vCloud Director инфраструктуры как услуги и развертывания.

vRealize Automation включает действия сценария сопоставления ресурсов vRealize Orchestrator для каждого из предоставленных сопоставлений ресурсов Все как услуга. Действия сценария предоставленных сопоставлений ресурсов расположены в пакете `com.vmware.vcac.asd.mappings` на встроенном сервере vRealize Orchestrator.

При создании действия ресурсов, которое выполняется на развернутой составной схеме элементов, которая использует рабочий процесс vRealize Orchestrator с `vCACAFE:CatalogResource` в качестве входного параметра, сопоставление развертывания применяется как тип входного ресурса. Сопоставление развертывания применяется только, если выбранный рабочий процесс включает `vCACAFE:CatalogResource` как входной параметр. Например, при создании действия для запроса действия ресурса от имени пользователя, тип ресурса на вкладке «Входной ресурс» будет определен как «Развертывание», потому что данный рабочий процесс использует `vCACAFE:CatalogResource`.

Сопоставления ресурсов виртуальной машины vCD инфраструктуры как услуги и виртуальной машины VC инфраструктуры как услуги используются действием для сопоставления виртуальных машин, которые сопоставляют ресурс инфраструктуры как услуги с виртуальной машиной vRealize Orchestrator vSphere или vCloud Director.

Разработка сопоставлений ресурсов

В зависимости от версии vRealize Orchestrator можно создать рабочий процесс vRealize Orchestrator или действие сценария для сопоставления ресурсов между vRealize Orchestrator и vRealize Automation.

При развертывании сопоставления ресурсов используются входной параметр типа `Properties`, который содержит пару «ключ-значение», определяющую подготовленный ресурс, и выходной параметр типа иерархии vRealize Orchestrator для соответствующего подключаемого модуля vRealize Orchestrator. Свойства, доступные для сопоставления, зависят от типа ресурса. Например, свойство `EXTERNAL_REFERENCE_ID` — это общий ключевой параметр, который определяет отдельные виртуальные машины и может использоваться для запроса ресурса каталога. При создании сопоставления для ресурса, который не использует `EXTERNAL_REFERENCE_ID`, можно использовать одно из других свойств, передаваемых для отдельных виртуальных машин. Например, имя, описание и т. д.

Дополнительные сведения о разработке рабочих процессов и действий сценариев см. в разделе *Разработка с использованием VMware vCenter Orchestrator*.

Создание сопоставления ресурсов

vRealize Automation позволяет выполнять сопоставление ресурсов для компьютеров vSphere, vCloud Director и vCloud Air. Можно создать дополнительные сопоставления для других типов ресурсов каталога.

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Убедитесь, что в vRealize Orchestrator доступен сценарий или рабочий процесс сопоставления. См. [Действия и рабочие процессы сценария сопоставления ресурсов](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Сопоставления ресурсов**.
2. Выберите значок **Создать (+)**.
3. Введите имя и, при необходимости, описание.
4. Введите версию.

Поддерживаемый формат расширен и имеет вид основной номер.промежуточный номер.номер микровыпуска-номер редакции.

5. В текстовом поле **Тип ресурса каталога** введите тип ресурса каталога и нажмите клавишу ВВОД. После этого тип ресурса каталога отобразится в представлении сведений подготовленного элемента.
6. Введите тип объекта vRealize Orchestrator в текстовом поле **Тип объекта оркестратора** и нажмите клавишу ВВОД.

Это выходной параметр рабочего процесса сопоставления ресурсов.

7. (дополнительно) Добавьте целевые критерии для ограничения доступности действий ресурсов, создаваемых с помощью сопоставления ресурсов.

Доступ к действиям ресурсов также можно ограничить с использованием прав и подтверждений.

- а) Выберите **Доступно по условиям**.
- б) Выберите тип условия.

Параметр	Описание
Все из указанного	Если все требования, заданные в предложениях, удовлетворены, действия ресурсов, создаваемые с помощью сопоставления ресурсов, доступны для пользователя.
Что-нибудь из указанного	Если требования, заданные в одном из предложений, удовлетворены, действия ресурсов, создаваемые с помощью сопоставления ресурсов, доступны для пользователя.
Ничего из указанного	Если требования, заданные в предложении, существуют, действия ресурсов, создаваемые с помощью сопоставления ресурсов, недоступны.

- в) Чтобы создать предложения и завершить создание условия, работайте с запросами.

8. В библиотеке vRealize Orchestrator выберите действие сценария сопоставления ресурсов или рабочий процесс.

9. Нажмите кнопку **ОК**.

Проектирование форм для схем элементов Все как услуга и действий

Все как услуга включает в себя конструктор форм, с помощью которого можно проектировать формы отправки данных и формы сведений для схем элементов и действий ресурсов. На основе представления рабочих процессов конструктор форм динамически создает формы и поля по умолчанию, с помощью которых можно изменять стандартные формы.

Вы можете создавать интерактивные формы, которые пользователи будут заполнять при отправке элементов каталога и действий ресурсов. Также можно создавать формы только для чтения, которые определяют, какая именно информация будет доступна в представлении сведений об элементе каталога или о подготовленном ресурсе.

По мере создания настраиваемых ресурсов Все как услуга, схем элементов Все как услуга и действий ресурса генерируются формы для обычных вариантов использования.

Таблица 3-59. Типы объектов Все как услуга и связанные формы

Тип объекта	Форма по умолчанию	Дополнительные формы
Настраиваемый ресурс	Форма сведений о ресурсе на основе атрибутов типа иерархии подключаемого модуля vRealize Orchestrator (только чтение).	■ Нет
Схема элементов Все как услуга	Форма отправки запроса, в основе которой лежит представление выбранного рабочего процесса.	■ Сведения об элементе каталога (только чтение) ■ Сведения об отправленном запросе (только чтение)
Действие ресурса	Форма отправки действия, в основе которой лежит представление выбранного рабочего процесса.	■ Сведения об отправленном действии (только чтение)

Можно изменять формы по умолчанию и создавать новые формы. Перетаскиванием можно добавлять в форму новые поля и изменять их порядок. Можно размещать ограничения для значений определенных полей, указывать значения по умолчанию и добавлять текст с инструкциями для конечного пользователя, который заполняет форму.

Количество операций, с помощью которых можно создавать формы только для чтения, весьма ограничено, если сравнивать их с количеством операций для разработки форм отправки данных.

Поля в конструкторе форм

Компоненты представления рабочего процесса и его возможности можно расширить путем добавления новых предварительно определенных полей в генерируемые по умолчанию формы действий ресурсов и схем элементов Все как услуга.

Если в рабочем процессе vRealize Orchestrator определен входной параметр, в vRealize Automation он будет отображаться в созданной по умолчанию форме. Если в форме не нужно использовать созданные по умолчанию поля, можно удалить их и перетащить новые поля из палитры. Созданные по умолчанию поля можно заменить, не нарушая сопоставления рабочих процессов. Для этого требуется использовать идентификатор заменяемого поля.

Можно также добавить новые поля, кроме тех, которые созданы на основе входных данных рабочего процесса vRealize Orchestrator. Ниже приведены возможные варианты расширения компонентов представления рабочего процесса и его возможностей.

■ Добавление ограничений для существующих полей

Например, можно создать новое раскрывающееся меню и присвоить ему имя `dd`. В это меню можно добавить следующие предварительно определенные значения: `Gold`, `Silver`, `Bronze` и «Пользовательское». При наличии предварительно определенного поля, например «ЦП», для него можно добавить следующие ограничения.

- Если в раскрывающемся меню «`dd`» выбрано значение `Gold`, в поле «ЦП» будет установлено значение «2000 МГц».
- Если в раскрывающемся меню «`dd`» выбрано значение `Silver`, в поле «ЦП» будет установлено значение «1000 МГц».

- Если в раскрывающемся меню «дд» выбрано значение Bronze, в поле «ЦП» будет установлено значение «500 МГц».
- Если в раскрывающемся меню «дд» выбрано значение «Пользовательское», потребитель может указать в поле «ЦП» пользовательское значение.

■ Добавление определений внешнего значения для полей

Для поля можно добавить определение внешнего значения, что дает возможность выполнять действия сценариев vRealize Orchestrator и предоставлять потребителям дополнительные сведения о проектируемых формах. Например, может возникнуть необходимость создать рабочий процесс для изменения параметров брандмауэра виртуальной машины. Нужно добавить возможность изменения параметров открытых портов на странице запроса на действие ресурса. При этом варианты должны ограничиваться лишь открытыми портами. Можно добавить определение внешнего значения для поля двойного списка и выбрать пользовательское действие сценария vRealize Orchestrator, которое запрашивает открытые порты. Во время загрузки формы запроса будет выполняться действие сценария и отобразятся открытые порты в качестве вариантов.

■ Добавление новых полей, которые обрабатываются в качестве глобальных параметров при выполнении рабочего процесса vRealize Orchestrator

Например, во время рабочего процесса осуществляется интеграция с системой стороннего производителя. При этом разработчик этого рабочего процесса настроил общую обработку входных параметров и оставил возможность для передачи настраиваемых полей. К примеру, в поле сценариев обрабатываются все глобальные параметры, которые начинаются с **my3rdparty**. Затем, чтобы передать конкретные значения для потребителей, разработчик архитектуры Все как услуга должен добавить новое поле с именем **my3rdparty_CPU.Все как услуга**.

Таблица 3-60. Новые поля в форме действий ресурсов или схемы элементов Все как услуга

Поле	Описание
Текстовое поле	Однострочное поле
Текстовая область	Многострочное поле
Ссылка	Поле, в котором клиенты вводят URL-адрес. Можно использовать http, https, ftp, mailto или /. Нельзя использовать file://.
Электронная почта	Поле, в котором потребители вводят адрес электронной почты
Поле пароля	Поле, в котором потребители вводят пароль
Поле с целым значением	Текстовое поле, в котором потребители вводят целые числа В это поле можно добавить ползунок с минимальным и максимальным значениями, а также значением приращения.
Поле с десятичным значением	Текстовое поле, в котором потребители вводят десятичные значения В это поле можно добавить ползунок с минимальным и максимальным значениями, а также значением приращения.
Дата и время	Текстовые поля, в которых потребители указывают дату (выбрав в меню календаря) и время (используя стрелки вверх и вниз)

Таблица 3-60. Новые поля в форме действий ресурсов или схемы элементов Все как услуга (продолжение)

Поле	Описание
Двойной список	Построитель списков, в котором потребители перемещают предварительно определенный набор значений между двумя списками: первый список содержит все невыбранные варианты, а второй — выбранные пользователем варианты.
Флажок	Флажок
Да/нет	Раскрывающееся меню для выбора варианта Да или Нет
Раскрывающийся список	Раскрывающееся меню
Список	Список
Список с флажками	Список с флажками
Группа переключателей	Группа переключателей
Поиск	Поле поиска, которое автоматически заполняет запрос. Здесь потребители выбирают объект
Дерево	Дерево, которое используют потребители, чтобы просматривать и выбирать доступные объекты
Сопоставление	Таблица сопоставлений, которую используют потребители, чтобы определить пары «ключ-значение» для свойств

Кроме того, можно использовать поле формы **Заголовок раздела**, чтобы разбить страницы формы на разделы с отдельными заголовками, и поле формы **Текст**, чтобы добавлять информационные тексты только для чтения.

Ограничения и значения в конструкторе форм

Редактируя элемент схемы элементов или форму действия ресурса, можно применить к элементу разные ограничения и значения.

ограничения

Ограничения, которые можно применить к элементу, варьируются в зависимости от типа элемента, который редактируется или добавляется к форме. Некоторые значения ограничений можно настроить в рабочем процессе vRealize Orchestrator. Эти значения не отображаются на вкладке Ограничения, потому что зачастую они зависят от условий, которые оцениваются во время выполнения рабочего процесса. Любые значения ограничений, настроенные для схемы элементов, формируют переопределения любых ограничений, включенных в рабочий процесс vRealize Orchestrator.

После вычисления привязок для поля их минимальные и максимальные значения будут пересчитаны только при запросе схемы элементов.

Какое бы ограничение вы ни применяли к элементу, вы можете выбрать для него один из следующих параметров.

Не задано

Получает свойство от представления рабочего процесса vRealize Orchestrator.

Константа

Задает для редактируемого элемента значение «Обязательно» или «Необязательно».

Поле

Привязывает элемент к другому элементу формы. Например, можно настроить элемент так, чтобы значение «Обязательно» применялось к нему, только если выбран другой элемент, например, если установлен флажок.

Условное

Применение условия. С помощью условий можно создать различные предложения и выражения и применить их к состоянию или ограничениям элементов.

Внешнее

Выберите действие сценария vRealize Orchestrator, определяющее значение.

Таблица 3-61. Ограничения в конструкторе форм

Ограничение	Описание
Обязательно	Обозначается обязательность элемента.
Только для чтения	Указывает, что поле доступно только для чтения.
Значение	Задает значение элемента.
Видимое	<p>Указывает, отображается элемент для покупателя или нет.</p> <p>Если для отображаемой группы в рабочем процессе vRealize Orchestrator задано ограничение видимости, то такое ограничение игнорируется в форме сведений об отправленном запросе Все как услуга, и поля, которые должны быть скрыты, отображаются в форме.</p> <p>Чтобы скрыть поля, которые не следует отображать в форме сведений об отправленном запросе и которые не требуются пользователю, отправляющему запрос, необходимо удалить эти поля из формы сведений об отправленном запросе во вкладке «Схема элементов» в конструкторе схемы элементов Все как услуга. Чтобы найти эту вкладку, см. Добавление новой формы схемы элементов Все как услуга.</p>
Минимальная длина	Задает минимальное количество символов вводимой строки.
Максимальная длина	Задает максимальное количество символов вводимой строки.
Минимальное значение	Задает минимальное значение вводимого числа.
Максимальное значение	Задает максимальное значение вводимого числа.
Приращение	<p>Задает приращение для элемента, например для поля Десятичное или Целое. Например, если нужно, чтобы поле Целое отображалось в качестве элемента Ползунок, можно задать значение для шага.</p>

Таблица 3-61. Ограничения в конструкторе форм (продолжение)

Ограничение	Описание
Минимальное количество	<p>Задаёт минимальное количество выбранных компонентов элемента.</p> <p>Например, добавляя или изменяя Список с флажками, можно задать минимальное количество флажков, которые покупателю нужно установить, чтобы продолжить работу.</p>
Максимальное количество	<p>Задаёт максимальное количество выбранных компонентов элемента.</p> <p>Например, добавляя или изменяя Список с флажками, можно задать максимальное количество флажков, которые покупателю нужно установить, чтобы продолжить работу.</p>

Значения

Вы можете задавать значения для некоторых элементов, тем самым определяя, что увидят потребители в некоторых полях. Доступность параметров зависит от типа редактируемого или добавляемого в форму элемента.

Таблица 3-62. Значения конструктора форм

Значение	Описание
Не задано	Получите значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Предварительно определенные значения	Выберите значения в списке связанных объектов из иерархии vRealize Orchestrator.
Значение	Определите статическое пользовательское значение с метками.
Внешние значения	Выберите действие сценария vRealize Orchestrator, которое определяет значение, используя информацию, которая непосредственно не предоставляется рабочим процессом.

Определения внешнего значения в конструкторе форм

При изменении некоторых элементов в конструкторе форм можно назначить определения внешнего значения, которые используются в настраиваемых действиях сценариев vRealize Orchestrator для предоставления сведений потребителям, не получающим их непосредственно из рабочего процесса.

Например, может возникнуть необходимость опубликовать действие ресурса для установки программного обеспечения на подготовленном компьютере. Вместо предоставления потребителю статического списка всего программного обеспечения, доступного для загрузки, можно динамически заполнить этот список сведениями о программном обеспечении, которое соответствует установленной на компьютере операционной системе, о программном обеспечении, ранее не установленным на компьютере, или об устаревшем программном обеспечении, которому требуется обновление.

Чтобы предоставлять пользовательское динамическое содержимое для потребителя, создайте действие сценария vRealize Orchestrator, которое извлекает необходимые сведения для потребителей. Действие сценария необходимо назначить полю в качестве определения внешнего значения в конструкторе форм. Когда для потребителей открывается форма схемы элементов ресурсов или службы, действие сценария извлекает пользовательские сведения и отображает их для потребителя.

Определения внешнего значения можно использовать для предоставления значений по умолчанию или значений только для чтения, создания логических выражений, определения ограничений или предоставления потребителям функции выбора из обычных списков, списков с флажками и т. п.

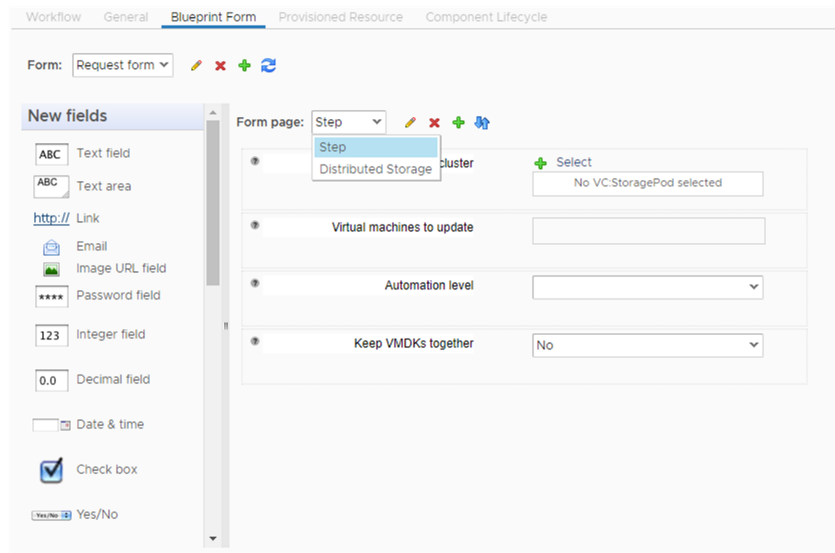
При создании схемы элементов с помощью рабочего процесса, который включает в себя обязательное поле, оно будет обязательным в форме запроса даже в том случае, если сделать его необязательным.

Работа с конструктором форм

При создании схем элементов Все как услуга, действий настраиваемых ресурсов, а также настраиваемых ресурсов можно изменить формы схем элементов, действий и ресурсов с помощью конструктора форм. Можно изменить представление и определить элементы и действия, отображаемые потребителям, когда они запрашивают элемент каталога или выполняют операцию последующей подготовки.

По умолчанию формы схем элементов Все как услуга, действий ресурсов или настраиваемых ресурсов создаются на основе представления рабочего процесса в vRealize Orchestrator.

Шаги в представлении vRealize Orchestrator показаны в виде страниц формы, а группы представления vRealize Orchestrator — в виде отдельных разделов. Типы входных данных выбранного рабочего процесса отображаются в форме в виде различных полей. Например, тип `string` vRealize Orchestrator представлен в виде текстового поля. Сложный тип, к примеру `VC:VirtualMachine`, представлен в виде поля поиска или дерева, чтобы потребители могли ввести значение из букв и цифр для поиска виртуальной машины или выбрать ее.



В конструкторе форм можно изменить вид объекта. Например, можно изменить представление по умолчанию VC:VirtualMachine, заменив поле поиска на дерево. Кроме того, можно добавить новые поля, такие как флажки, раскрывающиеся меню и т. д., а также применить различные ограничения. Если добавленные новые поля недопустимы или неправильно отображаются во входных данных рабочего процесса vRealize Orchestrator, когда пользователь запускает рабочий процесс, vRealize Orchestrator пропускает недопустимые или несопоставленные поля.

Проектирование настраиваемой формы ресурсов

Когда потребители подготавливают настраиваемый ресурс, все поля в форме сведений о ресурсе на странице сведений об элементах доступны им только для чтения. Вы можете выполнять базовые операции редактирования в форме, например удаление, изменение полей или изменение порядка полей. Или же вы можете добавлять новые поля, которые настроены извне и которые используют действия сценария vRealize Orchestrator, чтобы для потребителей отображалась дополнительная доступная только для чтения информация.

■ Изменение элементов настраиваемого ресурса

Изменить характеристики элемента можно на странице «Форма сведений» настраиваемого ресурса. Каждое заданное по умолчанию поле на странице представляет свойство настраиваемого ресурса. Изменить тип свойства или используемые по умолчанию значения нельзя, но можно изменить имя, размер и описание.

■ Добавление новой страницы формы настраиваемого ресурса

Чтобы расположить элементы формы на нескольких вкладках, можно добавить новую страницу.

■ Вставка заголовка раздела в форму настраиваемого ресурса

Чтобы разбить форму на разделы, можно вставить заголовок раздела.

■ Вставка элемента текста в форму настраиваемого ресурса

Чтобы добавить в форму текст описания, можно вставить текстовое поле.

■ Вставка внешне определяемого поля в форму настраиваемого ресурса

Можно вставить новое поле и присвоить ему определение внешнего значения для динамического предоставления сведений только для чтения, которые потребители могут увидеть на странице сведений об элементе при подготовке настраиваемых ресурсов.

Изменение элементов настраиваемого ресурса

Изменить характеристики элемента можно на странице «Форма сведений» настраиваемого ресурса. Каждое заданное по умолчанию поле на странице представляет свойство настраиваемого ресурса. Изменить тип свойства или используемые по умолчанию значения нельзя, но можно изменить имя, размер и описание.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление настраиваемого ресурса Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Щелкните настраиваемый ресурс, чтобы его изменить.
3. Перейдите на вкладку **Форма сведений**.
4. Подведите указатель мыши к элементу, который нужно изменить, и щелкните значок **Изменить**.
5. Чтобы изменить метку, введите новое имя для поля в текстовом поле **Метка**.
6. Измените описание в текстовом поле **Описание**.
7. Выберите параметр в раскрывающемся меню **Размер**, чтобы изменить размер элемента.
8. Выберите параметр в раскрывающемся списке **Размер метки**, чтобы изменить размер метки.
9. Нажмите кнопку **Отправить**.
10. Щелкните элемент **Готово**.

Добавление новой страницы формы настраиваемого ресурса

Чтобы расположить элементы формы на нескольких вкладках, можно добавить новую страницу.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление настраиваемого ресурса Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Щелкните настраиваемый ресурс, чтобы его изменить.
3. Перейдите на вкладку **Форма сведений**.

4. Щелкните значок **Новая страница** (+) рядом с именем **страницы формы**.

5. Выберите неиспользуемый тип экрана и нажмите кнопку **Отправить**.

Если у вас уже есть представление сведений о ресурсах или списка ресурсов, два представления одного и того же типа создать будет нельзя.

6. Нажмите кнопку **Отправить**.

7. Настройте форму.

8. Щелкните элемент **Готово**.

Результаты

Некоторые элементы можно удалить с исходной страницы формы и вставить на новую страницу формы. Кроме того, можно добавить новые поля, в которых для предоставления информации потребителям, не получающим ее непосредственно из рабочего процесса vRealize Orchestrator, используются определения внешних значений.

Вставка заголовка раздела в форму настраиваемого ресурса

Чтобы разбить форму на разделы, можно вставить заголовок раздела.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление настраиваемого ресурса Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Щелкните настраиваемый ресурс, чтобы его изменить.
3. Перейдите на вкладку **Форма сведений**.
4. Перетащите элемент **Заголовок раздела** из области «Формы» в область «Страница формы».
5. Введите имя раздела.
6. Щелкните за пределами элемента, чтобы сохранить изменения.
7. Щелкните элемент **Готово**.

Вставка элемента текста в форму настраиваемого ресурса

Чтобы добавить в форму текст описания, можно вставить текстовое поле.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление настраиваемого ресурса Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Щелкните настраиваемый ресурс, чтобы его изменить.
3. Перейдите на вкладку **Форма сведений**.
4. Перетащите элемент **Текст** из области «Формы» в область «Страница формы».
5. Введите текст, который необходимо добавить.
6. Щелкните за пределами элемента, чтобы сохранить изменения.
7. Щелкните элемент **Готово**.

Вставка внешне определяемого поля в форму настраиваемого ресурса

Можно вставить новое поле и присвоить ему определение внешнего значения для динамического предоставления сведений только для чтения, которые потребители могут увидеть на странице сведений об элементе при подготовке настраиваемых ресурсов.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление настраиваемого ресурса Все как услуга](#).
- Разработайте или импортируйте действия сценария vRealize Orchestrator для предоставления потребителям нужных сведений.

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
 2. Щелкните настраиваемый ресурс, чтобы его изменить.
 3. Перейдите на вкладку **Форма сведений**.
 4. Перетащите элемент из области «Новые поля» в область «Страница формы».
 5. В текстовом поле **Идентификатор** введите идентификатор для элемента.
 6. В текстовом поле **Метка** введите метку.
- Метки отображаются для потребителей в формах.
7. (дополнительно) Выберите тип поля в раскрывающемся меню **Тип**.
 8. Введите тип результата действия сценария vRealize Orchestrator в окне поиска **Тип сущности** и нажмите клавишу ВВОД.

Например, если нужно использовать действие сценария для отображения текущего пользователя, а сценарий возвращает результат типа vRealize OrchestratorLdapUser, введите **LdapUser** в окне поиска **Тип сущности** и нажмите клавишу ВВОД.

9. Щелкните **Добавить внешнее значение**.

10. Выберите настраиваемое действие сценария vRealize Orchestrator.
11. Нажмите кнопку **Отправить**.
12. Нажмите кнопку **Отправить** снова.
13. Щелкните элемент **Готово**.

Результаты

Когда для потребителей открывается форма, действие сценария извлекает пользовательские сведения и отображает их для потребителя.

Проектирование формы схемы элементов Все как услуга

При создании схемы элементов Все как услуга форму схемы элементов можно изменить путем добавления в нее новых полей, изменения существующих полей, удаления или изменения порядка полей. Кроме того, можно создать новые формы и страницы форм и перетащить в них новые поля.

■ [Добавление новой формы схемы элементов Все как услуга](#)

При изменении созданной по умолчанию формы рабочего процесса, который будет опубликован как схема элементов Все как услуга, можно добавить новую форму схемы элементов Все как услуга.

■ [Изменение элемента схемы элементов Все как услуга](#)

Изменить некоторые характеристики элемента можно на странице «Форма схемы элементов» схемы элементов Все как услуга. Можно изменить тип элемента и его значения по умолчанию, а также применить разные ограничения и значения.

■ [Добавление нового элемента](#)

При редактировании созданной по умолчанию формы схемы элементов Все как услуга в эту форму можно добавить предварительно определенный новый элемент. Например, если вы не хотите использовать созданное по умолчанию поле, его можно удалить и заменить новым.

■ [Вставка заголовка раздела в форму схемы элементов Все как услуга](#)

Чтобы разбить форму на разделы, можно вставить заголовок раздела.

■ [Добавление элемента текста в форму схемы элементов Все как услуга](#)

Чтобы добавить в форму текст описания, можно вставить текстовое поле.

Добавление новой формы схемы элементов Все как услуга

При изменении созданной по умолчанию формы рабочего процесса, который будет опубликован как схема элементов Все как услуга, можно добавить новую форму схемы элементов Все как услуга.

При добавлении новой формы схемы элементов Все как услуга определяется оформление страниц сведений об элементе каталога и сведений об отправленном запросе. Если не добавлять сведения об элементе каталога и формы сведений об отправленных запросах, потребители увидят, что определено в форме запроса.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.

■ [Добавление схемы элементов Все как услуга.](#)

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Щелкните схему элементов Все как услуга, которую требуется изменить.
3. Перейдите на вкладку **Форма схемы элементов**.
4. Щелкните значок **Новая форма** (+).
5. Введите имя и, при необходимости, описание.
6. Выберите тип экрана в меню **Тип экрана**.

Параметр	Описание
Сведения об элементе каталога	Страница сведений об элементе каталога, которую видят потребители, когда щелкают элемент каталога.
Форма запроса	Форма схемы элементов Все как услуга по умолчанию. Потребители видят форму запроса, когда запрашивают элемент каталога.
Сведения об отправленном запросе	Страница сведений о запросе, которую видят потребители после запроса элемента, если решают просмотреть сведения о запросе на вкладке Развертывания .

7. Нажмите кнопку **Отправить**.

Следующие шаги

Добавьте необходимые поля, перетаскивая их из области «Новые поля» в область «Страница формы».

Изменение элемента схемы элементов Все как услуга

Изменить некоторые характеристики элемента можно на странице «Форма схемы элементов» схемы элементов Все как услуга. Можно изменить тип элемента и его значения по умолчанию, а также применить разные ограничения и значения.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление схемы элементов Все как услуга.](#)

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Щелкните схему элементов Все как услуга, которую требуется изменить.
3. Перейдите на вкладку **Форма схемы элементов**.
4. Найдите элемент, который требуется изменить.
5. Щелкните значок **Изменить** (✎).

6. Введите новое имя поля в текстовом поле **Метка**, чтобы изменить метку, которая отображается для потребителей.
7. Измените описание в текстовом поле **Описание**.
8. Выберите параметр в раскрывающемся списке **Тип**, чтобы изменить тип отображения элемента.
Параметры отличаются в зависимости от типа редактируемого элемента.
9. Выберите параметр в раскрывающемся меню **Размер**, чтобы изменить размер элемента.
10. Выберите параметр в раскрывающемся списке **Размер метки**, чтобы изменить размер метки.
11. Измените значение по умолчанию для элемента.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Константа	Установка для редактируемого элемента заданной константы в качестве значения по умолчанию.
Поле	Привязка заданного по умолчанию значения элемента к параметру другого элемента из представления.
Условное	Применение условия. С помощью условий можно создать различные предложения и выражения и применить их к элементу.
Внешнее	Выберите действие сценария vRealize Orchestrator, чтобы определить значение.

12. Примените ограничения к элементу на вкладке **Ограничения**.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Константа	Установка для редактируемого элемента заданной константы в качестве значения по умолчанию.
Поле	Привязка заданного по умолчанию значения элемента к параметру другого элемента из представления.
Условное	Применение условия. С помощью условий можно создать различные предложения и выражения и применить их к элементу.
Внешнее	Выберите действие сценария vRealize Orchestrator, чтобы определить значение.

13. Добавьте одно или несколько значений для элемента на вкладке **Значения.**

Доступность параметров зависит от типа редактируемого элемента.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Предварительно определенные значения	<p>Выберите значения в списке связанных объектов из иерархии vRealize Orchestrator.</p> <p>а) Введите значение в поле поиска Предварительно определенные значения, чтобы найти его в иерархии vRealize Orchestrator.</p> <p>б) Выберите значение в результатах поиска и нажмите клавишу ВВОД.</p>
Значение	<p>Определите пользовательские значения с метками.</p> <p>а) В текстовом поле Значение введите значение.</p> <p>б) Введите метку значения в текстовом поле Метка.</p> <p>в) Щелкните значок Добавить (+).</p>
Внешние значения	<p>Выберите действие сценария vRealize Orchestrator, чтобы определить значение, используя информацию, которая непосредственно не предоставляется рабочим процессом.</p> <ul style="list-style-type: none"> ■ Выберите Добавить внешнее значение. ■ Выберите действие сценария vRealize Orchestrator. ■ Нажмите кнопку Отправить.

14. Нажмите кнопку **Отправить.****15. Щелкните элемент **Готово**.**

Добавление нового элемента

При редактировании созданной по умолчанию формы схемы элементов **Все как услуга** в эту форму можно добавить предварительно определенный новый элемент. Например, если вы не хотите использовать созданное по умолчанию поле, его можно удалить и заменить новым.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление схемы элементов Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Щелкните схему элементов **Все как услуга**, которую требуется изменить.
3. Перейдите на вкладку **Форма схемы элементов**.
4. Перетащите элемент из области «Новые поля» в область «Страница формы».
5. Введите идентификатор входного параметра рабочего процесса в текстовом поле **Идентификатор**.

6. В текстовом поле **Метка** введите метку.

Метки отображаются для потребителей в формах.

7. (дополнительно) Выберите тип поля в раскрывающемся меню **Тип**.
8. Введите объект vRealize Orchestrator в текстовом поле **Тип объекта** и нажмите клавишу ВВОД.

Для некоторых типов полей этот шаг необязателен.

Параметр	Описание
Тип результата	Если внешнее значение поля определяется с помощью действия сценария, введите тип результата действия сценария vRealize Orchestrator.
Входной параметр	Если поле используется, чтобы принимать введенные потребителем данные и передавать параметры обратно в vRealize Orchestrator, введите тип входного параметра, который принимает рабочий процесс vRealize Orchestrator.
Выходной параметр	Если поле используется, чтобы отображать информацию для потребителей, введите тип выходного параметра рабочего процесса vRealize Orchestrator.

9. (дополнительно) Установите флажок **Несколько значений**, чтобы потребители могли выбрать несколько объектов.

Для некоторых типов полей этот параметр недоступен.

10. Нажмите кнопку **Отправить**.

11. Щелкните **Обновить**.

Следующие шаги

Элемент можно редактировать, чтобы изменить параметры по умолчанию и применить различные ограничения или значения.

Вставка заголовка раздела в форму схемы элементов Все как услуга
Чтобы разбить форму на разделы, можно вставить заголовок раздела.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление схемы элементов Все как услуга](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Щелкните схему элементов Все как услуга, которую требуется изменить.
3. Перейдите на вкладку **Форма схемы элементов**.
4. Перетащите элемент **Заголовок раздела** из области «Формы» в область «Страница формы».
5. Введите имя раздела.
6. Щелкните за пределами элемента, чтобы сохранить изменения.

7. Щелкните **Обновить**.

Добавление элемента текста в форму схемы элементов Все как услуга

Чтобы добавить в форму текст описания, можно вставить текстовое поле.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Добавление схемы элементов Все как услуга.](#)

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Щелкните схему элементов Все как услуга, которую требуется изменить.
3. Перейдите на вкладку **Форма схемы элементов**.
4. Перетащите элемент **Текст** из области «Новые поля» в область «Страница формы».
5. Введите текст, который необходимо добавить.
6. Щелкните за пределами элемента, чтобы сохранить изменения.
7. Щелкните **Обновить**.

Проектирование формы действия ресурса

При создании действия ресурса можно изменить форму действия путем добавления новых полей в форму, изменения существующих полей, удаления или изменения порядка полей. Кроме того, можно создать новые формы и страницы форм и перетащить в них новые поля.

Добавление новой формы действия ресурса

При изменении созданной по умолчанию формы рабочего процесса, который будет опубликован как действие ресурса, можно добавить форму нового действия ресурса.

При добавлении новой формы действия ресурса определяется внешний вид страницы «Сведения об отправленном действии». Если не добавлять форму сведений об отправленном действии, потребители увидят, что определено в форме действия.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Создание действия ресурса.](#)

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Щелкните действие ресурса, которое требуется изменить.
3. Перейдите на вкладку **Форма**.
4. Щелкните значок **Новая форма (+)**.

5. Введите имя и, при необходимости, описание.
6. Выберите тип экрана в меню **Тип экрана**.

Параметр	Описание
Форма действия	Форма действия ресурса по умолчанию, которую видят потребители при выполнении действия последующей подготовки.
Сведения об отправленном действии	Страница сведений о запросе, которую видят потребители, когда они запрашивают действие и решают просмотреть сведения о запросе на вкладке Развертывания .

7. Нажмите кнопку **Отправить**.

Следующие шаги

Добавьте необходимые поля, перетащив их из области «Новые поля» в область «Страница формы».

Добавление нового элемента в форму действия ресурса

При редактировании созданной по умолчанию формы действия ресурса в эту форму можно добавить предварительно определенный новый элемент. Например, если вы не хотите использовать созданное по умолчанию поле, его можно удалить и заменить новым.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Создание действия ресурса](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Щелкните действие ресурса, которое требуется изменить.
3. Перейдите на вкладку **Форма**.
4. Перетащите элемент из области «Новые поля» в область «Страница формы».
5. Введите идентификатор входного параметра рабочего процесса в текстовом поле **Идентификатор**.
6. В текстовом поле **Метка** введите метку.
Метки отображаются для потребителей в формах.
7. (дополнительно) Выберите тип поля в раскрывающемся меню **Тип**.

8. Введите объект vRealize Orchestrator в текстовом поле **Тип объекта** и нажмите клавишу ВВОД.

Для некоторых типов полей этот шаг необязателен.

Параметр	Описание
Тип результата	Если внешнее значение поля определяется с помощью действия сценария, введите тип результата действия сценария vRealize Orchestrator.
Входной параметр	Если поле используется, чтобы принимать введенные потребителем данные и передавать параметры обратно в vRealize Orchestrator, введите тип входного параметра, который принимает рабочий процесс vRealize Orchestrator.
Выходной параметр	Если поле используется, чтобы отображать информацию для потребителей, введите тип выходного параметра рабочего процесса vRealize Orchestrator.

9. (дополнительно) Установите флажок **Несколько значений**, чтобы потребители могли выбрать несколько объектов.

Для некоторых типов полей этот параметр недоступен.

10. Нажмите кнопку **Отправить**.

11. Щелкните элемент **Готово**.

Следующие шаги

Элемент можно редактировать, чтобы изменить параметры по умолчанию и применить различные ограничения или значения.

Изменение элемента действия ресурса

Изменить характеристики элемента можно на странице «Форма действия» ресурса. Можно изменить тип элемента и его значения по умолчанию, а также применить разные ограничения и значения.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Создание действия ресурса](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Щелкните действие ресурса, которое требуется изменить.
3. Перейдите на вкладку **Форма**.
4. Найдите элемент, который требуется изменить.
5. Щелкните значок **Изменить** (✎).
6. Введите новое имя поля в текстовом поле **Метка**, чтобы изменить метку, которая отображается для потребителей.
7. Измените описание в текстовом поле **Описание**.

8. Выберите параметр в раскрывающемся списке **Тип**, чтобы изменить тип отображения элемента.

Параметры отличаются в зависимости от типа редактируемого элемента.

9. Выберите параметр в раскрывающемся меню **Размер**, чтобы изменить размер элемента.
10. Выберите параметр в раскрывающемся списке **Размер метки**, чтобы изменить размер метки.
11. Измените значение по умолчанию для элемента.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Константа	Установка для редактируемого элемента заданной константы в качестве значения по умолчанию.
Поле	Привязка заданного по умолчанию значения элемента к параметру другого элемента из представления.
Условное	Применение условия. С помощью условий можно создать различные предложения и выражения и применить их к элементу.
Внешнее	Выберите действие сценария vRealize Orchestrator, чтобы определить значение.

12. Примените ограничения к элементу на вкладке **Ограничения**.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Константа	Установка для редактируемого элемента заданной константы в качестве значения по умолчанию.
Поле	Привязка заданного по умолчанию значения элемента к параметру другого элемента из представления.
Условное	Применение условия. С помощью условий можно создать различные предложения и выражения и применить их к элементу.
Внешнее	Выберите действие сценария vRealize Orchestrator, чтобы определить значение.

13. Добавьте одно или несколько значений для элемента на вкладке **Значения**.

Доступность параметров зависит от типа редактируемого элемента.

Параметр	Описание
Не задано	Получение значения редактируемого элемента из представления рабочего процесса vRealize Orchestrator.
Предварительно определенные значения	<p>Выберите значения в списке связанных объектов из иерархии vRealize Orchestrator.</p> <p>а) Введите значение в поле поиска Предварительно определенные значения, чтобы найти его в иерархии vRealize Orchestrator.</p> <p>б) Выберите значение в результатах поиска и нажмите клавишу ВВОД.</p>

Параметр	Описание
Значение	<p>Определите пользовательские значения с метками.</p> <p>а) В текстовом поле Значение введите значение.</p> <p>б) Введите метку значения в текстовом поле Метка.</p> <p>в) Щелкните значок Добавить (+).</p>
Внешние значения	<p>Выберите действие сценария vRealize Orchestrator, чтобы определить значение, используя информацию, которая непосредственно не предоставляется рабочим процессом.</p> <ul style="list-style-type: none"> ■ Выберите Добавить внешнее значение. ■ Выберите действие сценария vRealize Orchestrator. ■ Нажмите кнопку Отправить.

14. Нажмите кнопку **Отправить**.

15. Щелкните **Обновить**.

Вставка заголовка раздела в форму действия ресурса

Чтобы разбить форму на разделы, можно вставить заголовок раздела.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Создание действия ресурса](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Щелкните действие ресурса, которое требуется изменить.
3. Перейдите на вкладку **Форма**.
4. Перетащите элемент **Заголовок раздела** из области «Формы» в область «Страница формы».
5. Введите имя раздела.
6. Щелкните за пределами элемента, чтобы сохранить изменения.
7. Щелкните элемент **Готово**.

Добавление элемента текста в форму действия ресурса

Чтобы добавить в форму текст описания, можно вставить текстовое поле.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **разработчик архитектуры служб «Все как услуга»**.
- [Создание действия ресурса](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Щелкните действие ресурса, которое требуется изменить.
3. Перейдите на вкладку **Форма**.
4. Перетащите элемент **Текст** из области «Новые поля» в область «Страница формы».
5. Введите текст, который необходимо добавить.
6. Щелкните за пределами элемента, чтобы сохранить изменения.
7. Щелкните элемент **Готово**.

Все как услуга Примеры и сценарии

В примерах и сценариях предложены способы применения vRealize Automation для решения общих задач с помощью элементов схем Все как услуга и действий ресурсов.

Создание схемы элементов Все как услуга и действия для создания и изменения пользователя

С помощью Все как услуга можно создавать и публиковать элемент каталога для подготовки пользователя в группе. Кроме того, новую операцию последующей подготовки можно связать с подготовленным пользователем. Например, операцию, позволяющую пользователям каталога служб изменять пароль пользователя.

Разработчик архитектуры Все как услуга создает настраиваемый ресурс, схему элементов Все как услуга и публикует элемент каталога для создания пользователя. Вы также создаете действие ресурса для изменения пароля пользователя.

Как администратор каталога вы создаете службу и включаете в нее элемент каталога схемы элементов. Кроме того, вы редактируете представление рабочего процесса элемента каталога с помощью конструктора форм и изменяете способ просмотра потребителями формы запроса.

Как менеджер бизнес-группы или администратор арендатора вы предоставляете потребителю право на новую созданную службу, элемент каталога и действие ресурса.

Необходимые условия

Убедитесь, что подключаемый модуль Active Directory правильно настроен и вы имеете права на создание пользователей в Active Directory.

Процедура

1. **Создание тестового пользователя в качестве настраиваемого ресурса**

Вы можете создать настраиваемый ресурс и привязать его к типу объекта vRealize OrchestratorAD:User.

2. Создание схемы элементов Все как услуга для создания пользователя

Элемент «Создать пользователя» в схеме элементов Все как услуга группы позволяет выполнять рабочий процесс по добавлению пользователя Active Directory и назначению пользователя группе Active Directory. Схему элементов можно создать как автономную схему элементов Все как услуга или как компонент схемы элементов. В этом сценарии создается автономная схема элементов.

3. Создание действия ресурса для изменения пароля пользователя

Можно создать действие ресурса, чтобы предоставить потребителям службы Все как услуга возможность создавать схему элементов пользователя для изменения пароля пользователя после подготовки пользователя к работе.

4. Создание службы и добавление схемы элементов «Создание тестового пользователя» в службу

Можно создать службу для отображения элемента «Создать каталог пользователя» в каталоге служб.

5. Предоставление права на службу и действие ресурса потребителю

Диспетчеры бизнес-групп и администраторы арендатора могут предоставить пользователю или группе пользователей право на использование службы и действия ресурса. После получения такого права они смогут увидеть эту службу у себя в каталоге и запросить элемент каталога «Создание тестового пользователя», содержащийся в службе. Подготовив элемент, потребители могут запросить изменение пароля пользователя.

Создание тестового пользователя в качестве настраиваемого ресурса

Вы можете создать настраиваемый ресурс и привязать его к типу объекта vRealize OrchestratorAD:User.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Проектирование > Все как услуга > Настраиваемые ресурсы**.
2. Выберите значок **Создать (+)**.
3. В текстовом поле **Тип оркестратора** введите **AD:User** и нажмите клавишу ВВОД.
4. Выберите пункт **AD:User** в списке.
5. Введите имя ресурса.

Например, **тестовый пользователь**.

6. Введите описание ресурса.

Например,

Это тестовый настраиваемый ресурс, который я буду использовать для своего элемента каталога, чтобы создать пользователя в группе.

7. Нажмите кнопку **Далее**.
8. Оставьте в форме значения по умолчанию.
9. Щелкните элемент **Готово**.

Результаты

Вы создали настраиваемый ресурс тестового пользователя, и он отображен на странице «Настраиваемые ресурсы».

Следующие шаги

Создайте схему элементов Все как услуга.

Создание схемы элементов Все как услуга для создания пользователя

Элемент «Создать пользователя» в схеме элементов Все как услуга группы позволяет выполнять рабочий процесс по добавлению пользователя Active Directory и назначению пользователя группе Active Directory. Схему элементов можно создать как автономную схему элементов Все как услуга или как компонент схемы элементов. В этом сценарии создается автономная схема элементов.

Необходимые условия

- Убедитесь, что создается настраиваемое действие ресурса, которое поддерживает подготовку пользователей Active Directory. См. раздел [Создание тестового пользователя в качестве настраиваемого ресурса](#).
- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Проектирование > Все как услуга > Схемы элементов «Все как услуга»**.
2. Выберите значок **Создать (+)**.
3. В области «Выбор рабочего процесса» последовательно выберите **Оркестратор > Библиотека > Microsoft > Active Directory > Пользователь** и выберите рабочий процесс **Создание пользователя в группе**.
4. Нажмите кнопку **Далее**.
5. Настройте параметры вкладки **Общие**.
 - а) Измените имя схемы элементов на **Создание тестового пользователя**, а описание оставьте без изменений.
 - б) Снимите флажок **Сделать доступным в качестве компонента на холсте проекта**.
 Эта схема элементов публикуется непосредственно в каталоге служб, а не используется как компонент схемы элементов на холсте проекта. Какие-либо рабочие процессы уменьшения или увеличения масштаба не нужно настраивать.
 Вкладка **Жизненный цикл компонента** удаляется из интерфейса пользователя.
6. Нажмите кнопку **Далее**.
7. Внесите изменения в форму схемы элементов.
 - а) Щелкните **доменное имя в форме Win2000**.
 - б) Перейдите на вкладку **Ограничения**.

- в) Щелкните стрелку раскрывающегося списка **Значение**, выберите пункт **Константа** в раскрывающемся меню и введите **test.domain**.
- г) Щелкните стрелку раскрывающегося списка **Видимое**, выберите пункт **Константа**, а затем — **Нет** в раскрывающемся меню.

Теперь доменное имя невидимо для потребителей элемента каталога.

- д) Нажмите кнопку **Применить**, чтобы сохранить изменения.
8. Нажмите кнопку **Далее**.
 9. Выберите **newUser [Тестовый пользователь]** как выходной параметр для подготовки.
 10. Нажмите кнопку **Далее**.
 11. Щелкните элемент **Готово**.
 12. На странице **Схемы элементов службы «Все как услуга»** выберите строку **Создание тестового пользователя** и щелкните **Опубликовать**.

Результаты

Создана схема элементов для создания тестового пользователя, которую можно добавить в службу.

Следующие шаги

Создайте действие, которое будет выполняться в отношении учетной записи подготовленного пользователя. См. раздел [Создание действия ресурса для изменения пароля пользователя](#).

Создание действия ресурса для изменения пароля пользователя

Можно создать действие ресурса, чтобы предоставить потребителям службы Все как услуга возможность создавать схему элементов пользователя для изменения пароля пользователя после подготовки пользователя к работе.

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Убедитесь, что создается настраиваемое действие ресурса, которое поддерживает подготовку пользователей Active Directory. См. раздел [Создание тестового пользователя в качестве настраиваемого ресурса](#).

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите значок **Создать (+)**.
3. В библиотеке рабочих циклов vRealize Orchestrator последовательно выберите **Оркестратор > Библиотека > Microsoft > Active Directory > Пользователь** и выберите рабочий цикл **Изменение пароля пользователя**.
4. Нажмите кнопку **Далее**.

5. В раскрывающемся меню **Тип ресурса** выберите пункт **Тестовый пользователь**.
Это созданный ранее настраиваемый ресурс.
6. Выберите **Пользователь** в раскрывающемся меню **Входной параметр**.
7. Нажмите кнопку **Далее**.
8. Измените имя действия ресурса на **Изменение пароля тестового пользователя**, а описание на вкладке **Сведения** оставьте без изменений.
9. Нажмите кнопку **Далее**.
10. (дополнительно) Оставьте форму без изменений.
11. Щелкните элемент **Готово**.
12. На странице «Действия ресурса» выберите строку **Изменить пароль тестового пользователя** и щелкните **Опубликовать**.

Результаты

Создано действие ресурса для изменения пароля пользователя, которое можно добавить в право.

Следующие шаги

Добавьте схему элементов «Создание тестового пользователя» в службу. См. раздел [Создание службы и добавление схемы элементов «Создание тестового пользователя» в службу](#).

Создание службы и добавление схемы элементов «Создание тестового пользователя» в службу
Можно создать службу для отображения элемента «Создать каталог пользователя» в каталоге служб.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Убедитесь, что создана схема элементов Все как услуга. См. раздел [Создание схемы элементов Все как услуга для создания пользователя](#).

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.

Процедура

1. Выберите **Администрирование > Управление каталогом > Службы**.
2. Выберите значок **Создать (+)**.
3. В качестве имени службы введите **Тестовый пользователь Active Directory**.
4. В раскрывающемся меню **Состояние** выберите значение **Активно**.
5. Оставьте другие текстовые поля пустыми.
6. Нажмите кнопку **ОК**.
7. В списке «Службы» выберите строку **Тестовый пользователь Active Directory** и щелкните **Управление элементами каталога**.

8. Выберите значок **Создать** (+).

9. Выберите **Создать тестового пользователя** и нажмите кнопку **ОК**.

Схема элементов «Создание тестового пользователя» Все как услуга добавится в список элементов каталога.

10. Нажмите кнопку **Заккрыть**.

Результаты

Служба «Тестовый пользователь Active Directory» теперь включает схему элементов «Создание тестового пользователя». Действия не нужно добавлять в службы.

Следующие шаги

Можно предоставить пользователям право запрашивать схему элементов и выполнять действие. См. раздел [Предоставление права на службу и действие ресурса потребителю](#).

Предоставление права на службу и действие ресурса потребителю

Диспетчеры бизнес-групп и администраторы арендатора могут предоставить пользователю или группе пользователей право на использование службы и действия ресурса. После получения такого права они смогут увидеть эту службу у себя в каталоге и запросить элемент каталога «Создание тестового пользователя», содержащийся в службе. Подготовив элемент, потребители могут запросить изменение пароля пользователя.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **администратора арендатора** или **диспетчера бизнес-групп**.
- Убедитесь, что схема элементов «Создание пользователя» добавлена в службу. См. раздел [Создание службы и добавление схемы элементов «Создание тестового пользователя» в службу](#).
- Убедитесь, что действие ресурса «Изменение пароля пользователя» существует. См. раздел [Создание действия ресурса для изменения пароля пользователя](#).

Процедура

1. Выберите **Администрирование > Управление каталогом > Права**.
2. Выберите значок **Создать** (+).
3. В текстовом поле **Имя** введите **Создание пользователя Active Directory**.
4. Оставьте текстовые поля **Описание** и **Срок действия** пустыми.
5. В раскрывающемся меню **Состояние** выберите значение **Активно**.
6. В раскрывающемся меню **Бизнес-группа** выберите целевую бизнес-группу.

Например, менеджеры по работе с ИТ-клиентами.

7. Выберите **Все пользователи и группы**, чтобы все члены данной бизнес-группы, например менеджеры по работе с ИТ-клиентами, могли создать учетную запись пользователя.

Для выбранных пользователей отображаются элементы службы и каталога, включенные в службу в каталоге. После создания учетной записи пользователя они могут запускать в отношении нее действие изменения пароля.

8. Нажмите кнопку **Далее**.

9. В текстовом поле **Уполномоченные службы** введите **Тестовый пользователь Active Directory** и нажмите клавишу ВВОД.

10. В текстовом поле **Уполномоченные действия** введите **Изменить пароль тестового пользователя** и нажмите клавишу ВВОД.

11. Щелкните элемент **Готово**.

Результаты

Создано активное право, позволяющее пользователям, которые состоят в бизнес-группах менеджеров по работе с ИТ-клиентами, создавать пользователей. После подготовки пользователя они смогут запускать действие ресурса изменения пароля в отношении подготовленной учетной записи пользователя.

Следующие шаги

Войдите в систему как пользователь с правом создания пользователя Active Directory. Перейдите на вкладку **Каталог** и убедитесь, что с помощью схемы элементов Все как услуга пользователь создается в соответствии с вашим запросом. После создания пользователя запустите действие изменения пароля на вкладке **Развертывания**.

Создание и публикация действия Все как услуга для переноса виртуальной машины

Вы можете создать и опубликовать действие ресурса Все как услуга для расширения операций, которые потребители могут выполнять на подготовленных с помощью Инфраструктура как услуга виртуальных машинах vSphere.

В этом сценарии вы создадите действие ресурса для быстрого переноса виртуальной машины vSphere.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. **Создание действия ресурса для миграции виртуальной машины vSphere**

Можно создать настраиваемое действие ресурса, чтобы предоставить потребителям возможность переносить виртуальные машины vSphere после того, как они подготовят виртуальные машины vSphere с помощью Инфраструктура как услуга.

2. **Публикация действий для перемещения виртуальной машины vSphere**

Чтобы использовать действие ресурса «Быстрое перемещение виртуальной машины» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Создание действия ресурса для миграции виртуальной машины vSphere

Можно создать настраиваемое действие ресурса, чтобы предоставить потребителям возможность переносить виртуальные машины vSphere после того, как они подготовят виртуальные машины vSphere с помощью Инфраструктура как услуга.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Нажмите кнопку **Добавить (+)**.
3. В библиотеке рабочих циклов vRealize Orchestrator последовательно выберите **Оркестратор > Библиотека > vCenter > Управление виртуальными машинами > Перемещение и миграция**, а затем выберите рабочий цикл **Быстрая миграция виртуальной машины**.
4. Нажмите кнопку **Далее**.
5. Выберите пункт **Виртуальная машина VC IaaS** в раскрывающемся меню **Тип ресурса**.
6. Выберите **ВМ** в раскрывающемся меню **Входной параметр**.
7. Нажмите кнопку **Далее**.
8. Оставьте имя действия ресурса и описание на вкладке **Сведения** без изменений.
9. Нажмите кнопку **Далее**.
10. Оставьте форму без изменений.
11. Щелкните элемент **Готово**.

Результаты

Вы создали действие ресурса для миграции виртуальной машины. Теперь это действие отображается в списке на странице «Действия ресурсов».

Следующие шаги

Публикация действий для перемещения виртуальной машины vSphere

Публикация действий для перемещения виртуальной машины vSphere

Чтобы использовать действие ресурса «Быстрое перемещение виртуальной машины» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите строку действия ресурса «Быстрое перемещение виртуальной машины» и нажмите кнопку **Опубликовать**.

Результаты

Вы создали и опубликовали рабочий процесс vRealize Orchestrator в качестве действия ресурса. Теперь можно последовательно выбрать **Администрирование > Управление каталогом > Действия**, чтобы увидеть действие ресурса «Быстрая миграция виртуальной машины» в списке действий. Действию ресурса можно назначить значок. См. раздел [Назначение значка действию ресурса Все как услуга](#).

Следующие шаги

Добавьте действие в права, которые содержат подготовленные для Инфраструктура как услуга виртуальные машины vSphere. См. [Предоставление пользователям права на использование службы, элементов каталога и действий](#).

Создание действия Все как услуга для переноса виртуальной машины с помощью vMotion

Используя Все как услуга, можно создавать и публиковать действие ресурса для переноса подготовленной посредством инфраструктуры IaaS виртуальной машины с помощью vMotion.

В этом сценарии вы создадите действие ресурса для переноса виртуальной машины vSphere с помощью vMotion. Кроме того, вы редактируете представление рабочего процесса с помощью конструктора форм и изменяете способ просмотра потребителями действия при его запросе.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Создание действия для переноса виртуальной машины vSphere с помощью vMotion

Вы можете создать действие настраиваемого ресурса, чтобы пользователи каталога служб могли переносить виртуальную машину vSphere с помощью vMotion после подготовки компьютера с использованием Инфраструктура как услуга.

2. Изменение формы действий ресурса

Форма действия ресурса сопоставляется с представлением рабочего процесса vRealize Orchestrator. Можно изменить форму и задать элементы, которые отображаются для потребителей действия ресурса тогда, когда потребители запускают операцию последующей подготовки.

3. Добавление формы сведений об отправленном действии и сохранение действия

Чтобы определить элементы, отображаемые для потребителей после запроса на выполнение операции последующей подготовки, можно добавить новую форму для действия ресурса «Миграция виртуальной машины с помощью vMotion».

4. Публикация действия для перемещения виртуальной машины с помощью vMotion

Чтобы использовать действие ресурса «Перемещение виртуальной машины с помощью vMotion» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Создание действия для переноса виртуальной машины vSphere с помощью vMotion

Вы можете создать действие настраиваемого ресурса, чтобы пользователи каталога служб могли переносить виртуальную машину vSphere с помощью vMotion после подготовки компьютера с использованием Инфраструктура как услуга.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Нажмите кнопку **Добавить** (+).
3. В библиотеке рабочих процессов vRealize Orchestrator последовательно выберите **Оркестратор > Библиотека > vCenter > Управление виртуальной машиной > Перемещение и миграция**, а затем выберите рабочий процесс **Миграция виртуальной машины с помощью vMotion**.
4. Нажмите кнопку **Далее**.
5. Выберите пункт **Виртуальная машина VC IaaS** в раскрывающемся меню **Тип ресурса**.
6. Выберите **ВМ** в раскрывающемся меню **Входной параметр**.
7. Нажмите кнопку **Далее**.
8. Оставьте имя действия ресурса и описание на вкладке **Сведения** без изменений.
9. Нажмите кнопку **Далее**.

Следующие шаги

Изменение формы действий ресурса.


Изменение формы действий ресурса

Форма действия ресурса сопоставляется с представлением рабочего процесса vRealize Orchestrator. Можно изменить форму и задать элементы, которые отображаются для потребителей действия ресурса тогда, когда потребители запускают операцию последующей подготовки.

Процедура


1. Щелкните значок **Удалить** (✖), чтобы удалить элемент пула.
2. Измените элемент узла.
 - а) Щелкните значок **Изменить** (✎) рядом с раскрывающимся полем **Узел**.
 - б) Введите **Узел назначения** в текстовом поле **Метка**.
 - в) Выберите пункт **Поиск** в раскрывающемся меню **Тип**.
 - г) Перейдите на вкладку **Ограничения**.
 - д) В раскрывающемся меню **Обязательно** выберите **Константа** и введите **Да**.
Теперь поле узла всегда является обязательным.
 - е) Нажмите кнопку **Отправить**.

3. Измените элемент **Приоритет**.

- а) Щелкните значок **Изменить** () рядом с раскрывающимся полем **Приоритет**.
- б) Введите **Приоритет задачи** в текстовом поле **Метка**.
- в) Выберите **Группа переключателей** в раскрывающемся меню **Тип**.
- г) Перейдите на вкладку **Значения** и снимите флажок **Не задано**.
- д) Введите **lowPriority** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- е) Введите **defaultPriority** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- ж) Введите **highPriority** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- з) Нажмите кнопку **Отправить**.

Когда потребители запрашивают действие ресурса, для них отображается группа с тремя переключателями: **lowPriority**, **defaultPriority** и **highPriority**.

4. Измените элемент **Состояние**.

- а) Щелкните значок **Изменить** () рядом с полем **Состояние**.
- б) Введите **Состояние виртуальной машины** в текстовом поле **Метка**.
- в) Выберите пункт **Раскрывающийся список** в раскрывающемся меню **Тип**.
- г) Перейдите на вкладку **Значения** и снимите флажок **Не задано**.
- д) Введите **poweredOff** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- е) Введите **poweredOn** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- ж) Введите **suspended** в текстовом поле поиска **Предварительно определенные значения** и нажмите клавишу ВВОД.
- з) Нажмите кнопку **Отправить**.

Когда потребители запрашивают действие ресурса, для них отображается раскрывающееся меню с тремя пунктами: **poweredOff**, **poweredOn** или **suspended**.

Результаты

Представление рабочего процесса «Перенос виртуальной машины с помощью рабочего процесса vMotion» будет изменено.

Следующие шаги

[Добавление формы сведений об отправленном действии и сохранение действия.](#)

Добавление формы сведений об отправленном действии и сохранение действия

Чтобы определить элементы, отображаемые для потребителей после запроса на выполнение операции последующей подготовки, можно добавить новую форму для действия ресурса «Миграция виртуальной машины с помощью vMotion».

Процедура

1. Щелкните значок **Новая форма** (+) рядом с раскрывающимся меню **Форма**.
2. Введите **Отправленное действие** в текстовом поле **Имя**.
3. Оставьте поле **Описание** пустым.
4. Выберите **Сведения об отправленном действии** в меню **Тип экрана**.
5. Нажмите кнопку **Отправить**.
6. Щелкните значок **Изменить** (✎) рядом с раскрывающимся меню **Страница формы**.
7. Введите **Сведения** в текстовом поле **Заголовок**.
8. Нажмите кнопку **Отправить**.
9. Перетащите элемент **Текст** из области «Формы» на страницу **Форма**.
10. Введите
Вы отправили запрос на миграцию компьютера с помощью vMotion. Дождитесь успешного завершения процесса.
11. Щелкните за пределами текстового поля, чтобы сохранить изменения.
12. Нажмите кнопку **Отправить**.
13. Нажмите кнопку **Добавить**.

Результаты

Вы создали действие ресурса для миграции виртуальной машины с помощью vMotion. Теперь это действие отображается в списке на странице «Действия ресурсов».

Следующие шаги

[Публикация действия для перемещения виртуальной машины с помощью vMotion.](#)

Публикация действия для перемещения виртуальной машины с помощью vMotion

Чтобы использовать действие ресурса «Перемещение виртуальной машины с помощью vMotion» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите строку действия «Перемещения виртуальной машины с помощью vMotion» и нажмите кнопку **Опубликовать**.

Результаты

Вы создали и опубликовали рабочий процесс vRealize Orchestrator в качестве действия ресурса. Теперь можно последовательно выбрать **Администрирование > Управление каталогом > Действия**, чтобы увидеть действие ресурса «Миграция виртуальной машины с помощью vMotion» в списке действий. Действию ресурса можно назначить значок. См. раздел [Назначение значка действию ресурса Все как услуга](#).

Кроме того, можно изменить представление рабочего процесса и определить оформление действия.

Следующие шаги

Диспетчеры бизнес-групп и администраторы арендатора могут добавить действие ресурса «Миграция виртуальной машины с помощью vMotion» в качестве права. Дополнительные сведения о создании и публикации схемы элементов инфраструктуры как услуги для виртуальных платформ, см. в разделе [Проектирование схем элементов компьютера](#).

Создание и публикация действия Все как услуга для создания моментального снимка

С помощью Все как услуга можно создавать и публиковать действие ресурса для создания моментального снимка виртуальной машины vSphere, которая была подготовлена с помощью Инфраструктура как услуга.

В этом сценарии вы создадите действие ресурса для создания моментального снимка виртуальной машины vSphere, подготовленной с помощью Инфраструктура как услуга. Кроме того, вы редактируете представление рабочего процесса с помощью конструктора форм и изменяете способ просмотра потребителями действия при его запросе.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Создание действия для создания моментального снимка виртуальной машины vSphere

Вы можете создать действие настраиваемого ресурса, чтобы клиенты службы могли делать снимок виртуальной машины vSphere после подготовки компьютера с помощью Инфраструктура как услуга.

2. Публикация действий для создания моментального снимка

Чтобы использовать действие ресурса «Создание моментального списка» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Создание действия для создания моментального снимка виртуальной машины vSphere

Вы можете создать действие настраиваемого ресурса, чтобы клиенты службы могли делать снимок виртуальной машины vSphere после подготовки компьютера с помощью Инфраструктура как услуга.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.

2. Нажмите кнопку **Добавить (+)**.
3. В библиотеке рабочих процессов vRealize Orchestrator последовательно выберите **Оркестратор > Библиотека > vCenter > Управление виртуальной машиной > Моментальный снимок**, а затем выберите рабочий процесс **Создание моментального снимка**.
4. Нажмите кнопку **Далее**.
5. Выберите пункт **Виртуальная машина VC IaaS** в раскрывающемся меню **Тип ресурса**.
6. Выберите **ВМ** в раскрывающемся меню **Входной параметр**.
7. Нажмите кнопку **Далее**.
8. Оставьте имя действия ресурса и описание на вкладке **Сведения** без изменений.
9. Нажмите кнопку **Далее**.
10. Оставьте форму без изменений.
11. Нажмите кнопку **Добавить**.

Результаты

Вы создали действие ресурса для создания моментального снимка виртуальной машины. Теперь это действие отображается в списке на странице «Действия ресурсов».

Следующие шаги

[Публикация действий для создания моментального снимка.](#)

Публикация действий для создания моментального снимка

Чтобы использовать действие ресурса «Создание моментального списка» в качестве процедуры последующей подготовки, его необходимо опубликовать.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите строку действия ресурса «Создание моментального списка» и нажмите кнопку **Опубликовать**.

Результаты

Вы создали и опубликовали рабочий процесс vRealize Orchestrator в качестве действия ресурса. Теперь можно последовательно выбрать **Администрирование > Управление каталогом > Действия**, чтобы увидеть действие ресурса «Создание моментального снимка» в списке действий. Действию ресурса можно назначить значок. См. раздел [Назначение значка действию ресурса Все как услуга](#).

Следующие шаги

Диспетчеры бизнес-групп и администраторы арендатора могут добавить действие ресурса «Создание моментального снимка» в качестве права. Дополнительные сведения о создании и публикации схемы элементов инфраструктуры как услуги для виртуальных платформ см. в разделе [Проектирование схем элементов компьютера](#).

Создание и публикация действия Все как услуга для запуска виртуальной машины Amazon

С помощью Все как услуга можно создавать и публиковать действия для расширения операций, которые потребители могут выполнять на сторонних подготовленных ресурсах.

В этом сценарии вы создадите и публикуете действие ресурса для быстрого запуска виртуальных машин Amazon.

Необходимые условия

- Установите подключаемый модуль vRealize Orchestrator для Amazon Web Services на заданном по умолчанию сервере vRealize Orchestrator.
- Создайте или импортируйте рабочий процесс vRealize Orchestrator для сопоставления ресурсов экземпляров Amazon.

Процедура

1. Создание сопоставления ресурсов для экземпляров Amazon

Можно создать сопоставление ресурсов, чтобы связать экземпляры Amazon, подготовленные с помощью Инфраструктура как услуга, с экземпляром AWS:EC2Instance типа vRealize Orchestrator, который предоставляется подключаемым модулем Amazon Web Services.

2. Создание действия ресурса для запуска виртуальной машины Amazon

Можно создать действие ресурса, чтобы потребители могли запускать подготовленные виртуальные машины Amazon.

3. Публикация действий для запуска экземпляров Amazon

Чтобы использовать созданное действие ресурса «Запуск экземпляров» для последующей подготовки на виртуальных машинах Amazon, необходимо опубликовать его.

Создание сопоставления ресурсов для экземпляров Amazon

Можно создать сопоставление ресурсов, чтобы связать экземпляры Amazon, подготовленные с помощью Инфраструктура как услуга, с экземпляром AWS:EC2Instance типа vRealize Orchestrator, который предоставляется подключаемым модулем Amazon Web Services.

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.
- Создайте или импортируйте рабочий цикл сопоставления ресурсов vRealize Orchestrator или действие сценария.

Процедура

1. Выберите **Проектирование > Все как услуга > Сопоставления ресурсов**.
2. Нажмите кнопку **Добавить (+)**.
3. В текстовом поле **Имя** введите **Экземпляр EC2**.
4. В текстовом поле **Тип ресурса каталога** введите **Облачный компьютер**.

5. В текстовом поле **Тип оркестратора** введите **AWS:EC2Instance**.
6. Выберите **Всегда доступно**.
7. Выберите тип сопоставления ресурсов.
8. В библиотеке vRealize Orchestrator выберите настраиваемое действие сценария сопоставления ресурсов или рабочий цикл.
9. Нажмите кнопку **Добавить**.

Результаты

Используя сопоставления ресурсов Amazon, можно создавать действия ресурсов для компьютеров Amazon, подготовленных с помощью инфраструктуры как услуги.

Следующие шаги

[Создание действия ресурса для запуска виртуальной машины Amazon.](#)

Создание действия ресурса для запуска виртуальной машины Amazon

Можно создать действие ресурса, чтобы потребители могли запускать подготовленные виртуальные машины Amazon.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Нажмите кнопку **Добавить (+)**.
3. Последовательно выберите **Оркестратор > Библиотека > Amazon Web Services > Эластичное облако > Экземпляры**, а затем в папке рабочих циклов выберите рабочий цикл **Запуск экземпляров**.
4. Нажмите кнопку **Далее**.
5. В раскрывающемся меню **Тип ресурса** выберите пункт **Экземпляр EC2**.
Это имя ранее созданного сопоставления ресурсов.
6. Выберите **Экземпляр** в раскрывающемся меню **Входной параметр**.
Это входной параметр рабочего цикла действия ресурса, соответствующий сопоставлению ресурсов.
7. Нажмите кнопку **Далее**.
8. Оставьте имя и описание без изменений.
Имя действия ресурса по умолчанию — «Запуск экземпляров».
9. Нажмите кнопку **Далее**.
10. Оставьте поля на вкладке **Форма** без изменений.
11. Нажмите кнопку **Добавить**.

Результаты

Вы создали действие ресурса для запуска виртуальных машин Amazon. Теперь это действие отображается на странице «Действия ресурсов».

Следующие шаги

[Публикация действий для запуска экземпляров Amazon.](#)

Публикация действий для запуска экземпляров Amazon

Чтобы использовать созданное действие ресурса «Запуск экземпляров» для последующей подготовки на виртуальных машинах Amazon, необходимо опубликовать его.

Необходимые условия

Войдите в службу vRealize Automation как **разработчик архитектуры служб «Все как услуга»**.

Процедура

1. Выберите **Проектирование > Все как услуга > Действия ресурсов**.
2. Выберите строку действия ресурса «Запуск экземпляров», которое нужно опубликовать, и нажмите кнопку **Опубликовать**.

Результаты

Состояние действия ресурса «Запуск экземпляров» измениться на «Опубликовано».

Следующие шаги

Добавьте действие «Запуск экземпляров» в право, которое включает элемент каталога Amazon. См.

[Предоставление пользователям права на использование службы, элементов каталога и действий.](#)

Устранение проблем с неправильными ударениями и специальными символами в схемах элементов Все как услуга

При создании схем элементов Все как услуга для языков, которые используют строки, отличные от ASCII, ударения и специальные символы отображаются в виде непригодных строк.

Причина

Свойство конфигурации vRealize Orchestrator, не установленное по умолчанию, может быть включено.

Решение

1. На сервере системы Orchestrator перейдите в каталог `/etc/vco/app-server/`.
2. Откройте файл конфигурации `vmo.properties` в текстовом редакторе.
3. Убедитесь, что следующее свойство деактивировано.

```
com.vmware.o11n.webview.htmlescaping.disabled
```

4. Сохраните файл `vmo.properties`.
5. Перезапустите сервер vRealize Orchestrator.

Публикация схемы элементов

Схемы элементов сохраняются как черновики, и их нужно опубликовать вручную, прежде чем их можно будет настроить как элементы каталога или использовать их как компоненты схемы элементов на холсте проекта.

После публикации схемы элементов можно назначить права на доступ к ней, чтобы ее можно было использовать для запроса на подготовку в каталоге служб.

Схема элементов публикуется только один раз. Любые изменения, внесенные в опубликованную схему элементов, автоматически отражаются в каталоге и компонентах вложенной схемы элементов.

Публикация схемы элементов

Можно опубликовать схему элементов для использования при подготовке компьютеров и при необходимости для повторного использования в другой схеме элементов. Чтобы использовать схему элементов для запроса подготовки компьютеров, после публикации необходимо назначить права на доступ к этой схеме элементов. Для схем элементов, которые используются в качестве компонентов в других схемах элементов, такие права не требуются.

Необходимые условия

- Войдите в службу vRealize Automation как **архитектор инфраструктуры**.
- Создайте схему элементов. См. раздел *Контрольный список для создания схем элементов vRealize Automation*.

Процедура

1. Перейдите на вкладку **Проектирование**.
2. Щелкните элемент **Схемы элементов**.
3. Наведите указатель на схему элементов, которую нужно опубликовать, и нажмите кнопку **Опубликовать**.
4. Нажмите кнопку **ОК**.

Результаты

После публикации схемы элементов в качестве элемента каталога нужно назначить права на доступ к ней, чтобы сделать ее доступной для пользователей в каталоге служб.

Следующие шаги

Добавьте схему элементов в службу каталога и разрешите пользователям запрашивать элемент каталога для подготовки компьютера, как определено в схеме элементов.

Работа со схемами элементов, создаваемыми разработчиками

Помимо создания схем элементов vRealize Automation на основе пользовательского интерфейса, существуют также программные средства работы со схемами элементов, в том числе vRealize CloudClient, возможности работы со схемами элементов, предоставляемыми отдельно или полученными из других источников, а также совместно с другими разработчиками с использованием рабочих процессов и приложений vRealize Suite и сторонних средств.

Дополнительные сведения об этих методах см. в следующих разделах:

- [Экспорт и импорт схем элементов и содержимого](#)
- [Загрузка и настройка стандартной автономной схемы элементов](#)
- [Создание схем элементов и другого контента инфраструктуры как услуги в среде для нескольких разработчиков](#)

Экспорт и импорт схем элементов и содержимого

Можно программно экспортировать схемы элементов и содержимое из одной среды vRealize Automation в другую, используя интерфейс REST API vRealize Automation или vRealize CloudClient.

Например, можно создать и проверить схемы элементов в среде разработки, а затем импортировать их в производственную среду. Помимо этого, можно импортировать определение свойства с форума сообщества в активный экземпляр арендатора vRealize Automation.

Можно программно импортировать и экспортировать любой из следующих элементов содержимого vRealize Automation.

- Схемы элементов приложения и все их компоненты
- схемы элементов компьютеров Инфраструктура как услуга
- Компоненты Программное обеспечение
- схемы элементов Все как услуга
- Профили компонентов
- Группы свойств

Информация о группе свойств зависит от конкретного арендатора и импортируется в составе схемы элементов, если данная группа свойств уже существует в целевом экземпляре vRealize Automation.

При экспорте схемы элементов из одного экземпляра арендатора vRealize Automation в другой информация о группе свойств, определенная для этой схемы элементов, не распознается в импортированной схеме элементов, пока данная группа свойств существует в целевом экземпляре арендатора. Например, если импортировать схему элементов, содержащую группу свойств с именем `micd1`, группа свойств `micd1` не будет представлена в импортируемой схеме элементов, пока группа свойств `micd1` существует в экземпляре vRealize Automation, в который импортирована эта схема. Чтобы избежать потери информации о группе свойств при экспорте схемы элементов из одного экземпляра vRealize Automation в другой, используйте vRealize CloudClient для создания ZIP-файла пакета

экспорта, содержащего группу свойств, а затем импортируйте этот пакет ZIP в целевой арендатор, прежде чем импортировать схему элементов. Для получения дополнительных сведений об использовании vRealize CloudClient для создания списка, упаковки, экспорта и импорта групп свойств, а также других элементов vRealize Automation посетите Центр разработчиков VMware по адресу <https://developercenter.vmware.com/tool/cloudclient>.

Таблица 3-63. Выбор средства импорта и экспорта

Средство	Дополнительная информация
vRealize CloudClient	См. страницу vRealize CloudClient на сайте VMware code.vmware.com по адресу https://developercenter.vmware.com/tool/cloudclient .
vRealize Automation REST API	См. документацию по API в VMware API Explorer для vRealize Automation по адресу https://code.vmware.com/apis/vrealize-automation .

Примечание При программном экспорте и импорте схемы элементов между развертываниями vRealize Automation, например из тестовой среды в производственную или из одной организации в другую, важно помнить, что в пакет включены данные шаблона клона. При импорте пакета схемы элементов, настройки по умолчанию заполняются на основе информации, содержащейся в пакете. Например, если выполняется экспорт, а затем импорт схемы элементов, которая была создана с помощью рабочего процесса на основе клонирования, а шаблон, из которого получены данные клона, не существует в конечной точке развертывания vRealize Automation, куда импортируется схема элементов, некоторые параметры импортированной схемы элементов для этого развертывания применяться не будут.

Сценарий: импорт образца приложения Dukes Bank для vSphere и его настройка для среды

ИТ-специалисту, оценивающему или изучающему vRealize Automation, нужно импортировать образец надежного приложения в экземпляр vRealize Automation, чтобы быстро ознакомиться с имеющимися функциями и определить способ создания схем элементов vRealize Automation, которые отвечают потребностям организации.

Необходимые условия

- Подготовьте эталонный компьютер CentOS 6.x Linux, преобразуйте его в шаблон и создайте спецификацию настройки. См. [Сценарий: подготовка к импорту схемы элементов образца приложения Dukes Bank для vSphere](#).
- Создайте внешний профиль сети, задав шлюз и диапазон IP-адресов. См. [Создание профиля внешней сети с помощью стороннего поставщика управления IP-адресами](#).
- Сопоставьте профиль внешней сети с резервированием vSphere. См. [Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer](#). Образец приложения нельзя успешно подготовить без внешнего профиля сети.

- Убедитесь, что вам предоставлены привилегии как **архитектора инфраструктуры**, так и **программного архитектора**. Обе роли необходимы для импорта примера приложения Dukes Bank и взаимодействия с программными компонентами, а также схемами элементов Dukes Bank.

Процедура

1. Сценарий: импорт образца приложения Dukes Bank для vSphere

Приложение Dukes Bank для vSphere загружается с устройства vRealize Automation. Образец приложения импортируется в арендатор vRealize Automation для просмотра работающего образца многоуровневой схемы элементов vRealize Automation, которая включает в себя несколько компонентов компьютера, а также сетевые и программные компоненты.

2. Сценарий: настройка образцов компонентов vSphere Dukes Bank для среды

Пользуясь привилегиями архитектора инфраструктуры, можно настроить каждый компонент компьютера Dukes Bank для использования спецификации настройки, шаблона и префиксов компьютера, созданных для среды.

Результаты

Образец приложения Dukes Bank для vSphere настроен для среды в качестве отправной точки для разработки собственных схем элементов, инструмента для оценки vRealize Automation или учебного материала, который позволит разобраться в функциях и компонентах vRealize Automation.

Сценарий: импорт образца приложения Dukes Bank для vSphere

Приложение Dukes Bank для vSphere загружается с устройства vRealize Automation. Образец приложения импортируется в арендатор vRealize Automation для просмотра работающего образца многоуровневой схемы элементов vRealize Automation, которая включает в себя несколько компонентов компьютера, а также сетевые и программные компоненты.

Процедура

1. Выполните вход в устройство vRealize Automation по протоколу SSH, используя права пользователя root.
2. Загрузите Dukes Bank для образца приложения vSphere из устройства vRealize Automation в каталог /tmp.

```
wget --no-check-certificate https://vRealize_VA_Hostname_fqdn:5480/blueprints/
DukesBankAppForvSphere.zip
```

Не распаковывайте пакет.

3. Загрузите vRealize CloudClient по ссылке <http://developercenter.vmware.com/tool/cloudclient> в каталог /tmp.
4. Распакуйте пакет cloudclient-4x-dist.zip.
5. Запустите vRealize CloudClient из каталога /bin.

```
$>./bin/cloudclient.sh
```

6. При появлении запроса примите условия лицензионного соглашения.
7. Войдите в устройство vRealize Automation в качестве пользователя с правами **программного архитектора** и **архитектора инфраструктуры**, используя vRealize CloudClient.

```
CloudClient>vra login userpass --server https://vRealize_VA_Hostname_fqdn --user
<user@domain.com> --tenant <Имя_арендатора>
```

8. При появлении запроса введите пароль для входа.
9. Убедитесь, что содержимое файла DukesBankAppForvSphere.zip доступно.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run true --resolution OVERWRITE
```

Обратите внимание, что в записи «ПЕРЕЗАПИСАТЬ» учитывается регистр. Ее нужно вводить заглавными буквами.

Если при настройке разрешения указать операцию перезаписи, а не *пропуск*, vRealize Automation сможет устранять конфликты в случаях, когда это возможно.

10. Импортируйте образец приложения Dukes Bank.

```
vra content import --path /<Path>/DukesBankAppForvSphere.zip --dry-run false --resolution
OVERWRITE
```

Обратите внимание, что в записи «ПЕРЕЗАПИСАТЬ» учитывается регистр. Ее нужно вводить заглавными буквами.

Результаты

При входе в консоль vRealize Automation в качестве пользователя с привилегиями архитектора инфраструктуры и программного архитектора схемы элементов и компоненты программного обеспечения Dukes Bank будут отображаться на вкладках **Проектирование > Схемы элементов** и **Проектирование > Компоненты программного обеспечения**.

Сценарий: настройка образцов компонентов vSphere Dukes Bank для среды

Пользуясь привилегиями архитектора инфраструктуры, можно настроить каждый компонент компьютера Dukes Bank для использования спецификации настройки, шаблона и префиксов компьютера, созданных для среды.

В этом сценарии настраиваются компоненты компьютера для клонирования компьютеров из шаблона, созданного в веб-клиенте vSphere. Если нужно создать компактные копии виртуальной машины на основе снимка, это можно сделать с помощью примера приложения, которое также поддерживает связанные клоны. Связанные клоны используют цепочку дельта-дисков, чтобы отслеживать отличия от родительского компьютера. Их можно быстро подготовить, они позволяют снизить расходы на хранилище и идеально подходят для случаев, когда производительность не является основным приоритетом.

Процедура

1. Войдите в консоль vRealize Automation в качестве **архитектора инфраструктуры**.

Можно настроить пример приложения Dukes Bank для работы в среде только для роли **архитектора инфраструктуры**. Но если требуется просмотреть или изменить компоненты программного обеспечения, необходимо также использовать роль **программного архитектора**.

2. Выберите **Проектирование > Схемы элементов**.
3. Выберите схему элементов **DukesBankApplication** и щелкните значок **Изменить**.
4. Измените appserver-node, чтобы решение vRealize Automation могло подготовить этот компонент компьютера в среде.

Настройте схему элементов, чтобы подготовить несколько экземпляров компонента этого компьютера. Это позволит проверять работоспособность узла подсистемы балансировки нагрузки.

- а) Щелкните компонент **appserver-node** на холсте проекта.

На нижней панели отобразятся сведения о конфигурации.

- б) В раскрывающемся меню **Префикс компьютера** выберите префикс компьютера.
- в) Настройте схему элементов для подготовки от двух до десяти экземпляров этого узла. Для этого выберите по крайней мере два экземпляра, но не больше десяти.

В форме запроса пользователи могут подготовить от двух до десяти узлов сервера appserver. Если пользователи уполномочены выполнять действия уменьшения и увеличения масштаба, они могут масштабировать свое развертывание для соответствия изменяющимся потребностям.

- г) Откройте вкладку **Информация о сборке**.
- д) Выберите **CloneWorkflow** в раскрывающемся меню **Рабочий процесс подготовки**.
- е) В диалоговом окне **Объект для клонирования** выберите **dukes_bank_template**.
- ж) В текстовом поле **Спецификации настройки** введите имя **Customspecs_sample**.

В этом поле учитывается регистр.

- з) Перейдите на вкладку **Ресурсы компьютера**.
- и) Убедитесь, что указан объем памяти не менее 2048 МБ.

5. Измените loadbalancer-node, чтобы решение vRealize Automation могло подготовить этот компонент компьютера в среде.

- а) Щелкните компонент **loadbalancer-node** на холсте проекта.
- б) В раскрывающемся меню **Префикс компьютера** выберите префикс компьютера.
- в) Откройте вкладку **Информация о сборке**.
- г) Выберите **CloneWorkflow** в раскрывающемся меню **Рабочий процесс подготовки**.
- д) В диалоговом окне **Объект для клонирования** выберите **dukes_bank_template**.

- е) В текстовом поле **Спецификации настройки** введите имя **Customspecs_sample**.

В этом поле учитывается регистр.

- ж) Перейдите на вкладку **Ресурсы компьютера**.
- з) Убедитесь, что указан объем памяти не менее 2048 МБ.

6. Повторите этап для компонента компьютера **database-node**.

7. Щелкните элементы **«Сохранить»** и **«Готово»**.

Изменения сохраняются и снова отображается вкладка **Схемы элементов**.

8. Выберите схему элементов **DukesBankApplication** и нажмите кнопку **Опубликовать**.

Результаты

Теперь схема элементов в образце приложения Dukes Bank настроена для среды, а ее окончательный вариант опубликован.

Следующие шаги

Опубликованные схемы элементов не отображаются в каталоге для пользователей, пока служба каталога не будет настроена, схема элементов не будет добавлена в службу, а пользователям не будут предоставлены права для запроса схемы элементов. См. раздел [Контрольный список для настройки каталога служб](#).

После настройки схемы элементов Dukes Bank для отображения в каталоге можно запросить подготовку образца приложения. См. раздел [Сценарий: тестирование образца приложения Dukes Bank](#).

Сценарий: тестирование образца приложения Dukes Bank

Для проверки изменений и просмотра функциональности схемы элементов vRealize Automation будет запрошен элемент «Dukes Bank» и выполнен вход в образец приложения.

Необходимые условия

- Импортируйте образец приложения Dukes Bank и настройте компоненты схемы элементов для работы в вашей среде. См. раздел [Сценарий: импорт образца приложения Dukes Bank для vSphere и его настройка для среды](#).
- Настройте каталог служб и предоставьте пользователям право запрашивать опубликованную схему элементов Dukes Bank. См. раздел [Контрольный список для настройки каталога служб](#).
- Убедитесь, что у подготавливаемых виртуальных машин имеется доступ к репозиторию yum .

Процедура

- 1.** Выполните вход в консоль vRealize Automation в качестве пользователя, имеющего права на элемент каталога Dukes Bank.
- 2.** Откройте вкладку **Каталог**.
- 3.** Найдите элемент каталога образца приложения Dukes Bank и нажмите **Запрос**.

4. Заполните необходимые сведения по запросу для каждого компонента, отмеченные красной звездочкой.

- а) Перейдите к компоненту JBossAppServer и заполните необходимые сведения по запросу.
- б) Введите полное доменное имя устройства vRealize Automation в текстовом поле **app_content_server_ip**.
- в) Перейдите к компонентам ПО Dukes_Bank_App и заполните необходимые сведения по запросу.
- г) Введите полное доменное имя устройства vRealize Automation в текстовых полях **app_content_server_ip**.

5. Нажмите кнопку **Отправить**.

Процесс полной подготовки образца приложения Dukes Bank может занять примерно 15-20 минут в зависимости от сети и экземпляра vCenter Server. Можно отслеживать данный статус на вкладке **Развертывания**. После подготовки приложения можно посматривать сведения об элементе каталога на вкладке **Развертывания**.

6. Чтобы получить доступ к образцу приложения Dukes Bank после его подготовки, уточните IP-адрес сервера подсистемы балансировки нагрузки.

- а) Нажмите **Развертывания**.
- б) Найдите развертывание примера приложения Dukes Bank и нажмите имя этого развертывания.
- в) На вкладке **Компоненты** выберите сервер Apache для балансировки нагрузки.
- г) Перейдите на вкладку **Сеть**.
- д) Запишите IP-адрес.

7. Выполните вход в образец приложения Dukes Bank.

- а) Перейдите на сервер подсистемы балансировки нагрузки по адресу `http://IP_Apache_Load_Balancer:8081/bank/main.faces`.

Если требуется прямой доступ к серверам приложений, можно перейти на `http://IP_AppServer:8080/bank/main.faces`.

- б) В текстовом поле **Имя пользователя** введите **200**.
- в) В текстовом поле **Пароль** введите **foobar**.

Результаты

Образец работающего приложения Dukes Bank настроен для использования в качестве отправной точки для разработки собственных схем элементов, инструмента для оценки vRealize Automation или учебного материала, который позволит разобраться в функциях и компонентах vRealize Automation.

Загрузка и настройка стандартной автономной схемы элементов

Стандартную автономную схему элементов и связанные с ней программные компоненты можно загрузить с устройства vRealize Automation.

В документе [Загрузка и настройка автономной схемы элементов vRealize Automation](#) описан процесс загрузки автономной схемы элементов vRealize Automation с устройства vRealize Automation и дальнейшего импорта, настройки и использования этой схемы элементов в vRealize Automation в сочетании с несколькими рабочими процессами vRealize Orchestrator.

Создание схем элементов и другого контента инфраструктуры как услуги в среде для нескольких разработчиков

Несколько разработчиков могут использовать рабочие процессы vRealize Orchestrator, vRealize Suite и сторонние инструменты, чтобы одновременно работать с различными артефактами vRealize Automation одной или разных схем элементов vRealize Automation.

С помощью таких инструментов, как vRealize Suite Lifecycle Manager, можно облегчить использование сред для нескольких разработчиков для vRealize Automation, других решений vRealize Suite и OVA, а также сторонних инструментов, например GitLab/itHub, Houdini и других артефактов приложений из [VMware Solutions Exchange](#).

Подробную информацию о создании схем элементов vRealize Automation и другого содержимого инфраструктуры как услуги, например свойств, подписок брокера событий, компонентов ПО и рабочих процессов vRealize Orchestrator в среде с несколькими разработчиками, см. в следующих материалах.

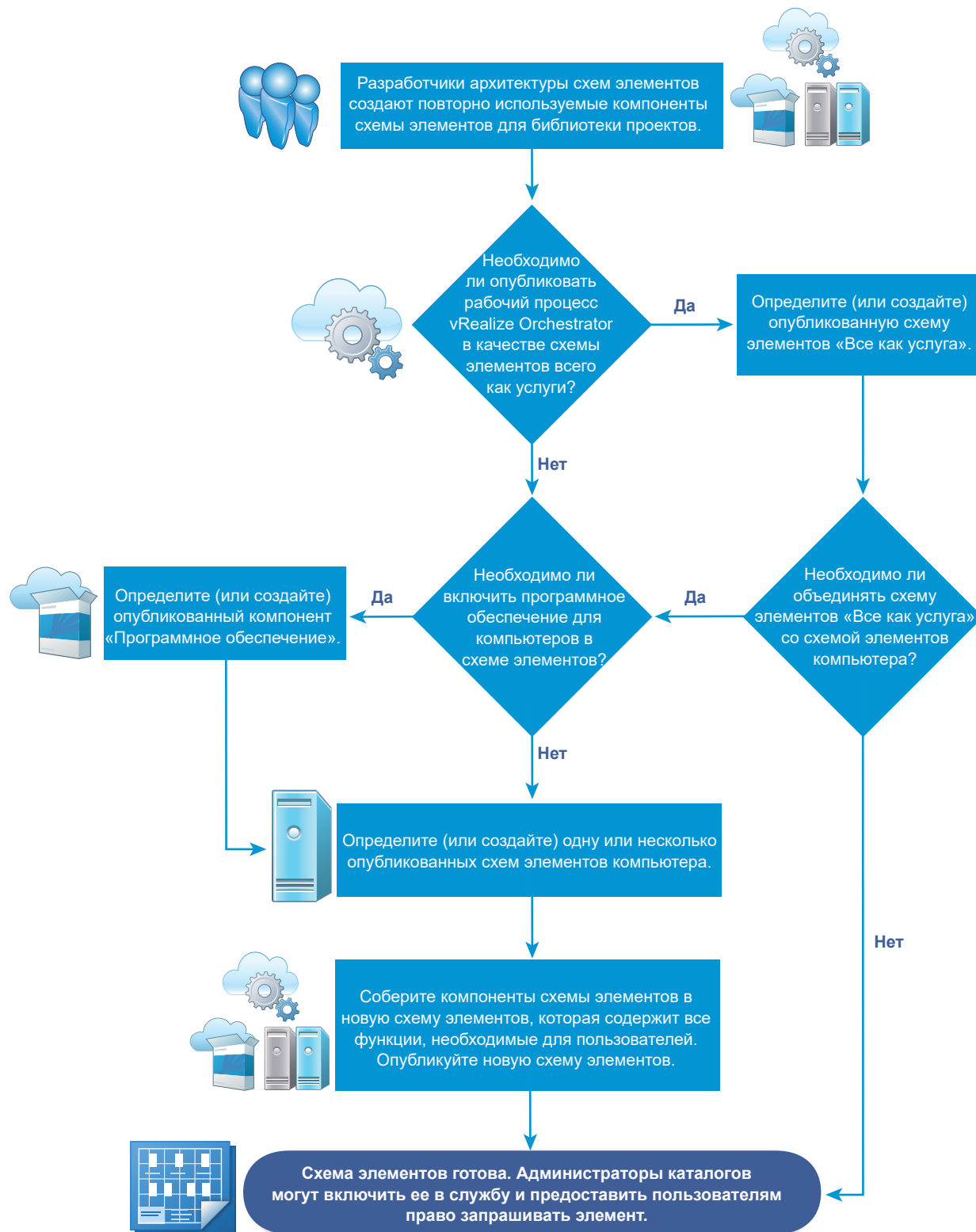
- [Видео «Нововведения Lifecycle Manager»](#)
- [Публикация в блоге «vRealize Automation со схемой элементов инфраструктуры. Конфигурация среды для нескольких разработчиков»](#)
- Документ [Загрузка и настройка стандартной автономной схемы элементов](#)
- [Публикация в блоге «Lifecycle Manager с интеграцией GitLab»](#)
- [Публикация в блоге «Обзор LifeCycle Manager»](#)

Сборка составных схем элементов

Повторно используя опубликованные схемы элементов и компоненты схем элементов и по-новому объединяя их, можно создать пакеты ИТ-услуг, обеспечивающие пользователям более специализированные функциональные возможности.

Если существуют настраиваемые формы для схем элементов компонентов, настраиваемые формы запросов не применяются к новой схеме элементов. Необходимо создать новые формы для новой схемы элементов. Подробные сведения о настраиваемых формах запросов см. в разделе [Настройка форм запроса схем элементов](#).

Рис. 3-5. Рабочий процесс сборки составных схем элементов



■ Общие сведения о поведении вложенных схем элементов

Можно повторно использовать схемы элементов, вкладывая их в другую схему элементов в качестве компонента. Схемы элементов вкладываются для управления повторным использованием и применением модулей при подготовке компьютера, но есть правила и особенности работы со вложенными схемами элементов.

- **Использование компонентов компьютера и компонентов Программное обеспечение при сборке схемы элементов**

Компоненты Программное обеспечение предоставляются путем размещения их на поддерживаемых компонентах компьютера при сборке схем элементов.

- **Создание привязки свойств между компонентами схемы элементов**

В нескольких сценариях развертывания для настройки одного компонента требуется значение свойства другого компонента. Свойства Все как услуга, компьютеров, Программное обеспечение и настраиваемые свойства можно связать с другими свойствами в схеме элементов.

- **Создание зависимостей и управление порядком подготовки**

Если информация из одного из компонентов схемы элементов необходима для завершения подготовки другого компонента, можно нарисовать явную зависимость на холсте проекта для организации подготовки таким образом, чтобы зависимый компонент не подготавливался преждевременно. Явные зависимости управляют порядком сборки развертывания и запускают зависимые обновления при выполнении операций увеличения или уменьшения масштаба.

Программные компоненты в схеме элементов должны быть упорядочены.

Общие сведения о поведении вложенных схем элементов

Можно повторно использовать схемы элементов, вкладывая их в другую схему элементов в качестве компонента. Схемы элементов вкладываются для управления повторным использованием и применением модулей при подготовке компьютера, но есть правила и особенности работы со вложенными схемами элементов.

Схема элементов с одной или несколькими вложенными схемами элементов называется внешней схемой элементов. Если схема элементов добавляется в качестве компонента на холст проекта во время создания или изменения другой схемы элементов, компонент схемы элементов называется вложенной схемой элементов, а схема элементов контейнера, в которую добавляется этот компонент, называется внешней схемой элементов.

Использование вложенных схем элементов характеризуется особенностями, которые не всегда очевидны. Чтобы эффективно использовать все возможности подготовки компьютера, важно понимать правила и особенности использования вложенных схем элементов.

Общие правила и особенности использования вложенных схем элементов

- Чтобы упростить работу со схемами элементов, следует сократить количество используемых уровней до трех, одним из которых должна быть схема элементов верхнего уровня.
- Если у пользователя есть права доступа к внешней схеме элементов, такой пользователь также может получить доступ к ее вложенным схемам элементов.

- К схеме элементов можно применить политику подтверждения. После подтверждения выполняется подготовка элемента каталога схемы элементов и всех его компонентов, в том числе вложенных схем элементов. К разным компонентам можно применить разные политики подтверждения. Перед подготовкой запрошенной схемы элементов необходимо подтвердить все политики подтверждения.
- При изменении опубликованной схемы элементов развертывания, которые уже подготовлены с использованием этой схемы элементов, не изменяются. При подготовке полученное развертывание считывает текущие значения из схемы элементов, в том числе из вложенных схем элементов. Единственные изменения, которые можно внести в подготовленные развертывания, — это изменения программных компонентов, например изменения в сценарии обновления или удаления.
- Параметры, заданные во внешней схеме элементов переопределяют параметры, настроенные во вложенных схемах элементов, за исключением описанных далее случаев.
 - Можно изменить имя вложенной схемы элементов, но нельзя изменить имя содержащегося в ней компонента компьютера или любого другого компонента.
 - Нельзя добавлять или удалять настраиваемые свойства для компонента компьютера во вложенной схеме элементов. Однако эти настраиваемые свойства можно изменять. Нельзя добавлять, изменять или удалять группы свойств для компонента компьютера во вложенной схеме элементов.
- Внесенные вами или другим архитектором изменения параметров вложенных схем элементов отображаются во внешних схемах элементов, если эти параметры не переопределены во внешней схеме элементов.
- Установите для максимального времени аренды внешней схемы элементов наименьшее максимальное значение аренды схемы элементов компонента.

Хотя для времени аренды, указанного во вложенной и внешней схемах элементов, можно установить любое значение, максимальное время аренды во внешней схеме элементов не должно превышать минимальное значение среди максимальных периодов аренды вложенных схем элементов. Это позволяет разработчику архитектуры приложений проектировать составную схему элементов с унифицированными и переменными значениями времени аренды, но в пределах ограничений, определенных архитектором инфраструктуры. Если максимальное значение времени аренды, определенное во вложенной схеме элементов, меньше указанного во внешней схеме, произойдет сбой запроса на подготовку.

- Во время работы во внешней схеме элементов можно переопределить параметры ресурсов компьютера, настроенные для компонента компьютера во вложенной схеме элементов.
- Во время работы во внешней схеме элементов можно перетаскивать программный компонент в компонент компьютера во вложенной схеме элементов.
- Если открыть схему элементов, в которой компонент компьютера во вложенной схеме элементов был удален или его ИД был изменен, и этот компонент компьютера был связан с компонентами в текущей схеме элементов, связанные компоненты будут удалены и отобразится такое или подобное сообщение:

Компонент компьютера во вложенной схеме элементов, на которую ссылаются компоненты в текущей схеме элементов, был удален или ИД компонента компьютера изменился. Все компоненты в текущей схеме элементов, которые были связаны с отсутствующим или измененным ИД компонента компьютера, удалены. Нажмите кнопку «Отмена», чтобы сохранить историю связей между

отсутствующим или измененным ИД компонента компьютера во вложенной схеме элементов и компонентами в текущей схеме элементов и исправить проблему во вложенной схеме элементов. Откройте вложенную схему элементов и повторно добавьте отсутствующий компонент компьютера с оригинальным ИД или укажите оригинальный ИД компонента компьютера. Нажмите кнопку «Сохранить», чтобы удалить историю связей между отсутствующим или измененным ИД компонента компьютера во вложенной схеме элементов и компонентами в текущей схеме элементов.

- При публикации схемы элементов данные компонента программного обеспечения обрабатываются как моментальный снимок. Если позже внести изменения в свойства компонента программного обеспечения, то только новые свойства будут распознаны схемой элементов, в которой находится этот компонент программного обеспечения. Изменения свойств, существовавших в компоненте программного обеспечения на момент публикации схемы элементов, не обновляются в этой схеме. В схеме элементов наследуются только свойства, добавленные после публикации самой схемы. Однако можно внести изменения в экземпляры компонента программного обеспечения в схемах элементов, в которых находится этот компонент, чтобы изменить конкретную схему элементов.

Правила и особенности сети и безопасности для вложенных схем элементов

- Компоненты сети и безопасности во внешних схемах элементов можно связать с компьютерами, которые определены во вложенных схемах элементов.
- Компоненты сети, безопасности и подсистемы балансировки нагрузки NSX и их параметры не поддерживаются во вложенных схемах элементов.
- Применение изоляции приложения во внешней схеме элементов переопределяет параметры изоляции приложения, указанные во вложенной схеме элементов.
- Параметры транспортной зоны, определенные во внешней схеме элементов, переопределяют соответствующие параметры во вложенных схемах элементов.
- Во время работы во внешней схеме элементов можно настроить параметры подсистемы балансировки нагрузки относительно параметров компонента сети и компьютера, которые настроены во внутренней или вложенной схеме элементов.
- Во внешней схеме элементов невозможно изменить диапазоны IP-адресов, указанные в компоненте сети NAT по требованию, который содержится во вложенной схеме элементов.
- Внешняя схема элементов не может содержать внутреннюю схему элементов, в которой находятся настройки сети по требованию или настройки подсистемы балансировки нагрузки по требованию. Не поддерживается использование внутренней схемы элементов, в которой содержатся компонент сети NSX по требованию или компонент подсистемы балансировки нагрузки NSX по требованию.
- Нельзя изменить сведения о профиле сети или о политике безопасности, указанные во вложенной схеме элементов, в которой содержатся компоненты сети и безопасности NSX. Однако эти параметры можно повторно использовать для других компонентов компьютера vSphere, добавленных во внешнюю схему элементов.
- Чтобы у компонентов сети и безопасности NSX во вложенных схемах элементов были уникальные имена в составной схеме элементов, vRealize Automation добавляет идентификатор вложенной схемы элементов сети в виде префикса к неуникальным именам компонентов сети и безопасности.

Например, если добавить схему элементов с именем идентификатора `xbp_1` во внешнюю схему элементов и при этом в обеих схемах содержится компонент группы безопасности по требованию с именем `OD_Security_Group_1`, на холсте проекта схемы элементов компоненту во вложенной схеме элементов будет назначено имя `xbp_1_OD_Security_Group_1`. К именам компонентов сети и безопасности во внешней схеме элементов не добавляются префиксы.

- Параметры компонента могут варьироваться в зависимости от того, в какой схеме элементов он находится. Например, если включить группы безопасности, теги безопасности или сети по требованию одновременно на внутреннем и внешнем уровнях схемы элементов, параметры внешней схемы элементов переопределяют параметры внутренней. Компоненты сети и безопасности поддерживаются только на уровне внешней схемы элементов (это не касается существующих сетей, работающих на уровне внутренней схемы элементов). Чтобы избежать проблем, добавляйте все группы безопасности, теги безопасности и сети по требованию только во внешнюю схему элементов.

Особенности программных компонентов для вложенных схем элементов

Для масштабируемых схем элементов рекомендуется создавать однослойные схемы элементов, которые не используют другие схемы элементов. Обычно процессы обновления во время операций масштабирования запускаются неявными зависимостями, например зависимостями, которые создаются при привязке программного свойства к свойству компьютера. Однако неявные зависимости во вложенной схеме элементов не всегда запускают процессы обновления. Если необходимо использовать вложенные схемы элементов в масштабируемой схеме элементов, можно вручную нарисовать зависимости между компонентами вложенной схемы элементов для создания явных зависимостей, которые всегда запускают обновление.

Использование компонентов компьютера и компонентов Программное обеспечение при сборке схемы элементов

Компоненты Программное обеспечение предоставляются путем размещения их на поддерживаемых компонентах компьютера при сборке схем элементов.

Чтобы обеспечить поддержку компонентов Программное обеспечение, выбранная схема элементов компьютера должна содержать компонент компьютера, который создан на основе шаблона, моментального снимка или образа компьютера Amazon и содержит гостевой агент и агент начальной загрузки Программное обеспечение, а также использовать поддерживаемый метод подготовки.

Поскольку агенты Программное обеспечение не поддерживают интернет-протокол версии 6 (IPv6), используйте параметры IPv4.

Примечание Зависимости между программными компонентами в схеме элементов должны быть упорядочены. Неупорядоченные программные компоненты в схеме элементов могут привести к сбою подготовки. Если между программными компонентами нет упорядоченных зависимостей, можно создать между ними искусственные зависимости, чтобы выполнить требование схемы элементов по упорядочиванию компонентов.

Если схемы элементов проектируются масштабируемыми, рекомендуется создавать однослойные схемы элементов, в которых не используются другие схемы элементов. Обычно процессы обновления, используемые во время операций масштабирования, инициируются неявными зависимостями, такими как привязки свойств. Однако неявные зависимости во вложенной схеме элементов не всегда запускают процессы обновления.

Архитекторы инфраструктуры как услуги, разработчики архитектуры приложений и программные архитекторы могут собирать схемы элементов, а архитекторы инфраструктуры как услуги могут настраивать компоненты компьютера. Пользователь, не являющийся архитектором инфраструктуры как услуги, не может настраивать компоненты своего компьютера, но он может использовать схемы элементов компьютера, которые создал и опубликовал архитектор инфраструктуры как услуги.

Чтобы добавить компоненты программного обеспечения на холст проекта, требуются также права участника бизнес-группы, администратора бизнес-группы или администратора арендатора для доступа к целевому каталогу.

Если необходимо использовать вложенные схемы элементов в масштабируемой схеме элементов, можно вручную нарисовать зависимости между компонентами вложенной схемы элементов для создания явных зависимостей, которые всегда запускают обновление.

Примечание При публикации схемы элементов данные компонента программного обеспечения обрабатываются как моментальный снимок. Если позже внести изменения в свойства компонента программного обеспечения, то только новые свойства будут распознаны схемой элементов, в которой находится этот компонент программного обеспечения. Изменения свойств, существовавших в компоненте программного обеспечения на момент публикации схемы элементов, не обновляются в этой схеме. В схеме элементов наследуются только свойства, добавленные после публикации самой схемы. Однако можно внести изменения в экземпляры компонента программного обеспечения в схемах элементов, в которых находится этот компонент, чтобы изменить конкретную схему элементов.

Таблица 3-64. Методы подготовки, которые поддерживают Программное обеспечение

Тип компьютера	Способ подготовки
vSphere	Клонирование
vSphere	Связанный клон
vCloud Director	Клонирование
vCloud Air	Клонирование
Amazon Web Services	Образ компьютера Amazon

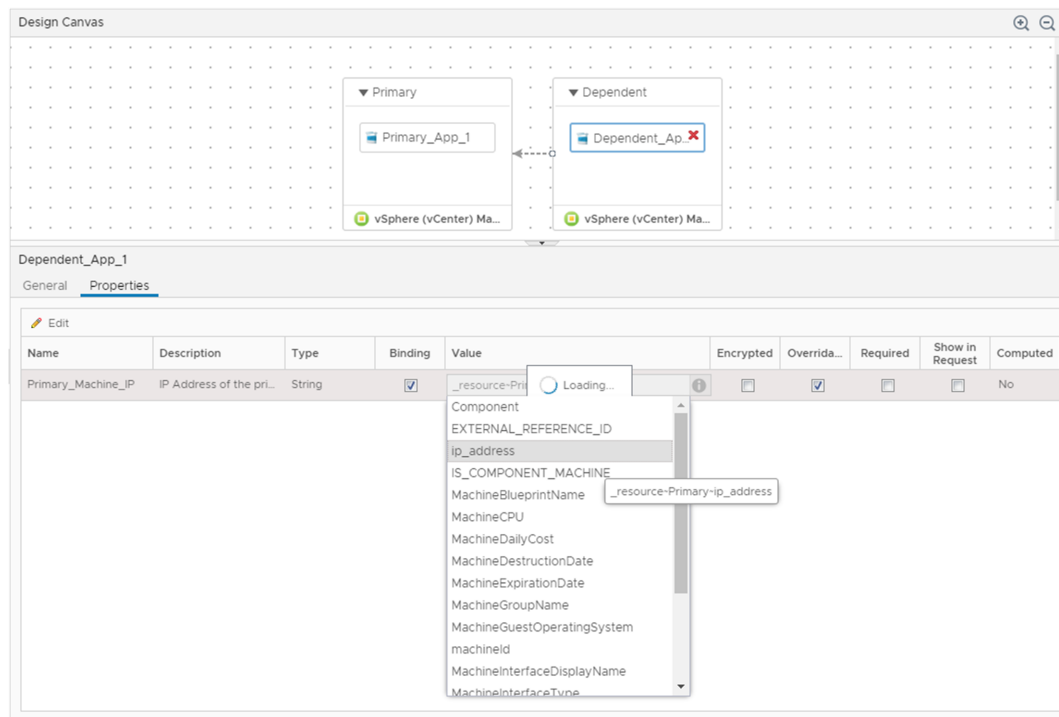
Создание привязки свойств между компонентами схемы элементов

В нескольких сценариях развертывания для настройки одного компонента требуется значение свойства другого компонента. Свойства Все как услуга, компьютеров, Программное обеспечение и настраиваемые свойства можно связать с другими свойствами в схеме элементов.

Например, программный архитектор может изменить определения свойств в сценариях жизненного цикла компонента WAR. Для компонента WAR, возможно, потребуется задать расположение установки компонента сервера Apache Tomcat, поэтому программному архитектору нужно настроить компонент WAR и установить значение свойства `server_home` для свойства `install_path` сервера Apache Tomcat. Архитектору, выполняющему сборку схемы элементов, необходимо привязать свойство `server_home` к свойству `install_path` сервера Apache Tomcat, чтобы успешно подготовить компонент Программное обеспечение.

Привязки свойств можно установить во время настройки компонентов в схеме элементов. На странице «Схема элементов» перетащите компонент на холст и выберите вкладку **Свойства**. Чтобы привязать свойство к другому свойству в схеме элементов, установите флажок **Привязать**. Можно ввести `ComponentName~PropertyName` в текстовом поле значения или щелкнуть стрелку вниз, чтобы создать список доступных параметров привязки. Символ тильды «~» используется в качестве разделителя компонентов и свойств. Например, чтобы привязать свойство к свойству `dp_port` программного компонента MySQL, можно ввести `mysql~db_port`. Чтобы привязать свойства, настроенные во время подготовки, например IP-адрес компьютера или имя узла компонента Программное обеспечение, введите `resource~ComponentName~PropertyName`. Например, чтобы выполнить привязку к имени резервирования компьютера, можно ввести `_resource~vSphere_Machine_1~MachineReservationName`.

Рис. 3-6. Привязка программного свойства к IP-адресу компьютера



Создание зависимостей и управление порядком подготовки

Если информация из одного из компонентов схемы элементов необходима для завершения подготовки другого компонента, можно нарисовать явную зависимость на холсте проекта для организации подготовки таким образом, чтобы зависимый компонент не подготавливался преждевременно. Явные зависимости

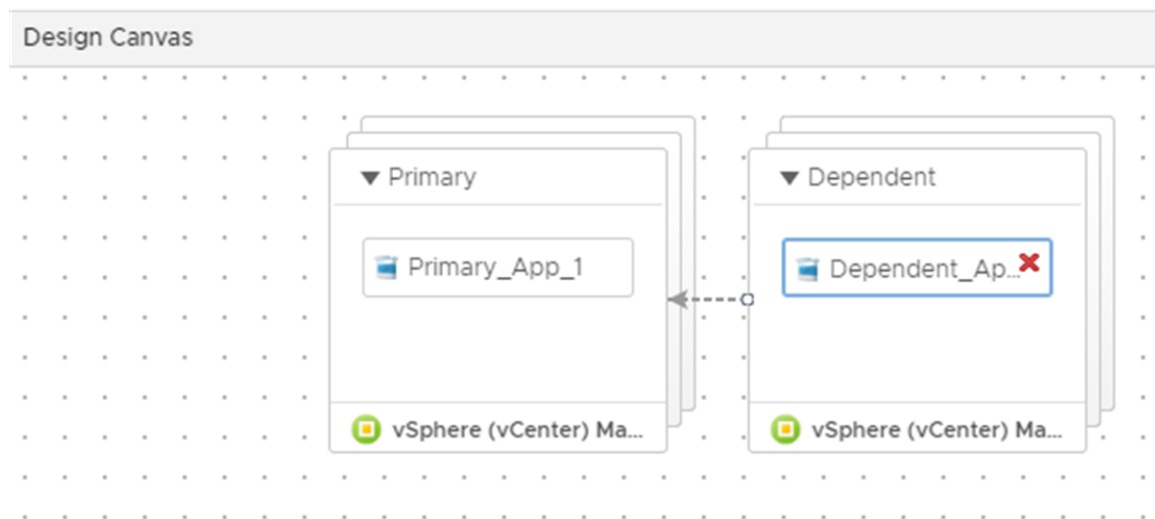
управляют порядком сборки развертывания и запускают зависимые обновления при выполнении операций увеличения или уменьшения масштаба. Программные компоненты в схеме элементов должны быть упорядочены.

При проектировании схемы элементов с несколькими компьютерами и приложениями свойства с одного компьютера могут требоваться для завершения установки приложения на другом. Например, при создании веб-сервера вам необходимо получить имя узла сервера базы данных до установки приложения и создания экземпляров таблиц баз данных. Если сопоставить явную зависимость, подготовка сервера базы данных начнется после завершения подготовки веб-сервера.

Примечание Зависимости между программными компонентами в схеме элементов должны быть упорядочены. Неупорядоченные программные компоненты в схеме элементов могут привести к сбою подготовки. Если между программными компонентами нет упорядоченных зависимостей, можно создать между ними искусственные зависимости, чтобы выполнить требование схемы элементов по упорядочиванию компонентов.

Чтобы сопоставить зависимость на холсте проекта, нужно провести линию от зависимого компонента до компонента, от которого тот зависит. По окончании компонент, который нужно собрать вторым, будем иметь стрелку, указывающую на компонент, который нужно собрать первым. Например, на рисунке «Управление порядком сборки путем сопоставления зависимостей» зависимый компьютер подготавливается только после создания основного компьютера. Также можно настроить одновременную подготовку обоих компьютеров, но при этом нарисовать зависимость между компонентами программного обеспечения.

Рис. 3-7. Управление порядком сборки путем сопоставления зависимостей



Если схемы элементов проектируются масштабируемыми, рекомендуется создавать однослойные схемы элементов, в которых не используются другие схемы элементов. Обычно процессы обновления во время операций масштабирования запускаются неявными зависимостями, например зависимостями, которые создаются при привязке программного свойства к свойству компьютера. Однако неявные зависимости во

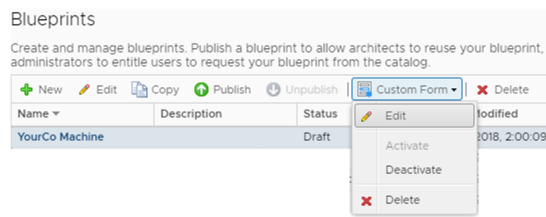
вложенной схеме элементов не всегда запускают процессы обновления. Если необходимо использовать вложенные схемы элементов в масштабируемой схеме элементов, можно вручную нарисовать зависимости между компонентами вложенной схемы элементов для создания явных зависимостей, которые всегда запускают обновление.

Настройка форм запроса схем элементов

В каждой создаваемой и публикуемой схеме элементов отображается форма, которая используется при запросе схемы элементов из каталога. Можно использовать форму по умолчанию или настроить индивидуальные формы запроса схемы элементов при ее создании или редактировании. Настройка формы выполняется тогда, когда данные, указанные или требуемые в форме по умолчанию, не соответствуют тому, что должны видеть пользователи.

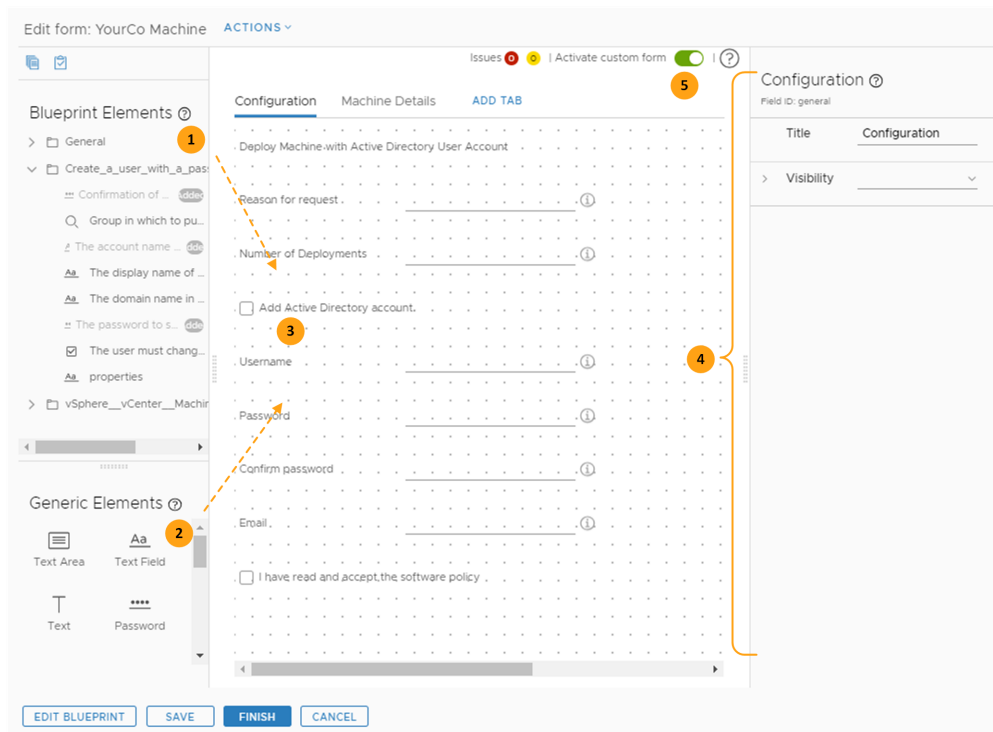
Настройка формы запроса

Доступ к конструктору настраиваемых форм запроса осуществляется из сетки данных схемы элементов или с холста схемы элементов.



Конструктор настраиваемых форм запросов

Конструктор форм используется для создания настраиваемых форм.



Порядок создания настраиваемой формы:

1. Перетащите элементы (1 и 2) на холст проекта (3).
2. Настройте каждый элемент с помощью панели свойств (4).
3. Активируйте форму (5).

Если свойство запрета перезаписи не настроено, то в списке элементов схемы элементов будут содержаться настраиваемые свойства. Если для параметра свойства «Допускает переопределение» выбрано значение «Нет», это поле невозможно настроить.

Проверка и ограничения

Конструктор настраиваемых форм позволяет выполнять проверку данных путем добавления ограничений к полю или с помощью внешних средств проверки. Варианты ограничений, которые применяются при создании формы, см. в разделе [Свойства полей в конструкторе настраиваемых форм](#).

- Пример ограничения см. в разделе [Создание настраиваемой формы запроса с параметрами Active Directory](#).
- Сведения о внешней проверке см. в разделе [Использование внешней проверки в конструкторе настраиваемых форм](#).

При добавлении проверки и зависимостей в формы запрашивающий пользователь должен заполнить поля или система должна их проверить. В противном случае зависимые поля могут не появиться в форме.

Например, если у вас есть поля на первой вкладке, от которых зависят последующие поля, зависимые поля могут не отображаться на вкладках, пока на предыдущих вкладках не будет указано зависимое значение.

Действия в настраиваемых формах запроса

Элементы меню действий помогают заполнять формы и совместно использовать их с другими системами.

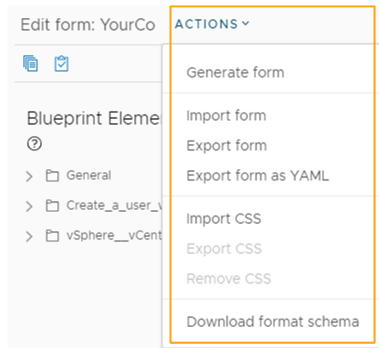


Таблица 3-65. Элементы меню действий в настраиваемой форме запроса

Элемент меню действий	Описание
Создать форму	<p>Добавляет все поля, связанные с каждым компонентом схемы элементов, в конструктор форм. Каждый компонент добавляется на вкладку. При использовании этого элемента меню после создания или изменения формы вновь созданная форма перезаписывает текущую форму.</p> <p>При использовании этого элемента меню можно скрыть или удалить поля, которые не должны отображаться в каталоге для пользователей. Если вы не создаете форму, вы все равно можете добавлять и настраивать текстовые поля, которые будут видны пользователям.</p>
Импортировать форму	Импорт настраиваемой формы из файла JSON или YAML.
Экспортировать форму	<p>Экспорт текущей настраиваемой формы в файл JSON.</p> <p>Экспорт файла выполняется, если вы хотите использовать его часть, которая соответствует компоненту, используемому в другой схеме элементов.</p>
Экспортировать форму как файл YAML	<p>Экспорт текущей настраиваемой формы в формате YAML.</p> <p>Экспорт в файл YAML выполняется, когда необходимо переместить настраиваемую форму из одного экземпляра vRealize Automation в другой. Например, из тестовой среды в производственную среду. Если вы хотите отредактировать форму в формате YAML, можно экспортировать ее, изменить и импортировать обратно в схему элементов.</p>

Таблица 3-65. Элементы меню действий в настраиваемой форме запроса (продолжение)

Элемент меню действий	Описание
Импортировать CSS	<p>Импорт CSS-файла, который улучшает вид формы запроса из каталога.</p> <p>Этот файл может иметь примерно следующий вид. Файл в примере ниже меняет размер шрифта и делает текст полужирным. Он относится к текстовому полю «Развернуть компьютер с помощью учетной записи пользователя Active Directory», которое отображается на рисунке, расположенном выше в разделе «Конструктор настраиваемых форм запросов».</p> <pre>#<field-ID> .grid-item { font-size: 16px; font-weight: bold; width: 600px; }</pre> <p>В этом примере <field-ID> — идентификатор поля на холсте. Чтобы найти значение, выберите поле на холсте. Значение находится на правой панели под именем. На рисунке выше значение имеет вид text_d947bc97.</p> <p>Импорт файла. Сохраните файл в виде <filename>.css.</p>
Экспортировать CSS	Экспорт импортированного CSS-файла.
Удалить CSS	<p>Удаление настраиваемого CSS-файла.</p> <p>Удаленный CSS-файл восстановлению не подлежит.</p>
Загрузить схему формата	<p>Загрузка файла JSON, содержащего структуру и описание элементов управления и состояний, используемых в настраиваемой форме.</p> <p>Эта схема используется, чтобы создать форму или изменить существующую форму. Измененный файл JSON можно импортировать как настраиваемую форму.</p>

Создание настраиваемой формы запроса с параметрами Active Directory

Настраиваемая форма создается, если в форме по умолчанию содержится слишком много или слишком мало информации для пользователя, отправляющего запрос. В такой форме можно добавить или скрыть поля, а также предварительно заполнить поля и показать их или скрыть.

Этот пример использования основан на схеме элементов, которая содержит тип виртуальной машины vSphere, и схеме элементов Все как услуга, которая настраивает учетную запись администратора Active Directory на виртуальной машине. Эта схема элементов Все как услуга основана на процессе создания пользователя с паролем в рабочем процессе группы.

В данном примере использования ваша цель состоит в следующем.

- Дать пользователю возможность настроить пароль администратора.

- Предварительно задать сведения о компьютере, чтобы значения ЦП и памяти были указаны в гигабайтах.

Что вы узнаете из этого примера использования? Этот пример использования включает в себя примеры следующих настроек формы.

- Добавление конкретных полей в пустую форму.
- Настройка флажка «Показать (скрыть)»
- Отображение полей лишь после того, как пользователь, отправляющий запрос, поставит флажок.
- Добавление проверки для полей.
- Отображение значений в поле памяти в гигабайтах, даже если в аналогичном поле в схеме элементов значение рассчитывается в мегабайтах.
- Использование регулярных выражений.

Необходимые условия

- Войдите в службу vRealize Automation как **разработчик архитектуры приложений, программный архитектор** или **архитектор инфраструктуры**.
- Для создания учетной записи пользователя Active Directory с паролем в группе создайте компьютер YourCo Machine и схему элементов пользователя, которая включает в себя схему элементов vSphere и схему элементов Все как услуга. Пример см. в разделе [Создание схемы элементов Все как услуга для создания пользователя](#).

Процедура

1. Выберите **Проектирование > Схемы элементов**.
2. Выделите строку, содержащую компьютер YourCo Machine и схему элементов пользователя, и щелкните **Настраиваемая форма > Изменить**.
3. Переименуйте вкладку «Общие».
 - а) Откройте вкладку.
 - б) Введите в свойство **Заголовок** на панели свойств справа название **Конфигурация**.

- На полученной вкладке «Конфигурация» добавьте и настройте следующие поля с указанными значениями.

The screenshot shows the vRealize Automation form editor interface. The main area is titled 'Edit form: YourCo Machine' and has a tab labeled 'ACTIONS'. Below this, there are three tabs: 'Configuration', 'Machine Details', and 'ADD TAB'. The 'Configuration' tab is active, showing a list of fields to be added to the form. The left sidebar contains 'Blueprint Elements' and 'Generic Elements'. The right sidebar shows the 'Configuration' settings for the selected field.

Configuration

Field ID: general

Title: Configuration

Visibility: [Dropdown]

Configuration Fields:

- Deploy Machine with Active Directory User Account
- Reason for request
- Number of Deployments
- Add Active Directory account
- Username
- Password
- Confirm password
- Email
- I have read and accept the software policy

Generic Elements:

- Text Area
- Text Field
- Text
- Password

Buttons at the bottom: EDIT BLUEPRINT, SAVE, FINISH, CANCEL.

Используйте заданные значения «Внешний вид», «Значения» и «Ограничения».

Все ошибки разрешаются в процессе сборки формы.

Поле на снимке экрана	Источник элемента схемы элементов	Внешний вид	Значения	ограничения
Развертывание компьютера с учетной записью пользователя Active Directory	Универсальные элементы > Текст	Метка и тип ■ Тип отображения = Текст Видимость ■ Источник значения = Константа ■ Отображается = Да	Значение по умолчанию ■ Значение по умолчанию = Развертывание компьютера с учетной записью пользователя Active Directory ■ Источник значения = Константа	
Причина запроса	Элементы схемы элементов > vSphere_vCenter_Machine > Описание	Метка и тип ■ Метка = Причина запроса ■ Тип отображения = Текстовое поле Видимость ■ Источник значения = Константа ■ Отображается = Да Только для чтения ■ Источник значения = Константа ■ Только для чтения = Нет Настраиваемая справка ■ Справка по указателям = Укажите причину запроса.		Обязательно ■ Источник значения = Константа ■ Обязательно = Да

Поле на снимке экрана	Источник элемента схемы элементов	Внешний вид	Значения	ограничения
Количество развертываний	Элементы схемы элементов > Общие > Количество развертываний	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Количество развертываний ■ Тип отображения = Целое число <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Отображается = Да <p>Только для чтения</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Только для чтения = Нет <p>Настраиваемая справка</p> <ul style="list-style-type: none"> ■ Справка по указателям = Выберите количество экземпляров схемы элементов для развертывания. 	<p>Значение по умолчанию</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Значение по умолчанию = 1 	<p>Обязательно</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Обязательно = Да <p>Минимальное значение</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Минимальное значение = 1
Флажок «Добавить учетную запись Active Directory»	Универсальные элементы > Флажок	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Добавить учетную запись Active Directory. ■ Тип отображения = Флажок <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Отображается = Да 		

Поле на снимке экрана	Источник элемента схемы элементов	Внешний вид	Значения	ограничения
Имя пользователя	Элементы схемы элементов > Создать пользователя с паролем в группе > Имя учетной записи пользователя	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Имя пользователя ■ Тип отображения = Текстовое поле <p>Видимость</p> <hr/> <p>Примечание Свойство «Видимость», которое настраивается таким же образом для последующих полей, скрывает поле, если не установлен флажок «Добавить учетную запись Active Directory».</p> <hr/> <ul style="list-style-type: none"> ■ Источник значения = Условное значение ■ Выражение = Заданное значение = Да Если параметр «Добавить учетную запись Active Directory» имеет значение «Да» <p>Настраиваемая справка</p> <ul style="list-style-type: none"> ■ Справка по указателям = Введите имя пользователя администратора. 	<p>Значение по умолчанию</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Значение по умолчанию = администратор 	<p>Обязательно</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Обязательно = Да <p>Регулярное выражение</p> <hr/> <p>Примечание Регулярные выражения должны соответствовать синтаксису JavaScript.</p> <hr/> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Регулярное выражение = "[a-z]*\$" ■ Сообщение об ошибке проверки = Имя пользователя не должно содержать специальных символов или цифр.

Поле на снимке экрана	Источник элемента схемы элементов	Внешний вид	Значения	ограничения
Пароль	Элементы схемы элементов > Создать пользователя с паролем в группе > Пароль, который будет задан для вновь созданной учетной записи	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Пароль ■ Тип отображения = Пароль <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Условное значение ■ Выражение = <p>Заданное значение = Да</p> <p>Если параметр «Добавить учетную запись Active Directory» имеет значение «Да»</p> <p>Настраиваемая справка</p> <ul style="list-style-type: none"> ■ Справка по указателям = Введите пароль для учетной записи администратора. 		<p>Обязательно</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Обязательно = Да <p>Регулярное выражение</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Регулярное выражение = <code>"^(?=.*[A-Z])(?=.*[O-9])(?=.*[a-z]).{8,}\$"</code> ■ Сообщение = Пароль администратора должен содержать не менее восьми символов и может включать в себя буквы, цифры и специальные символы.
Подтверждение пароля	Элементы схемы элементов > Создать пользователя с паролем в группе > Подтверждение пароля	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Подтверждение пароля <p>Тип отображения = Пароль</p> <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Условное значение ■ Выражение = <p>Задать значение «Да»</p> <p>Если параметр «Добавить учетную запись Active Directory» имеет значение «Да»</p> <p>Настраиваемая справка</p> <ul style="list-style-type: none"> ■ Справка по указателям = Повторно введите пароль для учетной записи администратора. 		<p>Обязательно</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Обязательно = Да <p>Поле соответствия</p> <ul style="list-style-type: none"> ■ Поле соответствия = Пароль

Поле на снимке экрана	Источник элемента схемы элементов	Внешний вид	Значения	ограничения
Электронная почта	Универсальные элементы > Текстовое поле	Метка и тип <ul style="list-style-type: none"> ■ Метка = Электронная почта ■ Тип отображения = Текстовое поле Видимость <ul style="list-style-type: none"> ■ Источник значения = Условное значение ■ Выражение = Заданное значение = Да Если параметр «Добавить учетную запись Active Directory» имеет значение «Да» Настраиваемая справка <ul style="list-style-type: none"> ■ Справка по указателям = Введите адрес эл. почты администратора. 	Значение по умолчанию <ul style="list-style-type: none"> ■ Источник значения = Вычисленное значение ■ Оператор = Объединить ■ Добавить значение = Поле Выберите имя пользователя ■ Добавить значение = Константа Введите @yourco.com 	Регулярное выражение <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Регулярное выражение = "^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$" ■ Сообщение об ошибке проверки = Введите допустимый адрес электронной почты.
Флажок «Я прочитал(а) и принимаю политику использования программного обеспечения».	Универсальные элементы > Флажок	Метка и тип <ul style="list-style-type: none"> ■ Метка элемента = Я прочитал(а) и принимаю политику использования программного обеспечения ■ Тип отображения = Флажок Видимость <ul style="list-style-type: none"> ■ Источник значения = Условное значение ■ Выражение = Заданное значение = Да Если параметр «Добавить учетную запись Active Directory» имеет значение «Да» 		

5. Нажмите **Добавить вкладку** и введите **Сведения о компьютере** в свойстве **Заголовок** справа.

6. Настройте следующие поля на вкладке «Сведения о компьютере».

The screenshot shows the 'Edit form' window for 'YourCo' with the 'Machine Details' tab selected. The 'Machine Details' tab contains fields for 'Storage (GB)', 'Number of CPUs', 'Memory (GB)', and 'Memory (MB)'. The 'Visibility' field is set to 'Yes'. The 'Generic Elements' section shows a 'Text Area' element. The 'Blueprint Elements' section shows a tree view with 'General', 'Create_a_user_with_', and 'vSphere_vCenter_' elements.

Используйте заданные значения «Внешний вид», «Значения» и «Ограничения».

Поле на снимке экрана	Источник элементов схемы элементов	Внешний вид	Значения	ограничения
Хранилище (ГБ)	Элементы схемы элементов > vSphere_vCenter_Machine > Хранилище (ГБ)	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Хранилище (ГБ) ■ Тип отображения = Целое число <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Видимость = Да <p>Только для чтения</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Только для чтения = Нет 	<p>Значение по умолчанию = Константа</p> <ul style="list-style-type: none"> ■ Значение по умолчанию = 4 	<p>Минимальное значение</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Минимальное значение = 2
Количество ЦП	Элементы схемы элементов > vSphere_vCenter_Machine > ЦП	<p>Метка и тип</p> <ul style="list-style-type: none"> ■ Метка = Количество ЦП ■ Тип отображения = Целое число <p>Видимость</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Видимость = Да 	<p>Значение по умолчанию = Константа</p> <ul style="list-style-type: none"> ■ Значение по умолчанию = 1 	<p>Минимальное значение</p> <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Минимальное значение = 1

Поле на снимке экрана	Источник элементов схемы элементов	Внешний вид	Значения	ограничения
Память (ГБ)	Универсальные элементы > Целое число	Метка и тип <ul style="list-style-type: none"> ■ Метка = Память (ГБ) ■ Тип отображения = Целое число Видимость <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Видимость = Да 	Значение по умолчанию <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Значение по умолчанию = 1 	Минимальное значение <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Минимальное значение = 1
Память (МБ)	Элементы схемы элементов > vSphere_vCenter_Machine > Память (МБ)	Метка и тип <ul style="list-style-type: none"> ■ Метка = Память (МБ) ■ Тип отображения = Целое число Видимость <ul style="list-style-type: none"> ■ Источник значения = Константа ■ Видимость = Нет 	Значение по умолчанию <ul style="list-style-type: none"> ■ Источник значения = Вычисленное значение ■ Оператор = Умножить ■ Добавить значение = Поле Выберите память (ГБ) ■ Добавить значение = Константа Введите 1024	

- Устраните ошибки. Форму можно сохранить, но нельзя активировать, пока в ней имеются ошибки.
- Чтобы сохранить форму и закрыть конструктор форм, нажмите кнопку **Готово**.
- Выберите схему элементов и нажмите кнопку **Опубликовать**.
- Чтобы сделать настраиваемую форму доступной для пользователей, запрашивающих этот элемент в каталоге служб, на панели инструментов страницы схемы элементов выберите **Настраиваемая форма > Активировать**.

Следующие шаги

- Сделайте схему элементов доступной в каталоге служб. См. раздел [Управление каталогом служб](#).
- В каталоге убедитесь, что форма запроса выглядит как на следующем примере.

Свойства полей в конструкторе настраиваемых форм

Свойства поля определяют вид выбранного поля и значения по умолчанию, которые предлагаются пользователю. Кроме того, они определяют, какие правила должны применяться к полю, чтобы пользователи вводили допустимые значения в форме запроса элементов каталога в vRealize Automation.

Каждое поле настраивается отдельно. Выберите поле и измените его свойства.

Вид поля

Чтобы определить, будет ли это поле отображаться в форме, а также какие метки и настраиваемые справочные ресурсы будут предоставлены пользователям каталога, используются свойства вида.

Некоторые схемы элементов могут включать в себя поля, которые содержат фиксированные значения. При добавлении полей такого типа в настраиваемую форму будут доступны только параметры внешнего вида, а само поле всегда будет доступно только для чтения.

Таблица 3-66. Параметры вкладки «Вид»

Параметр	Описание
Метка и тип	<p>Введите метку и выберите способ отображения.</p> <p>Доступные способы отображения зависят от поля. Некоторые поля поддерживают множество типов текста, некоторые — только несколько типов, а некоторые поддерживают только один тип. Возможные значения для всех типов:</p> <ul style="list-style-type: none"> ■ Комбинированный список ■ Десятичное ■ Раскрывающееся меню ■ Двойной список ■ Образ ■ Integer ■ Ссылка ■ Множественный выбор ■ Средство выбора нескольких значений ■ Пароль ■ Группа переключ. ■ Text ■ Текстовая область ■ Текстовые поля <p>Типы полей со множественным выбором и двойным списком обеспечивают одну и ту же функцию, но в двойном списке применяется более интуитивно понятный вариант, когда пользователь может выбрать более одного элемента в списке.</p> <p>Поля раскрывающегося меню и сетки данных включают параметр Заполнитель. Введенное значение отображается как внутренняя метка или инструкции в раскрывающемся меню или как общая метка или инструкции в сетке данных.</p> <p>Поля выбора значений и выбора в дереве включают параметр Тип ссылки. Тип ссылки — это тип ресурса vRealize Orchestrator, который используется для ограничения списка значений или дерева иерархией сервера vRealize Orchestrator, которая поддерживает данный тип. Можно дополнительно ограничить поиск, выбрав действие, которое поддерживает данный тип ссылки. Дополнительные сведения об этих средствах выбора см. в разделе Использование средства выбора значений или древовидного средства выбора в конструкторе настраиваемых форм.</p>
Видимость	<p>Показать или скрыть поля в форме запроса.</p> <ul style="list-style-type: none"> ■ Константа. Выберите «Да», чтобы отобразить поле в форме. Выберите «Нет», чтобы скрыть поле. ■ Условное значение. Видимость определяется первым истинным выражением. Например, поле отображается, если установлен флажок в форме. ■ Внешний источник. Видимость определяется результатами выбранного действия vRealize Orchestrator.

Таблица 3-66. Параметры вкладки «Вид» (продолжение)

Параметр	Описание
Только для чтения	<p>Запрет на изменение значений полей пользователями.</p> <ul style="list-style-type: none"> ■ Константа. Выберите «Да», чтобы значение отображалось, но изменения были бы запрещены. Выберите «Нет», чтобы разрешить изменения. ■ Условное значение. Статус определяется первым истинным выражением. Например, поле доступно только для чтения, если значение в поле хранилища превышает 2 ГБ. ■ Внешний источник. Статус определяется результатами выбранного действия vRealize Orchestrator.
Строк на странице	<p>Только для элементов сетки данных.</p> <p>Введите число строк.</p>
Настраиваемая справка	<p>Введите информацию о поле для пользователей. Эта информация будет отображаться в справке по указателям для данного поля.</p> <p>Можно использовать простой текст или HTML, включая ссылки href. Например, <code>vRealize Automation documentation</code>.</p>

Значения полей

Для предоставления любых значений по умолчанию используются свойства значений.

Таблица 3-67. Параметры вкладки «Значения»

Параметр	Описание
Столбцы	<p>Только для элемента сетки данных.</p> <p>Введите метку, идентификатор и тип значения для каждого столбца в таблице.</p> <p>Значение по умолчанию для сетки данных должно содержать данные заголовка, которые соответствуют определяемым столбцам. Например, если есть идентификатор <code>user_name</code> для одного столбца и идентификатор <code>user_role</code> для другого столбца, первая строка будет иметь следующий вид: <code>user_name,user_role</code>.</p> <p>Примеры конфигурации см. в разделе Использование элемента сетки данных в конструкторе пользовательских форм.</p>
Значение по умолчанию	<p>Поле заполняется значением по умолчанию на основе источника значения.</p> <p>Для многих свойств можно выбирать разные источники значений. Некоторые источники недоступны для некоторых типов полей и свойств. Доступные источники значений зависят от поля.</p> <ul style="list-style-type: none"> ■ Константа. Введенная строка. Это значение не изменяется. В зависимости от свойства значение может быть строкой, целым числом, регулярным выражением или вариантом из ограниченного списка, например «Да» или «Нет». <p>Например, можно указать «1» как целое значение по умолчанию, выбрать «Нет» как значение свойства «Только для чтения» или предоставить регулярное выражение для проверки значения, указанного в поле.</p> <ul style="list-style-type: none"> ■ Условное значение. Такое значение зависит от одного или нескольких условий. Условия обрабатываются в указанном порядке. Если более чем одно условие истинно, последнее истинное условие определяет особенности поля, к которому относится это свойство. Например, можно создать условие, которое определяет, видимо ли поле в зависимости от значения другого поля. <p>Например, значение по умолчанию поля хранилища составляет 1 ГБ, если в поле памяти указано менее 512 МБ. Оператор <code>contains</code> проверяет, что выбранное поле содержит заданное значение. Оператор <code>within</code> проверяет, что выбранные поля содержат заданную строку. Например, для выражения Field A within development, то это выражение будет истинным, когда <code>Field A = "dev", "lop"</code> или <code>"ment"</code>, но оно будет ложным, когда <code>Field A = "prod"</code> или <code>"test"</code>.</p> <ul style="list-style-type: none"> ■ Внешний источник. Это значение основано на результатах действия vRealize Orchestrator. Например, расчет затрат на основании действия в сценарии vRealize Orchestrator. <p>Пример см. в разделе Использование действий vRealize Orchestrator в конструкторе настраиваемых форм.</p>

Таблица 3-67. Параметры вкладки «Значения» (продолжение)

Параметр	Описание
	<ul style="list-style-type: none"> ■ Поле привязки. Это значение соответствует выбранному полю, к которому оно привязано. Доступные поля могут быть только одного и того же типа. Например, необходимо привязать значение по умолчанию поля с флажком «Требуется проверка подлинности» к другому полю с флажком. Если в форме запроса устанавливается флажок в поле, к которому привязано значение, в текущем поле привязки также устанавливается флажок. ■ Вычисленное значение. Значение основано на результатах указанных значений полей и выбранного оператора. В текстовых полях используется оператор «Объединить». В полях с целым значением используются выбранные операции сложения, вычитания, умножения или деления. Например, в поле с целым значением можно настроить перевод мегабайтов в гигабайты с помощью операции умножения. По умолчанию объем памяти в мегабайтах соответствует объему памяти в гигабайтах, умноженному на 1024.
Вариант значения	<p>Используется в раскрывающемся меню, группе переключателей, в списках выбора значений и полях множественного выбора.</p> <ul style="list-style-type: none"> ■ Константа. Формат списка: значение метка, значение метка, значение метка. Например, 2 Small, 4 Medium, 8 Large. ■ Внешний источник. Значение основано на результатах выбранного действия vRealize Orchestrator.
Шаг	<p>Для полей с целыми или десятичными значениям укажите шаг увеличения или уменьшения значения.</p> <p>Например, если указано значение по умолчанию «1» и задано значение шага «3», то допустимыми значениями являются 4, 7, 10 и т. д.</p>

Ограничения поля

Используйте ограничивающие свойства, чтобы пользователь, оформляющий запрос, вводил в форму допустимые значения.

Можно также использовать внешние средства проверки как альтернативный метод обеспечения допустимости значений. См. раздел [Использование внешней проверки в конструкторе настраиваемых форм](#).

Таблица 3-68. Параметры вкладки «Ограничения»

Параметр	Описание
Обязательно	<p>Пользователь, оформляющий запрос, должен указать значение в этом поле.</p> <ul style="list-style-type: none"> ■ Константа. Выберите «Да», чтобы указание значения было обязательным. Выберите «Нет», если это поле является необязательным. ■ Условное значение. Обязательность или необязательность заполнения поля определяется первым истинным выражением. Например, поле является обязательным, если название семейства операционных систем семейства в другом поле начинается со слова Darwin. ■ Внешний источник. Статус определяется результатами выбранного действия vRealize Orchestrator.
Регулярное выражение	<p>Введите регулярное выражение, которое проверяет значение, и текст сообщения, который отображается, если проверка не пройдена.</p> <p>Регулярные выражения должны соответствовать синтаксису JavaScript. Общий обзор см. в разделе Создание регулярных выражений. Более подробные инструкции см. в разделе Синтаксис.</p> <ul style="list-style-type: none"> ■ Константа. Введите регулярное выражение. Например, в случае адреса электронной почты регулярное выражение может иметь вид <code>^[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Za-z]{2,}\$</code>, а сообщение об ошибке проверки выглядит так: Недопустимый формат адреса электронной почты. Повторите попытку. ■ Условное значение. Используемое регулярное выражение определяется первым истинным выражением.
Минимальное значение	<p>Укажите минимальное числовое значение. Например, пароль должен содержать не менее 8 символов.</p> <p>Введите сообщение об ошибке. Например, Пароль должен содержать не менее 8 символов.</p> <ul style="list-style-type: none"> ■ Константа. Введите целое число. ■ Условное значение. Минимальное значение определяется первым истинным выражением. Например, минимальное количество ЦП составляет 4, если в качестве операционной системы выбрана не Linux. ■ Внешний источник. Значение основано на результатах выбранного действия vRealize Orchestrator.

Таблица 3-68. Параметры вкладки «Ограничения» (продолжение)

Параметр	Описание
Максимальное значение	<p>Максимальное числовое значение. Например, размер поля составляет не более 50 символов.</p> <p>Введите сообщение об ошибке. Например, Это описание не должно превышать 50 символов.</p> <ul style="list-style-type: none"> ■ Константа. Введите целое число. ■ Условное значение. Максимальное значение определяется первым истинным выражением. Например, максимальный объем хранилища — 2 ГБ, если в поле расположения развертывания указано АМЕА. ■ Внешний источник. Значение основано на результатах выбранного действия vRealize Orchestrator.
Поле соответствия	<p>Значение этого поля должно соответствовать значению выбранного поля.</p> <p>Например, значение поля подтверждения пароля должно соответствовать значению поля «Пароль».</p>

Использование действий vRealize Orchestrator в конструкторе настраиваемых форм

При настройке формы запроса для схемы элементов vRealize Automation можно задать поведение для некоторых полей в результатах действия vRealize Orchestrator.

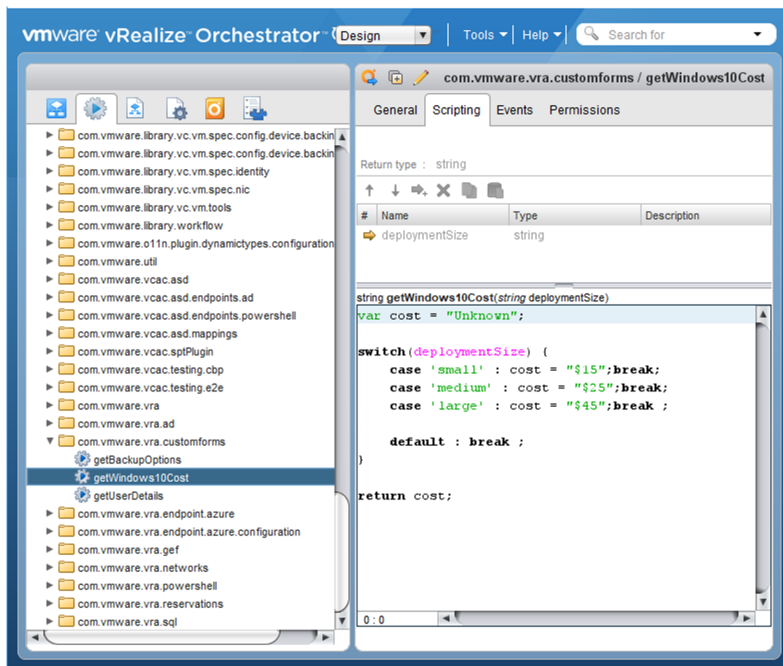
Существует несколько способов использования действий vRealize Orchestrator. Возможно, есть действие, которое получает данные из стороннего источника, или можно использовать сценарий, который определяет размер и затраты. В этом примере используется сценарий.

Если создается сценарий для заполнения полей с помощью действия, не следует использовать тип Array [Any].

Пример. Пример полей затрат и размера

В этом примере пользователь каталога должен выбрать размер виртуальной машины, а затем отобразить ежедневные затраты на эту машину. Для этого примера существует vRealize Orchestrator, который сопоставляет размер и затраты. Необходимо добавить поля затрат и размера в настраиваемую форму схемы элементов. Поле размера определяет значение, которое отображается в поле затрат.

1. В vRealize Orchestrator настройте действие `getWindows10Cost` с помощью сценария `deploymentSize`, как показано в следующем примере.



Используйте следующий пример сценария.

```
var cost = "Unknown";

switch(deploymentSize) {
  case 'small' : cost = "$15";break;
  case 'medium' : cost = "$25";break;
  case 'large' : cost = "$45";break ;

  default : break ;
}

return cost;
```

- В vRealize Automation добавьте и настройте поля размера и затрат в настраиваемой форме схемы элементов.

Настройте поле размера с выбором нескольких значений: небольшой, средний и большой.

The screenshot shows the configuration interface for a field named 'Size'. The 'Values' tab is selected. The 'Default value' is set to 'large'. The 'Value source' is set to 'Constant'. The 'Value options' are set to 'Constant'. The 'Value options' list contains the following values: 'small|Small, meduim|Meduim, large|Large'.

В vRealize Automation добавьте и настройте поля размера и затрат в настраиваемой форме схемы элементов.

На вкладке «Значения» настройте следующие значения свойств.

- Значение по умолчанию = **Большой**
- Параметры значений
 - Источник значения = **Константа**
 - Определение значения = **небольшой | Небольшой ,средний | Средний ,большой | Большой**

3. Настройте отображение в поле затрат, как определено в действии vRealize Orchestrator в зависимости от выбранного значения в поле размера.

Cost ☺
Field ID: cost

Appearance **Values** Constraints

▼ Default value External source

Value source	External source ▼
Select action	com.vmware.vra.customforms/getWindows10Cost
Action inputs	
deploymentSize	Field ▼ Size ▼

На вкладке «Значения» настройте следующие значения свойств.

- Значение по умолчанию = Внешний источник
- Выбор действия = <папка действий vRealize Orchestrator>/getWindows10Cost
- Входные значения действий
 - deploymentSize. Это значение настроено в действии.
 - Поле
 - Размер

Использование средства выбора значений или древовидного средства выбора в конструкторе настраиваемых форм

При настройке формы запроса можно предоставить элементы, в которых пользователь может выбрать из списка результатов поиска или просмотреть дерево, чтобы найти подходящее значение.

Список выбора значений и выбор в дереве используют тип ссылки, который определяется на вкладке "Вид" данной настраиваемой формы. Тип ссылки представляет собой ресурс vRealize Orchestrator. Например, это может быть AD:UserGroup или VC:Datastore. После определения типа ссылки, пользователь может ввести строку поиска, и результаты поиска или параметры дерева будут ограничены этой строкой или ресурсами, у которых есть соответствующий параметр.

В средстве выбора значения затем можно дополнительно ограничить набор возможных значений, настроив нужный внешний источник. В древовидном средстве выбора можно задать значение по умолчанию, настроив соответствующий внешний источник.

Работа со средством выбора значений

Средство выбора значений отображается в форме каталога как средство поиска. Пользователь вводит строку, и средство выбора предоставляет соответствующие варианты в зависимости от своих настроек. Средство выбора можно использовать в следующих ситуациях. Самое эффективное использование средства выбора значений — это его связывание с внешним источником значений.

- Средство выбора значений с источником постоянных значений. Используйте этот метод, если нужно, чтобы пользователь мог выбирать из списка предварительно определенных статических значений. Аналогично полю со списком, раскрывающемуся списку, множественному выбору и группе переключателей, этот метод предоставляет список результатов поиска на основе определенных постоянных значений и надписей.
- Средство выбора значений без источника значений. Используйте этот метод, если нужно, чтобы пользователь выполнял поиск в иерархии vRealize Orchestrator для конкретного объекта с настроенным типом ссылки. Например, таким типом ссылки может быть VC:Datastore, и нужно, чтобы пользователи могли выбирать хранилище данных из полученного списка.
- Средство выбора значений с внешним источником значений. Используйте этот метод, если нужно, чтобы пользователь выбирал из результатов, основанных на действии vRealize Orchestrator. Для средства выбора значений из внешнего источника это действие должно возвращать массив свойств, а не массив строк. Например, может быть определено действие, которое получает два или более значений из встроенной базы данных, и нужно, чтобы пользователи выбирали значение из полученного списка. Действие должно включать в себя фильтр `var filter = System.getContext().getParameter("__filter");` и возвращать массив свойств, а не массив строк. Если нужен массив строк, используйте поле типа «комбинированный список».

Использование древовидного средства выбора

Древовидное средство выбора отображается в виде каталога как вариант поиска. Пользователь вводит строку, и появляется данное средство выбора. Это дерево позволяет пользователям выбирать значения, которые соответствуют определенному типу ссылки. Например, если тип ссылки — VC:Datastore, то пользователь сможет выбрать объекты хранилищ данных. Если тип ссылки — VC:VirtualMachine, то пользователь сможет выбрать виртуальные машины.

- Древовидное средство выбора без источника значений. Используйте этот метод, если нужно, чтобы пользователь мог просматривать иерархическое дерево для конкретного объекта с настроенным типом ссылки. Например, если выбран тип ссылки VC:Datastore и нужно, чтобы пользователи могли выбирать хранилище данных из полученного дерева.
- Древовидное средство выбора с внешним источником значений. Используйте этот метод, если нужно предоставить в дереве значение по умолчанию. Пользователь сможет выбрать заранее установленное значение или просмотреть список других значений. Например, для типа ссылки VC:Datastore может потребоваться задать в этом дереве определенное хранилище данных на основании указанных для данного действия входных значений, которые определяют конкретную сеть.

Использование элемента сетки данных в конструкторе пользовательских форм

При настройке формы запроса для схемы элементов на эту форму можно добавить необходимые данные в формате таблицы. Пользователь, инициирующий запрос, может заполнить строки таблицы данными из запроса на подготовку.

После добавления таблицы ее можно заполнить данными вручную или с помощью внешнего источника. Некоторые элементы схемы элементов отображаются в виде сетки данных. К таким элементам относятся, например, диски виртуальных машин или сетевые адаптеры.

Кроме добавления полей в сетку данных можно также устанавливать ограничения на ввод данных, чтобы пользователь вводил только допустимые значения.

В следующих примерах используется сетка данных, при этом средство выбора нескольких значений можно использовать в качестве альтернативного способа ввода данных пользователями на форме запроса.

Различия можно увидеть, изменив свойство поля **Внешний вид > Метка и тип > Способ отображения**.

Пример. Пример предоставления данных из CSV-файла

В этом примере имеется таблица значений, которые предоставляются в настраиваемой форме запроса.

Информация в таблице предоставляется как постоянный источник значений. Источник основан на структуре данных CSV-файла, где первой строкой указывается заголовок. Заголовки являются идентификаторами столбцов с разделителем-запятой. Каждая дополнительная строка представляет собой данные, которые появляются в каждой строке таблицы.

1. Добавьте универсальный элемент сетки данных на холст проекта.
2. Выберите сетку данных и задайте значения в области свойств.

Data Grid ?

Field ID: datagrid_ecdf4fe3

Appearance
Values
Constraints

Columns

ADD COLUMN

Label
Username

Id
username

Type
String

Label
Employee ID

Id
employeeid

Type
Integer

Label
Manager

Id
manager

Type
String

Default value
Constant

Value
Constant

source
CSV

```
username,employeeid,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

Метка	Идентификатор	Тип
Имя пользователя	имя пользователя	String
Идентификатор сотрудника	employeeid	Integer
Руководитель	руководитель	String

Укажите значения CSV-файла.

```
username,employeeId,manager
leonardo,95621,Farah
vindhya,15496,Farah
martina,52648,Nikolai
```

- Убедитесь, что на сетке данных в форме запроса схемы элементов отображаются нужные данные.

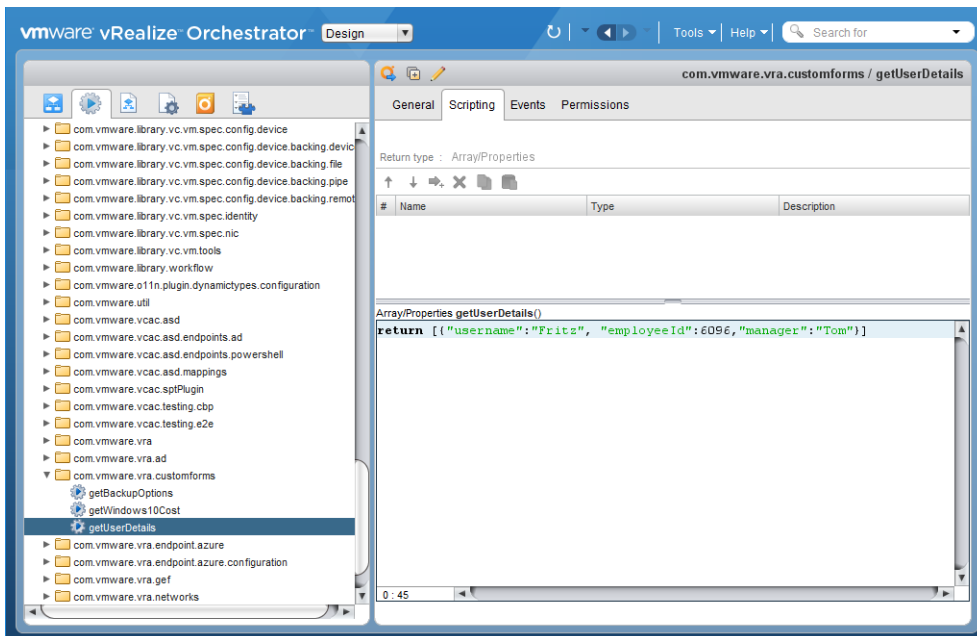
<input type="checkbox"/>	Username	Employee ID	Manager
<input type="checkbox"/>	leonardo	95621	Farah
<input type="checkbox"/>	vindhya	15496	Farah
<input type="checkbox"/>	martina	52648	Nikolai

Пример. Пример внешнего источника

В этом примере используется предыдущий пример, но значения основаны на действии vRealize Orchestrator. Несмотря на то, что это пример простого действия, можно использовать более сложное действие, с помощью которого эта информация извлекается из локальной базы данных или системы.

Действие, используемое для проверки, в качестве входного параметра должно использовать массив или свойства.

- В vRealize Orchestrator настройте действие getUserDetails с помощью массива, как показано в следующем примере.



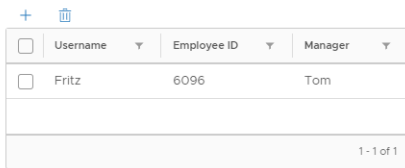
Используйте следующий пример сценария.

```
return [{"username": "Fritz", "employeeId": 6096, "manager": "Tom"}]
```

- В vRealize Automation добавьте сетку данных и задайте в ее столбцах следующие значения.

Метка	Идентификатор	Type
Имя пользователя	имя пользователя	String
Идентификатор сотрудника	employeeid	Integer
Руководитель	руководитель	String

- В списке «Источник значений» выберите **Внешний источник**.
- В разделе «Выбор действия» введите getUserDetails и выберите действие, созданное в vRealize Orchestrator.
- Сохраните и проверьте таблицу в форме запроса.



<input type="checkbox"/>	Username ▾	Employee ID ▾	Manager ▾
<input type="checkbox"/>	Fritz	6096	Tom
1 - 1 of 1			

Пример. Пример элемента из схемы элементов

Некоторые элементы схемы элементов можно добавить в форму, где они будут отображаться в виде сетки данных, когда пользователь запрашивает схему элементов. В виде сетки данных отображаются, например, диски и сетевые адаптеры.

В этом примере на форму добавляется элемент «Диски», чтобы пользователи могли добавлять дополнительные диски при запросе элементов каталога. Для лучшего контроля над тем, что именно пользователь может запрашивать, можно добавить необходимые ограничения. Например, можно ограничить емкость запоминающего устройства до 5 ГБ.

Значения элементов, определенные в схеме элементов (например диски), не отображаются в настраиваемой форме. Это не позволяет пользователю изменять конфигурацию, необходимую для успешной подготовки запроса.

- Создайте схему элементов с компьютером, емкость диска которого равна 6 ГБ.
- Добавьте на холст элемент «Диск».
- Выберите сетку данных и задайте ограничения на панели свойств.

В этом примере минимальная емкость диска равна 2, а максимальная — 5.

Disks ?

Field ID: vSphere__vCenter__Machine_1-disks

Appearance

Values

Constraints

> Drive letter / Mount path

> Volume ID

> ID

> Label

> custom_properties

> User Created

> Storage Reservation policy

> Capacity

> Required

No

▼

> Regular expression

Regular expression

> Minimum value

2

> Maximum value

5

- Сохраните и проверьте ограничения для таблицы на форме запроса.
- Щелкните значок плюса в сетке данных на форме запроса.

Обратите внимание, что активируется ограничение емкости, если ввести значение больше 5.

☐ Is Clone

Drive letter / Mount path _____

Volume ID _____



ID _____

Label _____

custom_properties _____

☐ User Created

Storage Reservation policy _____

Capacity 6  

Использование внешней проверки в конструкторе настраиваемых форм

Можно настроить форму запроса, чтобы обеспечить указание пользователями допустимых значений при запросе. Для этого необходимо добавить ограничения для полей или использовать внешний источник проверки.

Для некоторых свойств полей, таких как регулярные выражения, минимальные и максимальные значения, соответствие полей или непустое значение, можно настроить ограничения, чтобы обеспечить ввод допустимых значений. См. раздел [Свойства полей в конструкторе настраиваемых форм](#).

Внешняя проверка контролирует допустимые значения из внешнего источника с помощью действий vRealize Orchestrator.

Если проверяется значение из сетки данных, то действие, используемое для проверки, в качестве входного параметра должно использовать массив или свойства.

Ниже приведены некоторые примеры использования внешней проверки.

- Допустимые значения определяются во внешнем источнике. Например, vRealize Orchestrator.
- Проверка затрагивает несколько полей. Например, действие vRealize Orchestrator позволяет собирать данные о размере диска и емкости пула носителей и проверяет указанные значения размера на основе свободного места.

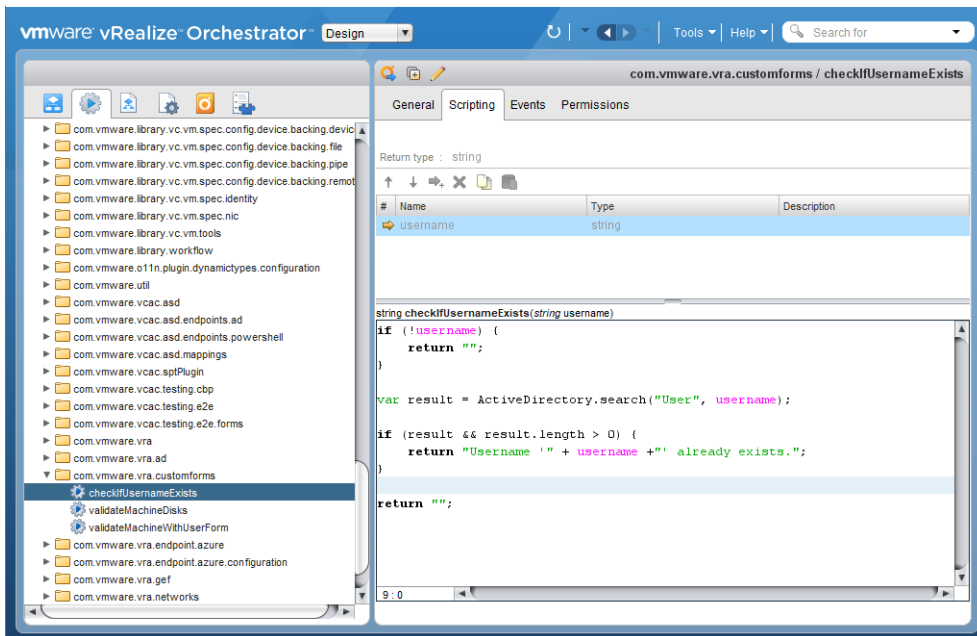
Как установить порядок проведения нескольких внешних проверок в одной схеме элементов? Проверки обрабатываются в порядке, в котором они появляются на холсте внешних проверок. При наличии двух проверок, обрабатывающих одно поле, результаты первой проверки будут перезаписаны результатами второй проверки. Чтобы изменить порядок проверок, можно щелкнуть и перетащить карточки на холсте.

Пример. Пример пользователя vRealize Orchestrator

В этом примере пользователь каталога должен предоставить только новое имя пользователя. Для этого предназначено действие vRealize Orchestrator, которое проверяет, существует ли указанное в форме имя пользователя в базе данных Active Directory. Если имя не существует, появляется сообщение об ошибке в форме запроса.

Этот случай использования применяется в примере [Создание настраиваемой формы запроса с параметрами Active Directory](#).

1. В vRealize Orchestrator настройте действие `checkIfUsernameExists` с помощью сценария, как показано в следующем примере.



Используйте следующий пример сценария. В этом примере `return` — это сообщение, которое отображается, если проверка не пройдена.

```

if (!username) {
    return "";
}

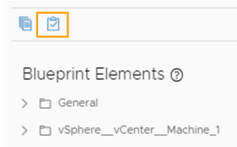
var result = ActiveDirectory.search("User", username);

if (result && result.length > 0) {
    return "Username '" + username + "' already exists.";
}

return "";

```

- В vRealize Automation откройте конструктор настраиваемых форм для схемы элементов, щелкните **Внешняя проверка** и перетащите тип **Проверка Orchestrator** на холст.



- Настройте параметры внешней проверки.

- Метка проверки = проверка наличия имени пользователя
- Выбор действия = <папка действий vRealize Orchestrator>/checkIfUsernameExists
- Входные значения действий
 - имя пользователя = поле и имя пользователя
- Выделенные поля
 - Щелкните **Добавить поле** и выберите имя пользователя.

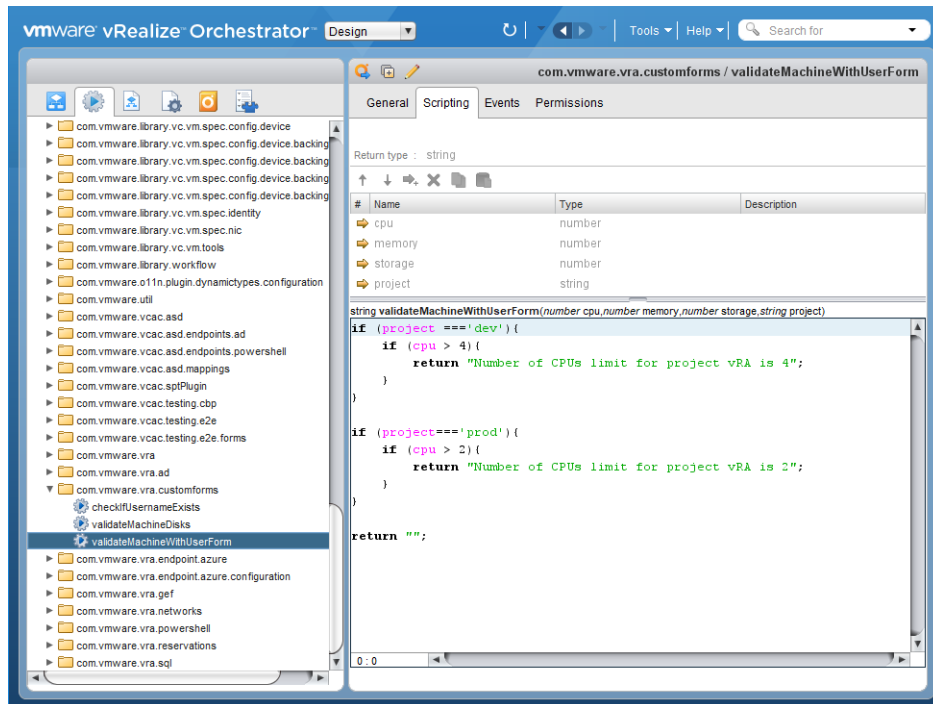
Если введенное значение не проходит проверку, в форме запроса каталога отображается ошибка проверки на уровне полей. Если требуется глобальная ошибка, не настраивайте выделенное поле.

Пример. Пример использования нескольких полей vRealize Orchestrator

В этом случае необходимо, проверка значений ЦП, памяти и хранилища основывалась на проектном значении. Например, если пользователи выбирают проект Dev, максимальное количество ЦП равно 4. Если они выбирают Prod, максимальное значение будет равно 2.

В этом случае добавьте поле проекта в пример [Создание настраиваемой формы запроса с параметрами Active Directory](#). Настройте проект в качестве раскрывающегося списка с элементами Dev и Prod.

- В vRealize Orchestrator настройте действие validateMachineWithUserForm с помощью сценария, как показано в следующем примере.



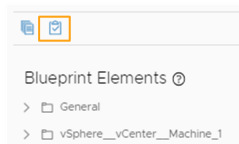
Используйте следующий пример сценария для проверки ЦП. При необходимости добавьте значения памяти и хранилища для сценария. В данном примере return — это сообщение, которое отображается, если проверка не пройдена.

```
if (project === 'dev'){
    if (cpu > 4){
        return "Number of CPUs limit for project vRA is 4";
    }
}

if (project === 'prod'){
    if (cpu > 2){
        return "Number of CPUs limit for project vRA is 2";
    }
}

return "";
```

2. В vRealize Automation откройте конструктор настраиваемых форм для схемы элементов, щелкните **Внешняя проверка** и перетащите тип **Проверка Orchestrator** на холст.



3. Настройте параметры внешней проверки.

- Метка проверки = проверка сведений о компьютере
- Выбор действия = <папка действий vRealize Orchestrator>/validateMachineWithUserForm
- Входные значения действий
 - ЦП = поле и количество ЦП
 - память = поле и объем памяти (ГБ)
 - хранилище = поле и размер хранилища (ГБ)
 - Проект = поле и проект
- Выделенные поля
 - Щелкните **Добавить поле** и выберите **Проект**.

В каталоге пользователь может увидеть ошибку проверки, которая показана в следующем примере.

Тестирование и устранение неполадок неудачных запросов на подготовку

Архитектор схемы элементов или администратор хотят убедиться, что они предоставляют пользователям работающие схемы элементов.

Сбой запросов каталога может происходить по нескольким причинам. Это может произойти из-за сетевого трафика, недостаточных ресурсов конечной точки или ошибок в спецификации схемы элементов. Кроме того, запрос на подготовку может быть выполнен успешно, но развертывание не работает правильно. Разработчик схемы элементов должен не допускать предоставления пользователям схем элементов, которые нельзя будет успешно развернуть.

Можно организовать тестовую службу и соответствующие права, чтобы развертывать схему элементов из каталога. См. раздел [Контрольный список для настройки каталога служб](#).

Если ресурсы не будут подготовлены успешно, для устранения неполадок неудачного развертывания можно использовать vRealize Automation.

Возможные состояния ошибки

В случае ошибки запроса на подготовку выдается сообщение об одном из следующих состояний.

- **Не выполнено.** Ошибка запроса может произойти по нескольким причинам. Одна причина заключается в том, что процесс подготовки мог не сработать из-за нехватки ресурсов на целевой конечной точке, недостаточного количества ресурсов для выполнения требований схемы элементов или неправильно составленной схемы элементов, которую нужно исправить. Другая причина заключается в том, что запросу требовалось подтверждение от кого-либо в вашей организации, и утверждающий отклонил этот запрос. Также может быть, что не удалось выполнить действие, запущенное пользователем для данного развертывания. Такая ошибка может быть вызвана уже упомянутыми причинами среды развертывания или утверждения запроса.

Чтобы установить причину проблемы, используйте следующий рабочий процесс устранения неполадок. Если можно устранить возникшую проблему, воспользуйтесь действиями **Отменить** и **Отправить повторно**. См. раздел [Пункты меню «Действие» для подготовленных ресурсов](#).

- **Частично успешно.** Запрос может быть выполнен частично, то есть некоторые компоненты были развернуты, но не все действия подготовки были выполнены успешно.

Чтобы определить, какие компоненты были развернуты только частично, и установить причину проблемы, используйте следующий рабочий процесс устранения неполадок. Если можно устранить возникшую проблему, воспользуйтесь действиями **Отменить** и, возможно, **Отправить повторно**. См. [Пункты меню «Действие» для подготовленных ресурсов](#) и [Как работает действие «Возобновить»](#).

Рабочий процесс устранения неполадок

Этот рабочий процесс можно использовать как первый этап анализа неудачного развертывания. Если ваш анализ обнаруживает, что ошибка была связана с временной проблемой среды развертывания, можно устранить эту проблему и повторно отправить запрос. Если проблема связана со спецификацией запроса, можно скорректировать используемую схему элементов и отправить новый запрос.

Таблица 3-69. Как начать устранение неполадок


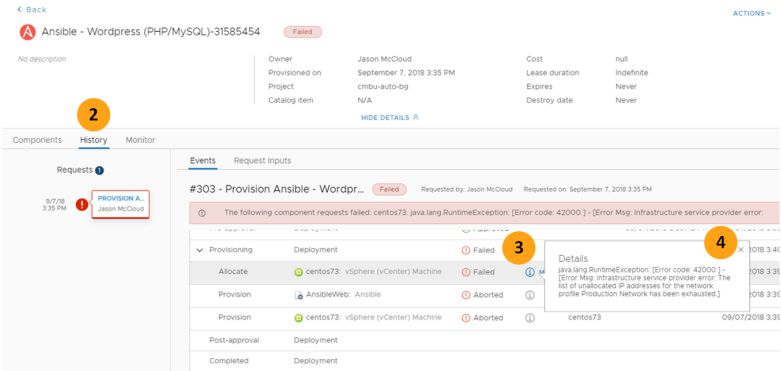
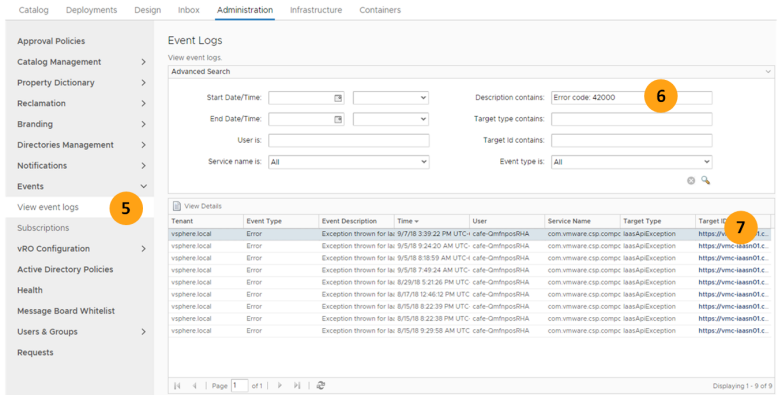
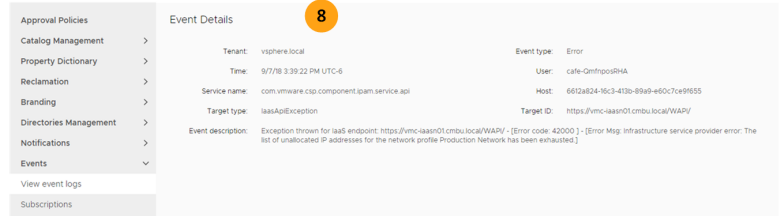
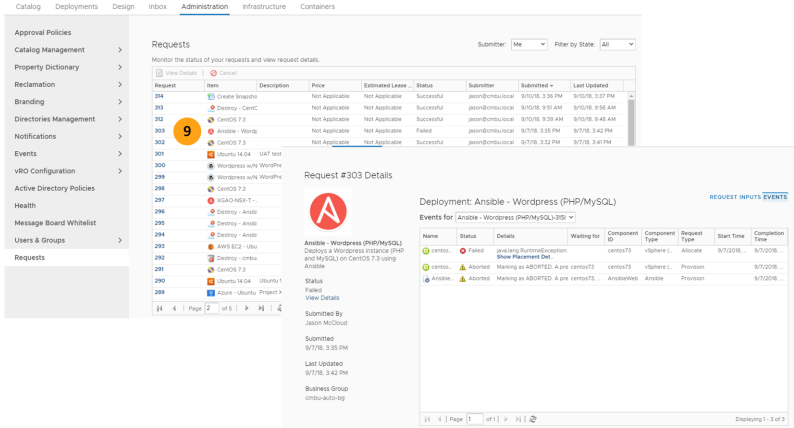
Рабочий процесс	Этап устранения неполадок	Пример
1	На вкладке Развертывания неудачные развертывания указываются в строке состояния. Данная карточка включает в себя последнее сообщение об ошибке. Для получения дополнительной информации нажмите имя развертывания или индикатор хода выполнения.	
2	На вкладке Журнал сведений о развертывании можно использовать рабочий процесс событий, чтобы определить, где в процессе подготовки произошла ошибка. Этот рабочий процесс также полезен, если выполнялось действие для развертывания, но произошла ошибка.	
3	Состояние ошибки указывает, где произошел сбой рабочего процесса.	
4	Данная информация предоставляет собой более подробное сообщение об ошибке. Если этих сведений в табличке с информацией недостаточно для определения причин проблемы и их устранения, можно дополнительно проанализировать журналы событий.	

Таблица 3-69. Как начать устранение неполадок (продолжение)

Рабочий процесс	Этап устранения неполадок	Пример
5	Для следующих шагов требуется роль администратора. Чтобы найти ошибку в контексте других ошибок и предупреждений, выберите Администрирование > События > Просмотр журналов событий .	
6	Для обнаружения ошибок можно использовать расширенный поиск на основании данных сообщения в сведениях о развертывании.	
7	Чтобы просмотреть сведения о событии, нажмите ссылку идентификатора в целевой системе.	
8	Сведения о событии содержат дополнительные данные о подготовке, которые могут помочь в устранении неполадок.	
9	Администратор может также просмотреть запрос в контексте запросов других пользователей. Выберите Администрирование > Запросы и нажмите номер запроса, чтобы просмотреть входные данные и события этого запроса.	

Как работает действие «Возобновить»

Действие возобновления можно применить в случае сбоя развертывания для перезапуска процесса подготовки с точки отказа и при определенных обстоятельствах. Если функция возобновления включена, она доступна для запросов на подготовку, завершившихся сбоем, и других применимых действий.

Чтобы выполнять возобновление запросов на подготовку, добавьте настраиваемое свойство `_debug_deployment = true` в схему элементов. По умолчанию для развертываний со сбоем выполняется откат и очистка для освобождения ресурсов. Свойство `_debug_deployment = true` сохраняет развертывание в точке отказа и позволяет использовать действие возобновления там, где оно поддерживается, и с учетом принципа его работы. Если возобновление используется только для поддерживаемых действий, `_debug_deployment` включать не нужно.

Дополнительные сведения о свойстве `_debug_deployment` см. в разделе *Справочник по настраиваемым свойствам*.

Чтобы выполнять возобновление запросов на подготовку или доступных действий, необходимо предоставить пользователям право на возобновление. См. раздел [Предоставление пользователям права на использование службы, элементов каталога и действий](#).

Пользователям можно предоставить право на действие возобновления для следующих операций подготовки.

- Запросы на подготовку
- Действие «Возобновить»
- Действие «Уменьшить масштаб»
- Действие «Увеличить масштаб»
- Действие «Удалить»

Ограничения действия возобновления

Выбирая, можно ли использовать возобновление, а не запрашивать новый экземпляр схемы элементов, необходимо учитывать некоторые ограничения.

- Начиная с момента запроса, схему элементов изменить нельзя.

В момент запроса неизменяемая версия схемы элементов привязывается к запросу в каталог. Это статическая версия содержит все спецификации, включая атрибуты, настраиваемые свойства, настройки и т. д., которые были выбраны в начале подготовки. Если в схеме элементов имеется ошибка, приводящая к сбою, исправление этой ошибки с последующим возобновлением не может быть выполнено, поскольку ошибка относится к версии, связанной с запросом. В этом случае необходимо подготовить новый экземпляр.

Примеры

- Схема элементов А запрашивает ОЗУ 5 ГБ, но запрос завершается ошибкой, так как зарезервировано только 3 ГБ. Если уменьшить требуемую память в схеме элементов до 3 ГБ, а

затем выполнить действие «Возобновить», то оно завершится сбоем. В ходе выполнения процесс возобновления проверяет исходный запрос и по-прежнему ищет 5 ГБ. Тем не менее, если увеличить системное резервирование для бизнес-группы до 5 ГБ и запустить возобновление, оно будет выполнено.

- При запросе схемы элементов В, которая включает в себя настраиваемую спецификацию гостевой системы, происходит сбой. Анализ показывает, что настраиваемая спецификация была переименована на экземпляре vCenter Server. Если указать новое имя схемы элементов и запустить действие «Возобновить», произойдет сбой. Схема элементов была обновлена, но для действия возобновления используется исходная версия. Если в дальнейшем вы планируете использовать новое имя, разверните новый экземпляр схемы элементов, а не используйте возобновление. В противном случае необходимо вернуть старое имя настраиваемой спецификации гостевой системы, соответствующее исходной версии, на экземпляре vCenter Server и выполнить возобновление. Для предотвращения сбоя очередного запроса на подготовку обязательно обновите схему элементов, указав правильную настраиваемую спецификацию гостевой системы.

Действие «Возобновить» выполняется, если обновить целевую среду развертывания в соответствии со спецификациями схем элементов, которые существовали на момент запроса.

- Повторное выполнение начинается с точки отказа.

Действие «Возобновить» повторно выполняет задачи компонентов, начиная с точки отказа. Оно не выполняет повторную отправку всего запроса на подготовку.

Примеры

- Схема элементов С создает виртуальную машину приложения и виртуальную машину базы данных. Виртуальная машина базы данных успешно развернута, но подготовка виртуальной машины приложения завершается сбоем. При выполнении действия «Возобновить» повторяется только подготовка виртуальной машины приложения.

Если зарегистрирован сбой подготовки компонента, система считает, что эта задача не выполнялась. Если установка завершается сбоем на этапе настройки виртуальной машины базы данных, например из-за ошибки в сценарии, но сама база данных не повреждена, то при запуске сценария в ходе возобновления эта база данных еще существует. Сценарий установки, включающий в себя сценарий настройки, не будет выполнен повторно. Таким образом, действие «Возобновить» не будет выполнено. Необходимо исправить сценарий и подготовить новый экземпляр.

- Еще один угол зрения: поиск этапа, который назначен, но подготовка выполнена со сбоем. В этом примере действие «Возобновить» выполняет повторную попытку подготовки с точки отказа, при этом запрос на возобновление обрабатывает устаревшую информацию о назначении, поэтому возобновление завершается сбоем.

Использование действия возобновления и подписок на рабочие процессы

Если рабочий процесс подписки завершается сбоем, невозможно выполнить действие возобновления, чтобы продолжить выполнение этого рабочего процесса. Действие возобновления можно запустить только в случае сбоя события подготовки, в результате чего будет запущен новый рабочий процесс.

Например, если вы подписаны на событие «Получен запрос в каталог», то каждый из запросов (запрос на подготовку, завершившийся сбоем, и новый запрос на возобновление) по отдельности удовлетворяет условиям подписки, но для подписки запрос, завершившийся сбоем, и запрос на возобновление не являются связанными действиями.

Принудительное удаление развертывания после неудачного запроса на удаление

Можно принудительно удалить развертывание, находящееся в несогласованном состоянии в результате неудачного запроса на удаление.

Если vRealize Automation не удается удалить ресурс развертывания в процессе удаления развертывания, процесс удаления немедленно прекращается, при этом оставшиеся ресурсы развертывания не удаляются. В результате этого сбоя развертывание остается в несогласованном состоянии, используя ресурсы без какого-то очевидного способа удаления развертывания. Администраторы бизнес-групп могут принудительно удалить развертывания, оставшиеся в несогласованном состоянии.

Необходимые условия

- Удостоверьтесь, что вы выполнили вход в vRealize Automation как **администратор бизнес-группы**.
- Перед выполнением действия «Принудительное удаление» просмотрите описание действия «Удаление» в разделе [Пункты меню «Действие» для подготовленных ресурсов](#).

Процедура

1. На вкладке **Развертывания** найдите развертывание, которое нужно удалить.
2. Щелкните **Действия**, затем щелкните **Удалить**.
3. Введите описание и причину запроса.
4. Выберите **Принудительное удаление** и щелкните **Отправить**.

Результаты

vRealize Automation попытается полностью удалить развертывание вместе со всеми его ресурсами. Если ПО vRealize Automation не удастся удалить ресурс развертывания, оно пропускает его и продолжает удаление остальных ресурсов развертывания.

Следующие шаги

Все ресурсы данного развертывания должны быть удалены. Все ресурсы, не удаленные во время принудительного удаления, должны быть удалены вручную. Также убедитесь, что удаляются все подготовленные объекты виртуальной машины, так как vRealize Automation может попытаться повторно использовать их имена узлов, IP-адреса и другие данные о конфигурации во время последующих операций по подготовке.

Устранение неполадок при неудачном развертывании, включающем рабочий процесс vRealize Orchestrator

Если в развертывание схемы элементов, которое завершилось сбоем, входит рабочий процесс vRealize Orchestrator, можно использовать идентификатор маркера для устранения неполадок, связанных с рабочим процессом. Используйте идентификатор маркера для поиска журналов в vRealize Orchestrator.

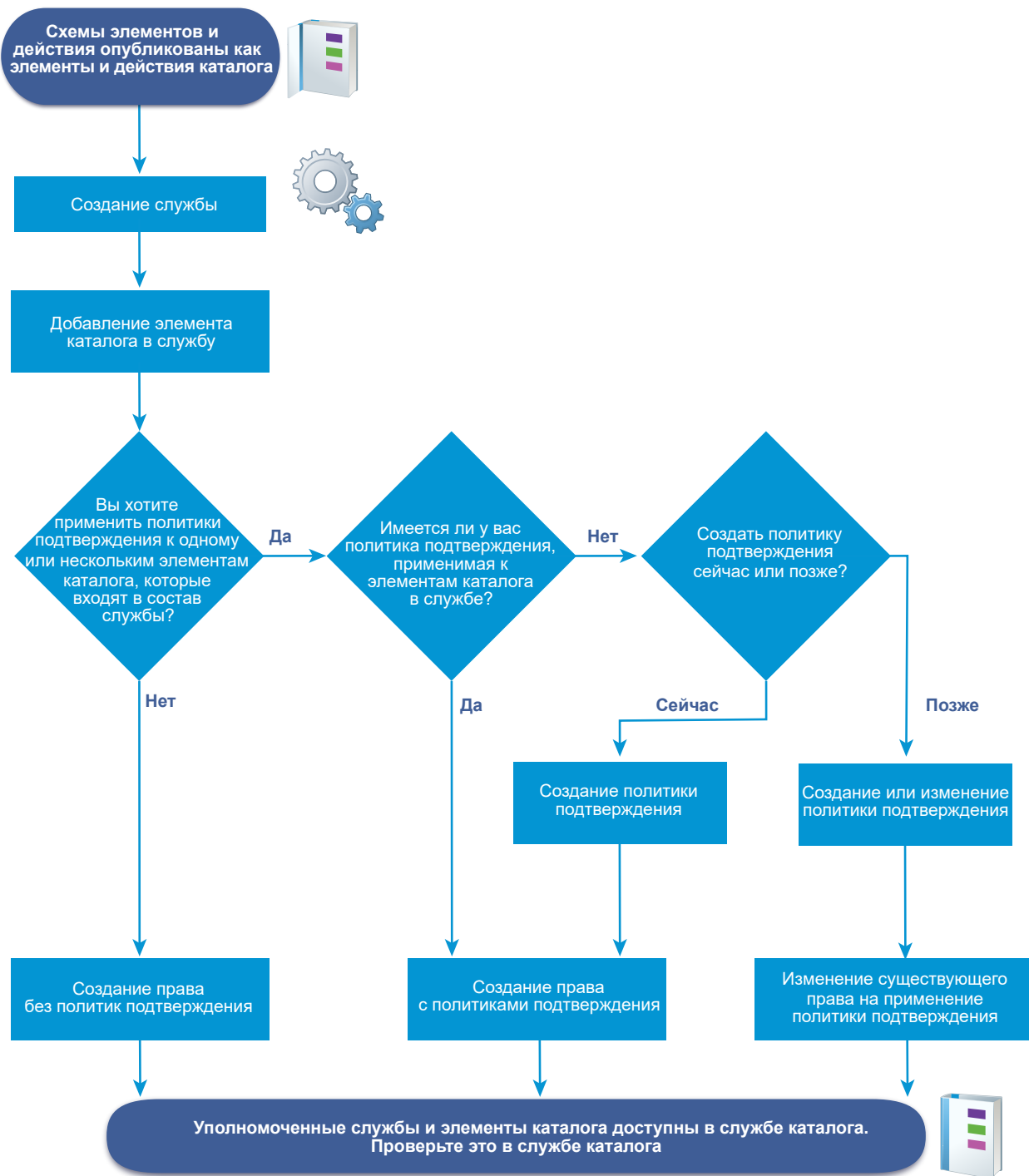
Решение

1. Найдите идентификатор маркера для рабочего процесса, который завершился сбоем.
 - а) В vRealize Automation перейдите на вкладку **Развертывания** и найдите нужное развертывание или действие.
 - б) Нажмите имя развертывания.
Запрос может относиться к развертыванию или действию.
 - в) Нажмите вкладку **Журнал**, а затем — вкладку **Входные данные запроса**.
Если схема элементов основана на рабочем процессе vRealize Orchestrator, заголовок страницы будет следующим: «Сведения о выполнении рабочего процесса vRealize Orchestrator».
 - г) Найдите идентификатор маркера и скопируйте его в буфер обмена или текстовый файл.
Например, ff8080815a685352015a6c8d450801ee.
2. Найдите журналы рабочего процесса в vRealize Orchestrator, используя центр управления.
 - а) Введите базовый URL-адрес для vRealize Automation в поле поиска браузера.
Появится страница устройства VMware vRealize Automation.
 - б) Щелкните **Центр управления vRealize Orchestrator**.
 - в) Выполните вход в качестве пользователя root.
 - г) Щелкните элемент **Проверить рабочие процессы**.
 - д) Щелкните элемент **Завершенные рабочие процессы**.
 - е) Вставьте маркер рабочего процесса в текстовое поле «Идентификатор маркера».
В списке будет показан рабочий процесс, соответствующий идентификатору маркера.
 - ж) Щелкните строку и проверьте журналы, чтобы найти причину сбоя.

Управление каталогом служб

Каталог служб — место, в котором заказчики запрашивают компьютеры и другие компоненты для использования. Управление доступом пользователей к элементам каталога служб осуществляется на основе структуры служб, управления и предоставления пользователям прав на один или несколько элементов.

Рабочий процесс по добавлению элементов в каталог служб отличается в зависимости от того, создаются или применяются политики подтверждения.



Контрольный список для настройки каталога служб

После создания и публикации схемы элементов и действий можно создать службу vRealize Automation, настроить элементы каталога и назначить права и подтверждения.

Настройка контрольного списка для каталога служб позволяет получить общее представление о шагах, которые необходимо выполнить, чтобы настроить каталог. В нем также приведены ссылки на описание точек принятия решений и подробные инструкции для каждого шага.

Таблица 3-70. Настройка контрольного списка для каталога служб

Задача	Требуемая роль	Сведения
<input type="checkbox"/> Добавление службы	администратор арендатора и администратор каталога	См. раздел Добавление службы .
<input type="checkbox"/> Добавление элемента каталога в службу	администратор арендатора и администратор каталога	См. раздел Добавление элементов каталога в службу .
<input type="checkbox"/> Настроить элемент каталога в службе.	администратор арендатора и администратор каталога	См. раздел Настройка элемента каталога .
<input type="checkbox"/> Создать и применить права на использование элемента каталога.	администратор арендатора или диспетчер бизнес- групп	См. раздел Предоставление пользователям права на использование службы, элементов каталога и действий .
<input type="checkbox"/> Создание и применение политик подтверждения к элементу каталога	администратор арендатора или администратор подтверждения может создавать политики подтверждения применять политики подтверждения может администратор арендатора или диспетчер бизнес- групп	См. раздел Создание политики подтверждения .

Создание служб

Служба — это группа элементов каталога, которые вы хотите иметь в каталоге служб. Вы можете уполномочить службу, а она, в свою очередь, уполномочивает пользователей бизнес-группы работать со всеми связанными элементами каталога. Кроме того, вы можете применить политику подтверждения к службе.

Служба функционирует как динамическая группа элементов каталога. Если уполномочить службу, то все элементы каталога, с ней связанные, доступны в каталоге служб указанным пользователям, а все элементы, добавленные в службу или удаленные из нее, влияют на каталог служб.

При создании службы ее можно использовать в качестве категории службы, чтобы можно было собирать предложения услуг для пользователей каталога службы. В качестве примера можно привести службу рабочих столов Windows, включающую в себя элементы каталога Windows 7, 8 и 10, или службу Linux, включающую в себя элементы операционных систем CentOS и RHEL.

Добавление службы

Добавьте службу, чтобы элементы каталога были доступны пользователям каталога служб. Все элементы каталога должны быть связаны со службой, чтобы можно было предоставить пользователям право на эти элементы.

После назначения пользователям права на использование службы, элементы каталога отображаются вместе в каталоге служб. Можно также предоставить пользователям право на отдельные элементы каталога.

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.

Процедура

1. Выберите **Администрирование > Управление каталогом > Службы**.

2. Выберите значок **Создать** (+).

3. Введите имя и описание.

Эти значения отображаются в каталоге служб для пользователей каталога.

4. Чтобы добавить для службы в каталоге служб определенный значок, нажмите кнопку **Обзор** и выберите изображение.

Поддерживаемые типы файлов изображений: GIF, JPG и PNG. Отображается изображение размером 40 x 40 пикселей. Если не выбрать пользовательское изображение, в каталоге служб будет отображаться значок по умолчанию.

5. В раскрывающемся меню **Состояние** выберите состояние.

Параметр	Описание
Неактивно	Служба недоступна в каталоге служб. Когда служба находится в этом состоянии, можно связать элементы каталога со службой, но невозможно предоставить пользователям право на использование службы. Если выбрать параметр Неактивно для активной уполномоченной службы, она удаляется из каталога служб до повторной активации.
Активно	(По умолчанию.) Пользователям можно предоставить право на использование службы и связанных с ней элементов каталога. В этом случае она доступна в каталоге служб таких пользователей.
Удалено	Удаление службы из vRealize Automation. Все связанные элементы каталога по-прежнему присутствуют, но ни один элемент, связанный со службой в каталоге служб, не доступен для пользователей каталога.

6. Настройка параметров службы.

Следующие параметры позволяют предоставить информацию пользователям каталога служб. Эти параметры не влияют на доступность службы.

Параметр	Описание
Часы	Настройте время, соответствующее периоду доступности группы поддержки. Это местное время. Время работы службы не должно переходить с одного дня на другой. Например, нельзя задать время работы службы с 16:00 до 4:00. Чтобы задать время работы после полуночи, создайте два права. Одно — для времени с 16:00 до 00:00, а другое — с 00:00 до 4:00.
Владелец	Укажите пользователя или группу пользователей, которые являются основными владельцами службы и связанных элементов каталога.
Группа поддержки	Укажите настраиваемую группу пользователей или пользователя, которые доступны для поддержки в случае возникновения каких-либо проблем у пользователей каталога служб при подготовке элементов с помощью службы.
Изменить окно	Выберите дату и время планируемых изменений в службе. Дата и время указываются только для справки и не влияют на доступность службы.

7. Нажмите кнопку **Добавить**.

Следующие шаги

Свяжите элементы каталога со службой, чтобы можно было предоставить пользователям право на эти элементы. См. [Добавление элементов каталога в службу](#).

Добавление элементов каталога в службу

Добавление элементов каталога в службы, чтобы предоставить пользователям право запрашивать элементы в каталоге служб. Элемент каталога можно связать только с одной службой.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Убедитесь, что служба существует. См. [Добавление службы](#).
- Убедитесь, что один или несколько элементов каталога опубликованы. См. [Настройка элемента каталога](#).

Процедура

1. Выберите **Администрирование > Управление каталогом > Службы**.
2. Выберите службу, в которую добавляются элементы каталога, и щелкните **Управление элементами каталога**.

3. Щелкните значок **Элементы каталога** (+).

- а) Выберите элементы каталога, чтобы включить их в эту службу.

В диалоговом окне «Выбор элементов каталога» отображаются только те элементы, которые еще не связаны со службой.

- б) Нажмите кнопку **Добавить**.

4. Нажмите кнопку **Заккрыть**.

Следующие шаги

- Для элемента каталога можно добавить собственный значок, который будет отображаться для элемента в каталоге служб. См. [Настройка элемента каталога](#).
- Предоставьте пользователям право на использование службы или элементов каталога, чтобы они могли запрашивать их в каталоге служб. См. [Создание прав](#).

Работа с элементами каталога и действиями

Элементы каталога — это опубликованные схемы элементов для компьютеров, компонентов программного обеспечения и других объектов. Действия в области управления каталогом — это опубликованные действия, которые можно выполнять с подготовленными элементами каталога. Чтобы определить опубликованные схемы элементов и действия, а также сделать их доступными для пользователей каталога служб, можно использовать списки.

Опубликованные элементы каталога

Элемент каталога — это опубликованная схема элементов. Опубликованные схемы элементов также можно использовать в других схемах элементов. Повторное использование схем элементов в других схемах элементов не отображается в списке элементов каталога.

Опубликованные элементы каталога могут также содержать элементы, которые являются только компонентами схем элементов. К примеру, опубликованные компоненты программного обеспечения перечислены как элементы каталога, но на самом деле они доступны лишь как часть развертывания.

Элементы каталога развертывания должны быть связаны со службой, чтобы их можно было сделать доступными в каталоге служб для пользователей, которым предоставлено соответствующее право. В каталоге служб появляются только активные элементы. Элементы каталога можно настроить для другой службы и деактивировать их, если необходимо временно удалить элементы из каталога служб. Кроме того, для них можно добавлять пользовательские значки, которые отображаются в каталоге.

Опубликованные действия

Действия — это изменения, внесенные в подготовленные элементы каталога. Например, виртуальную машину можно перезагрузить.

Действия могут включать в себя встроенные действия или действия, созданные с помощью Все как услуга. Встроенные действия вносят при добавлении компьютера или другой предоставленной схемы элементов. Действия Все как услуга необходимо создавать и публиковать.

Действия не связаны со службами. На действие должно распространяться право, в которое включен элемент каталога, в котором выполняется действие. Действия, на которые пользователям предоставляют права, не отображаются в каталоге служб. Действия могут выполняться с подготовленным элементом в каталоге служб на вкладке пользователя **Развертывания** в зависимости от возможности применения к элементу и текущему состоянию элемента.

Для действия, которое отображается на вкладке **Развертывания**, можно добавить пользовательский значок.

Настройка элемента каталога

Элемент каталога — это опубликованная схема элементов, на использование которой можно предоставить право пользователям. С помощью параметров элементов каталога можно изменить состояние или связанную службу. Можно также просмотреть права, которые позволяют выполнять действия с выбранным элементом каталога.

В каталоге служб отображаются только те элементы каталога, которые связаны со службой и назначены пользователям. Элементы каталога можно связать только с одной службой.

Если вы не хотите отображать элемент каталога в каталоге служб, но при этом не хотите удалять его из права или опубликованного списка элементов каталога, то можете деактивировать этот элемент. Деактивированный элемент каталога будет иметь статус «Списано» в таблице и «Неактивно» в параметрах настройки. Вы сможете активировать его позже.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Убедитесь, что по крайней мере одна схема элементов опубликована в качестве элемента каталога. См. раздел [Публикация схемы элементов](#).

Процедура

1. Выберите **Администрирование > Управление каталогом > Элементы каталога**.
2. Выберите элемент каталога и щелкните **Настроить**.

3. Настройте параметры элемента каталога.

Параметр	Описание
Значок	Найдите образ. Поддерживаемые типы файлов изображений: GIF, JPG и PNG. Отображается изображение размером 40 x 40 пикселей. Если не выбрать пользовательское изображение, в каталоге служб будет отображаться значок каталога по умолчанию.
Состояние	Возможные значения состояния: Активно , Неактивно , Промежуточное хранение . <ul style="list-style-type: none"> ■ Активно. Элемент каталога отображается в каталоге служб, и уполномоченные пользователи могут использовать его для подготовки ресурсов. В списке элементов каталога этот элемент будет отображаться как опубликованный. ■ Неактивно. Элемент каталога недоступен в каталоге служб. В списке элементов каталога этот элемент будет отображаться как списанный. ■ Промежуточное хранение. Элемент каталога недоступен в каталоге служб. Выберите этот пункт меню, если элемент был когда-то неактивным и состояние промежуточного хранения используется для того, чтобы показать, что планируется его повторная активация. В списке элементов каталога этот элемент будет отображаться с состоянием промежуточного хранения.
Квота	Задаёт количество экземпляров этого элемента каталога, которое может развернуть пользователь. Если пользователь превысит это количество, в данном запросе к каталогу отобразится соответствующее уведомление, и запрос не будет отправлен.
Служба	Выберите службу. Все элементы каталога должны быть связаны со службой, если они должны отображаться в каталоге служб для пользователей, которым предоставлено соответствующее право. В списке содержатся как активные, так и неактивные службы.

4. Чтобы просмотреть права, которые предоставляют пользователю доступ к элементам каталога, перейдите на вкладку **Права**.

5. Щелкните **Обновить**.

Следующие шаги

- Чтобы сделать элемент каталога доступным в каталоге служб, предоставьте пользователям право на использование службы, связанной с этим элементом, или отдельного элемента. См. раздел [Создание прав](#).
- Чтобы политики подтверждения применялись для отдельных пользователей надлежащим образом, необходимо задать порядок обработки прав. Чтобы сделать это, задайте уровень приоритета для нескольких прав одной бизнес-группе. См. раздел [Установка приоритета прав](#).

Настройка действия для каталога служб

Действие — это изменение или рабочий процесс, который может выполняться для подготовленных элементов. Можно добавить значок или просмотреть права, которые позволяют выполнять выбранное действие.

Действия бывают либо встроенными (применяются для подготовленных компонентов компьютера, сети и других схем элементов), либо опубликованными действиями Все как услуга.

Поддерживаемые типы файлов изображений для значков: GIF, JPG и PNG. Отображается изображение размером 40 x 40 пикселей. Если не выбрать пользовательское изображение, на вкладке **Развертывания** будет отображаться значок действия по умолчанию.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Убедитесь, что опубликовано по крайней мере одно действие. См. [Публикация схемы элементов](#) и [Публикация действия ресурса](#).

Процедура

1. Выберите **Администрирование > Управление каталогом > Действия**.
2. Выберите общее действие и нажмите **Просмотреть сведения** или для действий в отношении любого ресурса как услуга — **Настроить**.
3. Найдите образ.
4. Чтобы просмотреть права, которые позволяют пользователю выполнять действие, перейдите на вкладку **Права**.
5. Щелкните элемент **Готово**.

Следующие шаги

[Предоставление пользователям права на использование службы, элементов каталога и действий](#).

Создание прав

Права определяют, какие элементы и действия доступны в каталоге службы для участников выбранной бизнес-группы. Чтобы элементы отображались в каталоге служб, необходимо активировать соответствующее право. Если для некоторых элементов требуется управление, можно с помощью прав применить политики подтверждения к разным элементам.

Чтобы можно было настроить право, элементы каталога нужно включить в службу. Права позволяют выполнять действия с различными службами, элементами каталога из служб, на которые распространяются другие права, а также действия, которые можно выполнять над развертываемыми элементами каталога.

Общие сведения о взаимодействии параметров в составе прав

От настройки права зависит содержимое каталога служб. Взаимодействие служб, элементов и компонентов каталога, действий и политик подтверждения влияет на то, что пользователь каталога служб может запрашивать и как применяются политики подтверждения.

При создании права нужно принять во внимание взаимодействие служб, элементов каталога, действий и подтверждений.

■ Службы в рамках прав

Уполномоченная служба функционирует как динамическая группа элементов каталога. Если элемент каталога добавляется в службу после назначения ему права, он становится доступным для указанных пользователей без дополнительной настройки.

■ Компоненты и элементы каталога в рамках прав

Уполномоченные элементы каталога представляют собой схемы элементов, которые можно запрашивать в каталоге служб. Уполномоченные компоненты входят в состав схем элементов, но их нельзя запрашивать в каталоге служб.

■ Действия в рамках прав

Действия, выполняемые с развернутыми элементами каталога. На вкладке «Развертывания» отображаются подготовленные элементы каталога и действия, которые вы можете с ними выполнять. Чтобы можно было выполнить действие с развернутым элементом, оно должно быть включено в право вместе с элементом каталога, подготовившего элемент из каталога служб.

■ Политики подтверждения в рамках прав

Политики подтверждения применяются в составе прав, обеспечивая управление ресурсами в среде.

Службы в рамках прав

Уполномоченная служба функционирует как динамическая группа элементов каталога. Если элемент каталога добавляется в службу после назначения ему права, он становится доступным для указанных пользователей без дополнительной настройки.

Если применить политику подтверждения к службе, то она будет применяться ко всем запрашиваемым элементам службы.

Компоненты и элементы каталога в рамках прав

Уполномоченные элементы каталога представляют собой схемы элементов, которые можно запрашивать в каталоге служб. Уполномоченные компоненты входят в состав схем элементов, но их нельзя запрашивать в каталоге служб.

Ниже перечислены различные виды уполномоченных компонентов и элементов каталога.

Элементы каталога

- Элементы из любой службы, доступ к которой вы хотите предоставить уполномоченным пользователям, в том числе элементы службы, не входящей в текущее право.

Например, как администратор каталога вы связываете разные версии Red Hat Enterprise Linux со службой Red Hat и предоставляете право на использование службы инженерам по контролю качества продукта А. Затем вы получаете запрос на создание элементов каталога службы, который включает в себя только последнюю версию операционных систем на основе Linux для учебных групп. Создайте право для учебной группы, в которое включены последние версии других операционных систем в службе. Последняя версия RHEL уже связана с другой службой, поэтому нужно добавить RHEL в качестве элемента каталога, а не добавлять всю службу Red Hat.

- Элементы, входящие в службу, которая включена в текущее право. При этом к отдельному элементу каталога нужно применять политику подтверждения, которая отличается от политики, применяемой к службе.

Например, как диспетчер бизнес-группы вы даете своей команде разработки право пользоваться службой, которая включает в себя три элемента каталога виртуальных машин. Затем вы применяете политику подтверждения, для которой, если речь идет о компьютерах с более чем четырьмя ЦП, требуется подтверждение администратора виртуальной инфраструктуры. Одна виртуальная машина используется для тестирования производительности, поэтому вы добавляете ее в качестве элемента каталога и применяете менее ограничительную политику подтверждения для той же группы пользователей.

Компоненты

- Компоненты не доступны по имени в службе каталога, поскольку являются частью элемента каталога. Права для них назначаются отдельно, поэтому к компоненту можно применить политику подтверждения, которая отличается от политики элемента каталога, в который входит данный компонент.

Например, элемент включает в себя компьютер и программное обеспечение. Компьютер доступен в качестве подготавливаемого элемента. Для него действует политика подтверждения, для которой требуется подтверждение диспетчера сайта. Программное обеспечение недоступно в качестве автономного подготавливаемого элемента. Оно доступно только как часть запроса компьютера., но для политики подтверждения программного обеспечения требуется подтверждение администратора лицензирования программного обеспечения в вашей организации. Когда компьютер запрашивается в каталоге службы, это должны подтвердить администратор сайта и администратор лицензирования программного обеспечения перед его подготовкой. После подготовки компьютер с записью программного обеспечения отображается на вкладке «Развертывания» запросившей стороны как часть компьютера.

Действия в рамках прав

Действия, выполняемые с развернутыми элементами каталога. На вкладке «Развертывания» отображаются подготовленные элементы каталога и действия, которые вы можете с ними выполнять. Чтобы можно было выполнить действие с развернутым элементом, оно должно быть включено в право вместе с элементом каталога, подготовившего элемент из каталога служб.

Например, право 1 включает виртуальную машину vSphere и действие создания моментального снимка, а право 2 включает только виртуальную машину vSphere. При развертывании компьютера vSphere из права 1 становится доступным действие создания моментального снимка. При развертывании компьютера vSphere из права 2 не становится доступным ни одно действие. Чтобы это действие было доступно пользователям права 2, добавьте действие создания моментального снимка в право 2.

Если выбрать действие, неприменимое ни к одному элементу каталога в праве, оно не будет отображаться как действие на вкладке «Развертывания». Например, ваше право включает в себя компьютер vSphere и вы разрешаете действие уничтожения для облачного компьютера. На подготовленном компьютере действие уничтожения не будет доступным.

Вы можете применить политику подтверждения к действию, отличающемуся от политики, примененной к элементу каталога в праве.

Если пользователь каталога служб участвует в нескольких бизнес-группах и у одной из групп есть только право на включение и выключение, а у другой — на удаление, пользователь сможет выполнять все три действия в отношении соответствующего подготовленного компьютера.

Практические рекомендации по предоставлению пользователям прав на действия

Схемы элементов являются достаточно сложными по своей природе, поэтому предоставление прав по выполнению действий в подготовленных схемах элементов может привести к непредсказуемому поведению. При предоставлении пользователям каталога служб прав на выполнение действий со своими подготовленными элементами следуйте следующим практическим рекомендациям.

- Когда вы предоставляете пользователям право на действие «Удалить компьютер», предоставьте им право на действие «Удалить развертывание». Подготовленная схема элементов является развертыванием.

Развертывание может содержать компьютер. Если пользователю каталога служб предоставлено право на выполнение действия «Удалить компьютер» и не предоставлено право на действие «Удалить развертывание», то при выполнении действия «Удалить компьютер» на последнем или единственном компьютере в развертывании появляется сообщение об отсутствии разрешения на выполнение данного действия. Если право предоставлено на выполнение обоих действий, развертывание будет удалено из среды. Для управления действием «Удалить развертывание» можно создать политику предварительного подтверждения и применить его к действию. Эта политика позволит заданному утверждающему проверять запрос «Удалить развертывание» перед его выполнением.

- Если вы предоставляете пользователям каталога служб право на действие «Изменить аренду», «Изменить владельца», «Завершить срок действия», «Перенастроить» и другие действия, которые могут применяться к компьютерам и развертываниям, предоставьте им право на оба действия.

Политики подтверждения в рамках прав

Политики подтверждения применяются в составе прав, обеспечивая управление ресурсами в среде.

Чтобы политику подтверждения можно было применить при создании права, эта политика должна уже существовать. В ином случае можно создать право и оставить его в состоянии черновика или неактивном состоянии до тех пор, пока не будут созданы политики подтверждения, нужные для элементов каталога и действия в этом праве, а политики применить потом.

Вы не обязаны применять политику подтверждения к любому элементу и действию. Если никакая политика подтверждения не применяется, элементы и действия развертываются по запросу без активации запроса на подтверждение.

Предоставление пользователям права на использование службы, элементов каталога и действий

При добавлении службы, элемента каталога или действия к праву пользователям, указанным в праве, дается возможность запрашивать подготавливаемые элементы в каталоге служб. Действия связаны с элементами и отображаются на вкладке **Развертывания** запрашивающего пользователя.

Есть несколько ролей пользователя, с помощью которых можно создавать права для бизнес-групп.

- Администраторы арендатора могут создавать права для любой бизнес-группы в своем арендаторе.
- Диспетчеры бизнес-групп могут создавать права для групп, которыми они управляют.
- Администраторы каталога могут создавать права для любой бизнес-группы в своем арендаторе.

При создании права необходимо выбрать бизнес-группу и членов в данной бизнес-группе, которым будет предоставлено право.

Сведения о том, как создать право для использования взаимодействий между службами, элементами каталога и действий с подтверждениями см. в разделе [Создание прав](#).

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Убедитесь, что элементы каталога, право на использование которых вы предоставляете пользователям, связаны со службой. См. раздел [Добавление элементов каталога в службу](#).
- Убедитесь, что бизнес-группа, для которой определяется право, существует и что определены пользователи-участники и группы пользователей. См. раздел [Создание бизнес-группы](#).
- Если при создании этого права вы планируете добавить подтверждения, убедитесь, что политики подтверждения существуют. См. раздел [Создание политики подтверждения](#). Если необходимо предоставить пользователям право доступа к элементам каталога служб без подтверждений, можно добавить подтверждения позже, изменив соответствующим образом право.

Процедура

1. Выберите **Администрирование > Управление каталогом > Права**.
2. Выберите значок **Создать** (+).
3. Настройте группу параметров **Сведения**.

Параметры «Сведения» определяют способ отображения права в списке прав и пользователей, которые имеют доступ к элементам в каталоге служб.

Параметр	Описание
Имя и описание	Информация о праве, которое отображается в списке прав.
Срок действия	Укажите дату и время, если нужно, чтобы право стало активным в определенный день..
Состояние	<p>Можно выбрать одно из следующих значений: «Активно», «Неактивно» и «Удалено».</p> <ul style="list-style-type: none"> ■ Активно. Элементы доступны в каталоге служб. Этот параметр доступен, когда вы добавляете или изменяете права. ■ Неактивно. Элементы недоступны в каталоге служб. Право было деактивировано из-за истечения срока действия, или его деактивировал пользователь. ■ Удалено. Выполняется удаление права.

Параметр	Описание
Бизнес-группа	<p>Выберите бизнес-группу. Вы можете создать права только для одной бизнес-группы, и уполномоченные пользователи должны быть участниками бизнес-группы.</p> <p>Если необходимо, чтобы право было доступно всем пользователям, у вас должна быть бизнес-группа «Все пользователи» либо же нужно создать права для каждой бизнес-группы.</p> <p>Если вы вошли как диспетчер бизнес-группы, вы можете создать права только для вашей бизнес-группы.</p>
Пользователи и группы	<p>Выберите Все пользователи и группы, чтобы предоставить всем членам бизнес-группы право доступа к элементам каталога и действиям в нем. Также можно предоставить право отдельным пользователям или группам. Для активации права необходимо выбрать хотя бы одного пользователя бизнес-группы или группу.</p>

4. Нажмите кнопку **Далее**.

- Щелкните значок **Создать** (+), чтобы предоставить пользователям право на использование служб, элементов каталога или действий.

Можно создать право с разными сочетаниями служб, элементов и действий.

Параметр	Описание
Уполномоченные службы	<p>Чтобы предоставить уполномоченным пользователям доступ ко всем элементам опубликованного каталога, связанным со службой, добавьте службу.</p> <p>Уполномоченная служба предполагает динамическое право. Если элемент добавляется в службу позже, он попадает в каталог служб для уполномоченных пользователей. Права могут включать в себя как службы, так и индивидуальные элементы каталога.</p>
Уполномоченные компоненты и элементы каталога	<p>Добавьте отдельные элементы, доступные уполномоченным пользователям.</p> <p>Права могут включать в себя как службы, так и индивидуальные элементы каталога. Чтобы применить к элементу, включенному в службу, другую политику подтверждения, добавьте ее в качестве элемента каталога. Политика подтверждения, указанная для элемента, имеет более высокий приоритет, чем политика подтверждения службы, к которой принадлежит этот элемент, если на службу и элемент распространяется одно и то же право. Если они относятся к разным правам, порядок зависит от заданного приоритета.</p> <p>Элементы каталога должны быть связаны со службой, чтобы быть доступными в каталоге служб. Элемент каталога может быть связан с любой службой, а не только со службой в текущем праве.</p> <p>Компоненты входят в состав того или иного элемента каталога, но они не доступны по имени в каталоге служб. Например, программное обеспечение MySQL является компонентом элемента каталога «виртуальная машина CentOS». Компонентам предоставляются те же права, что и элементам каталога, в которые они входят. Если требуется применить политику подтверждения для конкретного программного обеспечения, необходимо предоставить данное право соответствующему элементу. В остальных случаях для развертывания компонента вместе с родительским элементом компоненту не требуется предоставлять отдельные права.</p>

Параметр	Описание
Уполномоченные действия	<p>Добавьте действия, если нужно позволить пользователям выполнять действия по отношению к подготовленному элементу.</p> <p>Действия, которые нужно выполнить по отношению к элементам, подготовленным на основе этого права, нужно включить в это право.</p> <p>Уполномоченные действия не отображаются в каталоге служб. Они отображаются на вкладке "Развертывания" для подготовленного элемента.</p>
Действия применяются только к элементам, заданным в этом праве	<p>Определяет, к чему можно применять уполномоченные действия: ко всем применимым элементам каталога служб или только к элементам в этом праве.</p> <p>Если установлен этот флажок, члены бизнес-группы могут выполнять действия по отношению к соответствующим элементам в этом праве. Данный метод назначения права на действия позволяет задавать действия для конкретных элементов.</p> <p>Если этот флажок не установлен, пользователи, для которых назначено право, могут выполнять действия по отношению ко всем применимым элементам каталога, вне зависимости от того, распространяется ли на них это право. Активны также любые политики подтверждения, примененные к этим действиям.</p>

- Для фильтрации доступных элементов воспользуйтесь раскрывающимися меню в каждом разделе.
- Чтобы включить элементы в право, установите соответствующие флажки.
- Чтобы добавить политику подтверждения в выбранную службу, элемент или действие, выберите политику подтверждения в раскрывающемся меню **Применить эту политику к выбранным элементам**.

Если применить к службе политику подтверждения, то все элементы в службе будут относиться к одной и той же политике подтверждения. Чтобы применить к элементу другую политику, добавьте его в качестве элемента каталога и примените соответствующую политику.

- Нажмите кнопку **ОК**.

Служба, элемент и действие будут добавлены в право.

- Чтобы сохранить право, щелкните **Готово**.

Результаты

Если право является активным, то служба и элементы будут добавлены в каталог служб.

Следующие шаги

Убедитесь, что уполномоченные службы и элементы каталога отображаются для уполномоченных пользователей в каталоге служб и что запрошенные элементы подготавливают целевые объекты так, как ожидалось. Можно запросить элемент от имени выбранных пользователей.

Установка приоритета прав

Если для одной бизнес-группы существует несколько прав, можно задать их приоритет, чтобы при запросе пользователя каталога служб право и связанная с ним политика подтверждения обрабатывались в указанном порядке.

Если настроить политику подтверждения для группы пользователей, и нужно, чтобы у участника группы была уникальная политика для одной или нескольких служб, элементов каталога или действий, задайте для права участника больший приоритет, чем для права группы. Когда участник запрашивает элемент в каталоге служб, применяемая политика подтверждения основывается на уровне приоритета прав для бизнес-группы. При первом поиске имени участника (в качестве участника пользовательской группы или отдельного пользователя) применяется политика подтверждения.

Например, создается две группы прав для одного и того же элемента каталога, чтобы одну политику подтверждения можно было применить к группе пользователей «Учет», а другую — к Игорю, участнику этой группы.

Таблица 3-71. Примеры прав

Право 1	Право 2
Бизнес-группа: «Финансы»	Бизнес-группа: «Финансы»
Пользователи и группы: группа «Учет»	Пользователи и группы: Игорь
Элемент каталога 1: политика А	Элемент каталога 1: политика С

Игорь запрашивает элемент каталога 1 в каталоге служб. В зависимости от уровня приоритета для бизнес-группы «Финансы» к запросу Игоря применяется другая политика.


Таблица 3-72. Примеры результатов

Конфигурация и результат	Уровень приоритета	Уровень приоритета
Уровень приоритета	1: право 1 2: право 2	1: право 2 2: право 1
Применяемая политика	Применяется политика А. Игорь входит в группу пользователей «Учет». Поиск Игоря в качестве пользователя, обладающего правами, прекращается на праве 1, и применяется политика подтверждения.	Применяется политика С. Поиск Игоря в качестве пользователя, обладающего правами, прекращается на праве 2, и применяется политика подтверждения.

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.

Процедура

1. Выберите **Администрирование > Управление каталогом > Права**.
2. Щелкните значок **Установить приоритет** ().
3. В раскрывающемся списке **Бизнес-группа** выберите бизнес-группу.
4. Перетащите право в новое расположение в списке, чтобы изменить его приоритет.

5. Выберите способ обновления.

Параметр	Описание
Обновить	Сохранение изменений.
Обновить и закрыть	Сохранение изменений и закрытие окна Установить приоритет элементов .

Работа с политиками подтверждения

Политики подтверждения являются средствами управления, добавляемыми к запросам в каталог служб для управления ресурсами в среде. Каждая политика представляет собой определенный набор условий, которые могут быть применены к службам, элементам каталога и действиям при предоставлении пользователям прав на эти элементы.

Процесс применения политики подтверждения

Во-первых, администратор арендатора или администратор подтверждения создает политику подтверждения там, где необходимо управление подготовкой.

Политики подтверждения создаются для типов политик подтверждения или конкретных элементов. Если политика основывается на типе политики, то можно применить ее к соответствующим типам элементов каталога. Например, если политика основана на типе политики «Программное обеспечение», то можно задать и применять ее для каких-либо программных элементов в правах. Если политика определена для конкретного элемента, то она должна применяться только к этому элементу. Например, если элемент является определенным элементом программного обеспечения, то необходимо применять его только к этому конкретному элементу программного обеспечения баз данных в праве.

Политики могут включать требования предварительного подтверждения и фактического подтверждения. Для политик с требованием предварительного подтверждения запрос должен быть подтвержден до подготовки запрашиваемого элемента. Для политик с требованиями фактического подтверждения необходимо, чтобы утверждающее лицо приняло запрос до того, как подготовленный элемент становится доступным для запрашивающего пользователя.

Конфигурации предварительного и фактического подтверждения состоят из одного или нескольких уровней, которые определяют, когда политика подтверждения срабатывает, а также кто подтверждает или как подтверждается запрос. Можно включать несколько уровней. Например, политика подтверждения может иметь один уровень для подтверждения руководителя, за которым следует уровень для финансового подтверждения.

Далее администратор арендатора или менеджер бизнес-группы применяет политику подтверждения к службам, элементам каталога и действиям по мере необходимости.

Наконец, когда пользователь каталога служб запрашивает элемент, к которому применяется политика подтверждения, утверждающие лица согласуют или отклоняют запрос на вкладке **Входящие**.

Запрашивающий пользователь может отслеживать состояние подтверждения для конкретного запроса на своей вкладке **Развертывания**.

Примеры политик подтверждения, основанных на типе политики виртуальной машины

Вы можете создать политику подтверждения и применять ее к конкретному типу элементов каталога, но в случае запроса элемента в каталоге служб такая политика будет давать разные результаты. В зависимости от способа определения и применения политики подтверждения ее влияние на пользователя каталога служб и утверждающего будет разным.

В таблице ниже приведены примеры различных политик подтверждения, которые основаны на одном типе политики подтверждения. Эти примеры иллюстрируют некоторые возможные способы настройки политик подтверждения для обеспечения управления различного типа.

Таблица 3-73. Примеры политик подтверждения и результатов их применения

Цели управления	Выбранный тип политики	Предварительное или последующее подтверждение	Когда требуется подтверждение	Кто является утверждающим и	Как политика применяется в праве	Результаты при запросе элемента в каталоге служб
Диспетчер бизнес-группы должен подтверждать любые запросы виртуальных машин. Политика подтверждения должна применяться к нескольким бизнес-группам в различных правах.	Каталог служб — Запрос элемента каталога — Виртуальная машина	Вкладка «Добавить к предварительному подтверждению»	Выберите «Всегда требуется»	Выберите Определить утверждающих из запроса. Выберите условие Бизнес-группа > Диспетчеры > Пользователи > Диспетчер. Выберите Подтвердить может кто угодно.	Права основаны на бизнес-группах. Это подтверждение может использоваться в любом праве, где для виртуальной машины требуется подтверждение диспетчера.	Когда пользователь каталога служб запрашивает виртуальную машину, к которой было применено это подтверждение, диспетчер бизнес-группы должен подтвердить запрос до подготовки компьютера.
Администратор виртуальной инфраструктуры должен проверить корректность подготовки виртуальной машины и подтвердить запрос до того, как виртуальная машина будет предоставлена запрашивающему пользователю.	Каталог служб — Запрос элемента каталога — Виртуальная машина	Вкладка «Добавить к последующему подтверждению»	Выберите «Всегда требуется»	Выберите Определенные пользователи и группы. Выберите администраторов виртуальной инфраструктуры и настраиваемые группы пользователей. Выберите Подтвердить может кто угодно.	Это подтверждение может использоваться в любом праве, где необходимо, чтобы администратор виртуальной инфраструктуры проверял виртуальную машину в vCenter Server после ее подготовки.	Когда пользователь каталога служб запрашивает виртуальную машину, к которой было применено это подтверждение, выполняется подготовка этой виртуальной машины. Если каждый член группы администратора в виртуальной инфраструктуры подтверждает запрос, машина предоставляется пользователю.

Таблица 3-73. Примеры политик подтверждения и результатов их применения (продолжение)

Цели управления	Выбранный тип политики	Предварительное или последующее подтверждение	Когда требуется подтверждение	Кто является утверждающим и	Как политика применяется в праве	Результаты при запросе элемента в каталоге служб
Для управления ресурсами виртуальной инфраструктуры и контроля затрат необходимо добавить два уровня предварительного подтверждения, так как одно подтверждение предназначено для ресурсов компьютера, а второе — для затрат на компьютер на каждый день.	Каталог служб — Запрос элемента каталога — Виртуальная машина	Вкладка «Добавить к предварительно му подтверждению»	Уровень 1 Выберите Требуется при определенных условиях. Настройте условия, когда число ЦП > 6, память > 8 или хранилище > 100 ГБ.	Выберите Определить утверждающих из запроса. Выберите условие «Отправитель запроса > диспетчер». Выберите . Щелкните Свойства системы и выберите ЦП Память и Хранилище, чтобы утверждающий мог изменить значение и указать допустимый уровень.	Эта политика подтверждения может использоваться в праве, где необходимо, чтобы запрос подтверждали диспетчер запрашивающего пользователя и сотрудник финансового отдела.	Когда пользователь каталога служб запрашивает виртуальную машину, выполняется анализ запроса, чтобы определить, не превышают ли запрашиваемое количество ЦП, объем памяти или хранилища значения, указанные на уровне 1. Если не превышают, анализируется условие для уровня 2. Если запросы превышают, по крайней мере, одно из условий для уровня 1, диспетчер должен подтвердить запрос. Диспетчер может уменьшить запрашиваемый объем ресурсов для конфигурации и дать подтверждение или отклонить запрос.

Таблица 3-73. Примеры политик подтверждения и результатов их применения (продолжение)

Цели управления	Выбранный тип политики	Предварительное или последующее подтверждение	Когда требуется подтверждение	Кто является утверждающим и	Как политика применяется в праве	Результаты при запросе элемента в каталоге служб
			Уровень 2 Выберите Требуется при определенных условиях. Настройте условие «Затраты > 15,00 в день».	Выберите Определенные пользователи и группы. Выберите настраиваемую группу пользователей — финансы. Выберите Подтвердить может кто угодно.		
Для параметризованный элементов каталога схемы элементов администратор облака должен подтвердить запросы на развертывание, в которых для профиля size компонента компьютера vSphere установлено значение large.	Каталог служб — Запрос элемента каталога — Виртуальная машина	Вкладка «Добавить к предварительно му подтверждению»	Уровень 1 Выберите Требуется при определенных условиях. Уровень 2 Выберите Одно условие. Выберите Профиль компонента > Размер компьютера vSphere. Для условия size задайте значение large.	Выберите Определенные пользователи и группы. Выберите пользователей и группы, которым разрешено подтверждать запросы. Выберите Подтвердить может кто угодно.	Эту политику подтверждения можно использовать в праве, позволяющем администратор у облака подтверждать запрос на подготовку.	Когда пользователь каталога служб запрашивает виртуальную машину, к которой было применено это подтверждение, администратор облака должен подтвердить запрос до подготовки компьютера.

Пример действий с политиками подтверждения, применяемыми в составном развертывании

При применении политик подтверждения к действиям, которые могут выполняться в различных компонентах составной схемы элементов, процесс подтверждения зависит от способа настройки права и применения политик подтверждения.

В этом примере для создания схемы элементов используются конкретные сведения, а затем политики подтверждения применяются к действиям, которые можно выполнить из каталога служб в подготовленной схеме элементов в различных правах. Схема элементов представляет собой составную схему элементов, в которой содержится еще одна схема элементов. Используемые действия выполняют удаление подготовленных элементов, удаление развертывания для схем элементов и виртуальной машины для компьютера. В результате действия удаления применяются к выбранным элементам и применяемые политики подтверждения запускают запросы на подтверждение.

Пример схемы элементов

В этом примере настраивается схема элементов, которая включает в себя вложенную схему элементов с виртуальной машиной.

- Схема элементов 1 — схема элементов непрерывной интеграции
 - Схема элементов 2 — схема элементов предпроизводственной среды
 - Виртуальная машина 1 — виртуальная машина vSphere TestAsAService

Политики подтверждения для действий удаления

Чтобы удалить подготовленные элементы, нужно настроить две политики подтверждения. Удаление А — действие развертывания, которое может выполняться в схеме элементов 1 или схеме элементов 2 в этом примере. Удаление А — действие виртуальной машины, которое может выполняться на виртуальной машине 1. Создаются политики подтверждения, которые будут применяться к действиям в праве.

Имя политики подтверждения	Тип политики подтверждения
Политика подтверждения А	Каталог служб: запрос на действие ресурсов — удаление — развертывание
Политика подтверждения Б	Каталог служб: запрос на действие ресурсов — удаление — виртуальная машина

Права и политики подтверждения, применяемые к действиям

Настраиваются три права. Каждое право включает в себя составную схему элементов. Для каждого права добавляются действия удаления и применяются политики подтверждения.

Название права	Уполномоченное действие в подготовленном компьютере	Применяемая политика подтверждения
Право 1	Удаление — развертывание	Политика подтверждения А
Право 2	Удаление — виртуальная машина	Политика подтверждения Б
Право 3	Удаление — развертывание	Политика подтверждения А
	Удаление — виртуальная машина	Политика подтверждения Б

Действия пользователя в каталоге служб

Когда пользователь каталога служб выполняет действие, происходит удаление схем элементов или компьютеров в зависимости от элемента, для которого выполнялось действие.

Действие пользователя в каталоге служб	Выбранное действие	Удаленные схемы элементов или компьютеры
Действие 1	Удаление — действие развертывания, выполняемое в схеме элементов 1 — схема элементов непрерывной интеграции	Схема элементов 1, схема элементов 2 и виртуальная машина 1
Действие 2	Удаление — действие развертывания, выполняемое во вложенной схеме элементов 2 — схема элементов предпроизводственной среды	Схема элементов 2 и виртуальная машина 1
Действие 3	Удаление — действие виртуальной машины, выполняемое в компьютере, который находится внутри развертывания, виртуальная машина 1 — виртуальная машина vSphere TestAsAService	Виртуальная машина 1

Политики подтверждения, применяемые к действиям в правах

После подтверждения политик подтверждения утверждающие получают запрос на подтверждение в зависимости от схемы элементов или компьютера, в котором пользователь каталога служб выполнил действие.

Название права	Политика подтверждения в действиях	Действие пользователя	Запущенный запрос на подтверждение	Схемы элементов или компьютеры, удаляемые при подтверждении
Право 1 — удаление политики подтверждения развертывания	Политика А (политика подтверждения развертывания удаления) — только действие развертывания	Действие 1 (выполнение удаления — действие развертывания в схеме элементов 1)	Запросы на подтверждение запускаются только для схемы элементов 1	Схема элементов 1, схема элементов 2 и виртуальная машина 1
		Действие 2 (выполнение удаления — действие развертывания в схеме элементов 2)	Запросы на подтверждение запускаются только для схемы элементов 2	Схема элементов 2 и виртуальная машина 1
		Действие 3 (удаление — действие виртуальной машины выполняется на виртуальной машине 1)	Нет запущенных запросов на подтверждение	Виртуальная машина 1
Право 2	Политика Б (удаление — политика виртуальной машины) — только действие виртуальной машины	Действие 1 (выполнение удаления — действие развертывания в схеме элементов 1)	Нет запущенных запросов на подтверждение	Схема элементов 1, схема элементов 2 и виртуальная машина 1
		Действие 2 (выполнение удаления — действие развертывания в схеме элементов 2)	Нет запущенных запросов на подтверждение	Схема элементов 2 и виртуальная машина 1

Название права	Политика подтверждения в действиях	Действие пользователя	Запущенный запрос на подтверждение	Схемы элементов или компьютеры, удаляемые при подтверждении
		Действие 3 (удаление — действие виртуальной машины выполняется на виртуальной машине 1)	Запросы на подтверждение запускаются только для виртуальной машины 1	Виртуальная машина 1
Право 3	Политика А (политика подтверждения развертывания удаления) удаления — действие развертывания и политика Б (удаление — политика виртуальной машины) удаления — действие виртуальной машины	Действие 1 (выполнение удаления — действие развертывания в схеме элементов 1)	Запросы на подтверждение запускаются только для схемы элементов 1	Схема элементов 1, схема элементов 2 и виртуальная машина 1
		Действие 2 (выполнение удаления — действие развертывания в схеме элементов 2)	Запросы на подтверждение запускаются только для схемы элементов 2	Схема элементов 2 и виртуальная машина 1
		Действие 3 (удаление — действие виртуальной машины выполняется на виртуальной машине 1)	Запросы на подтверждение запускаются только для виртуальной машины 1	Виртуальная машина 1

Пример политики подтверждения в рамках нескольких прав

Если применить политику подтверждения к элементу, который используется в нескольких правах, назначенных одним и тем же пользователям в бизнес-группе, она запустится в элементе службы, даже в том случае, если эта политика напрямую не применяется в праве.

Например, можно создать следующие схемы элементов, службы, политики подтверждения и права.

Схемы элементов

- Виртуальная машина vSphere RHEL
- Тестирование обеспечения качества выполняется для виртуальной машины vSphere RHEL.
- Обучение обеспечению качества выполняется для виртуальной машины vSphere RHEL.

Службы

- Схема элементов тестирования обеспечения качества связана со службой тестирования.
- Схема элементов обучения обеспечению качества связана со службой тестирования.

Права

- Право 1
- Право 2

Таблица 3-74. Конфигурации права

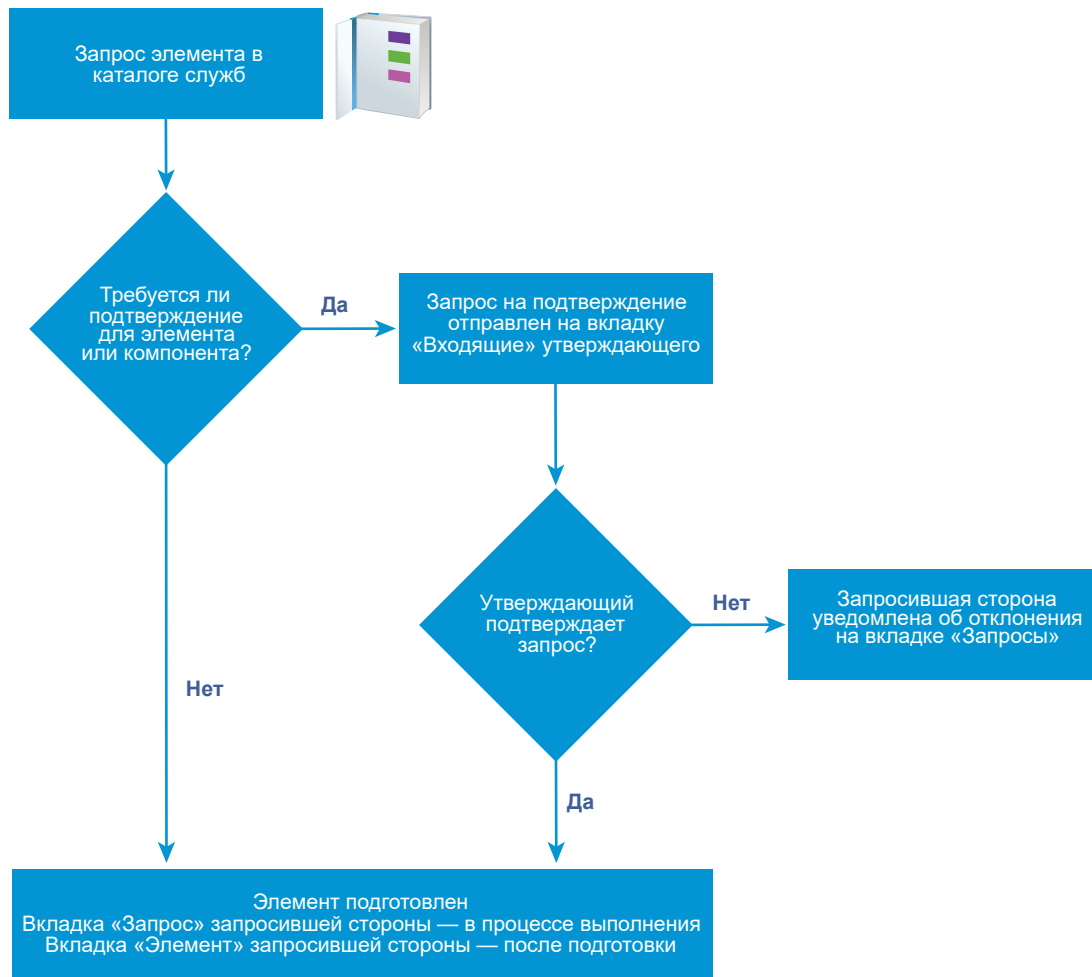
Название права	Бизнес-группа	Уполномоченная служба	Уполномоченный элемент
Право 1	Обеспечения качества	Тестирование	Запрос на элемент каталога — виртуальная машина применяется к компоненту виртуальной машины
Право 2	Обеспечения качества	Обучение	

Результаты

Если пользователь в каталоге служб выбирает обучение обеспечению качества, политика подтверждения запускается для виртуальной машины vSphere RHEL. Это обусловлено тем, что схема элементов этой машины создана на основе компонента виртуальной машины, который используется в схеме элементов обучения обеспечению качества.

Обработка политик подтверждения в каталоге служб

Когда пользователь запрашивает объект каталога служб, к которому применяется политика подтверждения, рабочий процесс обработки запроса утверждающим и запрашивающим пользователями аналогичен следующему:



Создание политики подтверждения

Администраторы арендатора и администраторы подтверждения могут определять политики подтверждения и использовать их для управления правами. В политике подтверждения можно настроить несколько уровней, чтобы использовать события перед подтверждением и после подтверждения.

Если изменить какой-либо параметр в схеме элементов программного компонента и политика подтверждения использует этот параметр для запуска запросов на подтверждение, политика подтверждения может не работать должным образом. Если необходимо изменить параметр компонента, убедитесь, что изменения не повлияют на политики подтверждения.

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.

Процедура

1. Настройка сведений о политике подтверждения

При создании политики подтверждения задается тип политики подтверждения, ее имя, описание и состояние.

2. Создание уровня подтверждения

При создании политики подтверждения можно добавить уровни предварительного или последующего подтверждения.

3. Настройка формы подтверждения для добавления системных и настраиваемых свойств

Пользователи могут добавлять системные и настраиваемые свойства, которые будут отображаться в формах подтверждения. Эти свойства позволяют утверждающим изменять значения системных свойств для параметров ресурсов компьютера, например процессора или памяти, а также изменять настраиваемые свойства, прежде чем запрос на подтверждение будет заполнен.

4. Параметры политики подтверждения

При создании политики подтверждения настраиваются различные параметры, определяющие условия подтверждения элемента, запрашиваемого пользователями каталога служб. Подтверждение может потребоваться до начала подготовки по запросу или после подготовки элемента, но до его предоставления запрашивающему пользователю.

Настройка сведений о политике подтверждения

При создании политики подтверждения задается тип политики подтверждения, ее имя, описание и состояние.

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.
2. Выберите значок **Создать** (+).

3. Выберите тип политики или компонент программного обеспечения.

Параметр	Описание
Выберите тип политики подтверждения	<p>Позволяет создать политику подтверждения в зависимости от типа запросов.</p> <p>Выберите этот параметр, чтобы определить политику подтверждения, которая будет применяться ко всем элементам каталога этого типа. Доступны следующие типы запросов: универсальный, запрос на элемент каталога или на действие ресурса.</p> <p>Доступные параметры конфигурации условий зависят от типа. Определенному типу соответствуют конкретные поля конфигурации. Например, если выбрать «Каталог служб: запрос на элемент каталога», будут доступны поля, которые являются общими для всех запросов на элементы каталога, а если выбрать «Каталог служб: запрос на элемент каталога — виртуальная машина» — будут доступны общие параметры, а также параметры, зависящие от виртуальных машин.</p> <p>Выбор определенного типа запроса ограничивает ряд элементов каталога или действий, к которым можно применить политику подтверждения.</p>
Выберите элемент	<p>Позволяет создать политику подтверждения на основе определенного элемента.</p> <p>Выберите этот параметр, чтобы определить политику подтверждения, которую следует применять к конкретным элементам, недоступным в виде отдельных элементов в каталоге служб, а доступным только в составе компьютера или другого развертывания, например к компонентам программного обеспечения.</p> <p>Доступные поля конфигурации условий зависят от элемента и могут предоставлять более подробные данные, чем критерии, доступные для элемента согласно типу политики.</p>
Список	<p>Предоставляет список доступных типов политики или элементов каталога.</p> <p>Позволяет искать или сортировать столбцы для поиска конкретного элемента или типа.</p>

4. Нажмите кнопку **ОК**.

5. Введите имя и, при необходимости, описание.

6. Выберите состояние политики в раскрывающемся меню **Состояние**.

Параметр	Описание
Черновик	Сохранение политики подтверждения в состоянии с возможностью редактирования.
Активно	Сохранение политики подтверждения в состоянии с доступом только для чтения, которое можно использовать для права.
Неактивно	Сохранение политики подтверждения в состоянии с доступом только для чтения, которое нельзя использовать для права, пока не будет активирована политика.

Следующие шаги

Создайте уровни до и после подтверждения.

Создание уровня подтверждения

При создании политики подтверждения можно добавить уровни предварительного или последующего подтверждения.

Для одной политики подтверждения можно создать несколько уровней подтверждения. Когда пользователь каталога служб запросит элемент, к которому применяется политика подтверждения с несколькими уровнями, для отправки запроса на подтверждение следующему утверждающему требуется подтверждение первого уровня. См. раздел [Работа с политиками подтверждения](#).

Если настроить политику подтверждения, которая запускается по запросу на продление аренды, необходимо выбрать для требования подтверждения значение "Всегда требуется".

Необходимые условия

[Настройка сведений о политике подтверждения.](#)

Процедура

1. На вкладке **Предварительное подтверждение** или **Последующее подтверждение** щелкните значок **Создать (+)**.
2. Введите имя и, при необходимости, описание.
3. Выберите требование в отношении подтверждения.

Параметр	Описание
Всегда требуется	Политика подтверждения срабатывает для каждого запроса.
Требуется при определенных условиях	<p>Политика подтверждения основывается на одном или нескольких предложениях условий.</p> <p>Если выбрать этот параметр, необходимо создать условия. Если эта политика подтверждения применяется к соответствующим службам, элементам каталога или действиям, относящимся к праву, происходит оценка условий. При соответствии условиям прежде чем запрос будет подготовлен, его должен подтвердить определенный утверждающий. Если он не соответствует условиям, подготовка запроса происходит без подтверждения. Например, все запросы на виртуальную машину с 4 и более процессорами должен подтвердить администратор виртуальной инфраструктуры.</p> <p>Доступные поля, на основе которых формируются условия, зависят от выбранного типа политики подтверждения или элемента каталога.</p> <p>При вводе значения для условия учитывается регистр.</p> <p>Чтобы настроить несколько предложений условия, выберите для условий логическую операцию.</p>

4. Выберите утверждающих.

Параметр	Действие
Определенные пользователи и группы	Обеспечивает отправку запросов на подтверждение выбранным пользователям.
Определить утверждающих из запроса	<p>Обеспечивает отправку запроса на подтверждение пользователям в зависимости от определенного условия.</p> <p>Примечание Убедитесь в том, что все пользователи, которые будут динамически определены запросом и инициатором запроса, существуют в vRealize Automation, что они синхронизированы в Active Directory и доступны для просмотра в разделе Администрирование > Пользователи и группы > Пользователи и группы каталога.</p> <p>Если пользователь не синхронизирован в поставщике удостоверений службы управления каталогами и он указывается во время запроса каталога, то при обработке такого запроса возникает ошибка «Утверждение запрашиваемого элемента».</p>
Использовать подписку на события	<p>Обеспечивает обработку запросов на подтверждение на основе определенных подписок на события.</p> <p>Чтобы определить подписку на рабочий процесс, выберите Администрирование > События > Подписки. Соответствующие подписки на рабочие процессы используются перед подтверждением и после него.</p>

5. Укажите утверждающего запросов или действий.

Параметр	Описание
Подтвердить может кто угодно	<p>Прежде чем запрос будет обработан, его должен подтвердить один из утверждающих.</p> <p>При получении запроса на элемент каталога служб запросы на подтверждение отправляются всем утверждающим. Если один утверждающий подтвердит запрос, запрос будет считаться подтвержденным, после чего он будет удален из папок входящих запросов других утверждающих.</p>
Подтвердить должны все	Прежде чем запрос будет обработан, его должны подтвердить все утверждающие.

6. Добавьте свойства в форму подтверждения или сохраните уровень.

- Чтобы добавить свойства в форму подтверждения, щелкните **Свойства системы** или **Настраиваемые свойства**.
- Чтобы сохранить уровень, нажмите кнопку **ОК**.

Следующие шаги

Сведения о добавлении свойств в форму подтверждения см. в разделе [Настройка формы подтверждения для добавления системных и настраиваемых свойств](#).

Настройка формы подтверждения для добавления системных и настраиваемых свойств

Пользователи могут добавлять системные и настраиваемые свойства, которые будут отображаться в формах подтверждения. Эти свойства позволяют утверждающим изменять значения системных свойств для

параметров ресурсов компьютера, например процессора или памяти, а также изменять настраиваемые свойства, прежде чем запрос на подтверждение будет заполнен.

Доступные свойства системы зависят от типа политики подтверждения и конфигурации схемы элементов. Чтобы некоторые свойства отображались в списке свойств системы, в их полях, настроенных в схеме элементов, должны быть заданы минимальное и максимальное значения.

Настраиваемые свойства можно включать при добавлении уровня подтверждения. Если настраиваемое свойство настроено и включено в схему элементов, при дальнейшем добавлении настраиваемых свойств в форму подтверждения экземпляры соответствующего свойства будут перезаписаны, например в схемах элементов, группах свойств или конечных точках.

Утверждающий может изменить выбранные или настроенные свойства в форме подтверждения.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.
- [Создание уровня подтверждения](#).

Процедура

1. На вкладке **Предварительное подтверждение** или **Последующее подтверждение** щелкните значок **Создать (+)**.
2. Перейдите на вкладку **Свойства системы**.
3. Установите флажок для каждого свойства системы, которое должен настроить утверждающий во время подтверждения.
4. Настройте настраиваемые свойства.

Добавьте одно или несколько свойств системы, которое должен настроить утверждающий во время подтверждения.

а) Перейдите на вкладку **Настраиваемые свойства**.

б) Выберите значок **Создать (+)**.

в) Введите значения настраиваемых свойств.

Параметр	Описание
Имя	Введите имя свойства.
Метка	Введите метку, которая будет показана утверждающему в форме подтверждения.
Описание	Введите подробную информацию для утверждающего. Она отображается в подсказке к полю в форме.

г) Нажмите кнопку **Сохранить**.

д) Чтобы удалить несколько настраиваемых свойств, выберите строки и нажмите кнопку **Удалить**.

5. Нажмите кнопку **ОК**.

Следующие шаги

- Добавьте дополнительные уровни предварительного и последующего подтверждения.
- Сохраните политику подтверждения. Политика должна быть активной, чтобы ее можно было применять к службам, элементам или действиям в разделе **Права**.

Параметры политики подтверждения

При создании политики подтверждения настраиваются различные параметры, определяющие условия подтверждения элемента, запрашиваемого пользователями каталога служб. Подтверждение может потребоваться до начала подготовки по запросу или после подготовки элемента, но до его предоставления запрашивающему пользователю.

Выберите **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**.

■ [Параметры типа политики подтверждения](#)

Тип политики подтверждения определяет ее параметры, а также то, к каким элементам или действиям в рамках предоставленного права ее можно применить. При добавлении уровней подтверждения от типа или элемента политики зависит, для каких полей можно будет создать условия для уровней подтверждения.

■ [Добавление параметров политики подтверждения](#)

Вы настраиваете основные сведения о политике подтверждения, включая состояние политики, чтобы иметь возможность управлять этой политикой.

■ [Добавление сведений об уровне в параметры политики подтверждения](#)

Уровень подтверждения включает условия, которые запускают процесс утверждения, когда пользователь каталога служб запрашивает элемент, а также любые свойства системы и настраиваемые свойства, которые вы хотите включить. После запуска запросы на подтверждение отправляются указанным утверждающим.

■ [Добавление свойств системы в параметры политики подтверждения](#)

Вы выбрали свойства системы, которые требуется добавить в форму подтверждения и разрешить утверждающему изменять значение.

■ [Добавление настраиваемых свойств в параметры политики подтверждения](#)

Вы настраиваете свойства, которые требуется добавить в форму подтверждения, чтобы утверждающий мог изменять значение.

Параметры типа политики подтверждения

Тип политики подтверждения определяет ее параметры, а также то, к каким элементам или действиям в рамках предоставленного права ее можно применить. При добавлении уровней подтверждения от типа или элемента политики зависит, для каких полей можно будет создать условия для уровней подтверждения.

Выберите **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**.

Таблица 3-75. Параметры типа политики подтверждения

Параметр	Описание
Выберите тип политики подтверждения	<p>Позволяет создать политику подтверждения в зависимости от типа запросов.</p> <p>Выберите этот параметр, чтобы определить политику подтверждения, которая будет применяться ко всем элементам каталога этого типа. Доступны следующие типы запросов: универсальный, запрос на элемент каталога или на действие ресурса.</p> <p>Доступные параметры конфигурации условий зависят от типа. Определенному типу соответствуют конкретные поля конфигурации. Например, если выбрать «Каталог служб: запрос на элемент каталога», будут доступны поля, которые являются общими для всех запросов на элементы каталога, а если выбрать «Каталог служб: запрос на элемент каталога — виртуальная машина» — будут доступны общие параметры, а также параметры, зависящие от виртуальных машин.</p> <p>Выбор определенного типа запроса ограничивает ряд элементов каталога или действий, к которым можно применить политику подтверждения.</p>
Выберите элемент	<p>Позволяет создать политику подтверждения на основе определенного элемента.</p> <p>Выберите этот параметр, чтобы определить политику подтверждения, которую следует применять к конкретным элементам, недоступным в виде отдельных элементов в каталоге служб, а доступным только в составе компьютера или другого развертывания, например к компонентам программного обеспечения.</p> <p>Доступные поля конфигурации условий зависят от элемента и могут предоставлять более подробные данные, чем критерии, доступные для элемента согласно типу политики.</p>
Список	<p>Предоставляет список доступных типов политики или элементов каталога.</p> <p>Позволяет искать или сортировать столбцы для поиска конкретного элемента или типа.</p>

Добавление параметров политики подтверждения

Вы настраиваете основные сведения о политике подтверждения, включая состояние политики, чтобы иметь возможность управлять этой политикой.

Для определения основных сведений о политике подтверждения выберите **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**. Выберите тип политики и нажмите кнопку **ОК**.

Таблица 3-76. Параметры политики подтверждения

Параметр	Описание
Имя	Имя, которое появляется при применении политики подтверждения в праве.
Описание	Введите подробное описание структуры политики подтверждения. Эти сведения необходимы для управления политиками подтверждения.

Таблица 3-76. Параметры политики подтверждения (продолжение)

Параметр	Описание
Состояние	<p>Возможны следующие значения:</p> <ul style="list-style-type: none"> ■ Черновик. Политика подтверждения недоступна для применения в правах. После перевода политики в активное состояние ее будет невозможно вернуть в состояние черновика. ■ Активно. Политика подтверждения доступна для применения в правах. ■ Неактивно. Политика подтверждения недоступна для применения в правах. Если политика не была применена к правам и вы делаете ее неактивной, ее можно удалить, но повторно активировать данную политику будет невозможно. Если политика была применена и вы делаете ее неактивной, элементы, к которым она применяется, необходимо связать с другой политикой, в противном случае связь этих элементов будет удалена. Права на несвязанные элементы и действия по-прежнему предоставляются пользователям, но применяемая политика подтверждения отсутствует.
Тип политики	<p>Отображает тип запроса политики подтверждения.</p> <p>Если выбран элемент каталога, который можно использовать в качестве основы для политики подтверждения, отображается соответствующий тип запроса.</p>
Элемент	<p>Отображает выбранный элемент каталога.</p> <p>Если выбран элемент каталога, который можно использовать в качестве основы для политики подтверждения, это поле остается пустым.</p>
Автор последнего обновления	Имя пользователя, который внес изменения в политику подтверждения.
Дата последнего обновления	Дата последнего изменения политики подтверждения.
Уровень предварительного подтверждения	Чтобы требовать подтверждение перед подготовкой запрашиваемых элементов или выполнением действия, настройте одно или несколько условий, которые запускают процесс утверждения, когда пользователь каталога служб запрашивает элемент.

Таблица 3-76. Параметры политики подтверждения (продолжение)

Параметр	Описание
Уровень последующего подтверждения	<p>Чтобы требовать подтверждение после подготовки элемента, но до предоставления подготовленного или измененного элемента запрашивающему пользователю каталога служб, настройте одно или несколько условий, которые запускают процесс утверждения.</p> <p>Например, администратор виртуальной инфраструктуры проверяет, что виртуальная машина находится в работоспособном состоянии, прежде чем предоставить ее пользователю каталога служб.</p>
Просмотреть связанные права	<p>Отображаются все права, в рамках которых политика подтверждения применяется к службам, элементам каталога или действиям. Элементы в одном праве можно связать с другой политикой.</p> <p>Этот параметр доступен только при просмотре активной политики подтверждения.</p>

Добавление сведений об уровне в параметры политики подтверждения

Уровень подтверждения включает условия, которые запускают процесс утверждения, когда пользователь каталога служб запрашивает элемент, а также любые свойства системы и настраиваемые свойства, которые вы хотите включить. После запуска запросы на подтверждение отправляются указанным утверждающим.

Для определения основных сведений о политике подтверждения выберите **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**. Выберите тип политики и нажмите кнопку **ОК**. На вкладке «Предварительное подтверждение» или «Последующее подтверждение» щелкните значок **Создать (+)**.

Вы устанавливаете приоритеты для уровней исходя из порядка их обработки. После запуска политики подтверждения запрос отклоняется, если отклоняется первый уровень подтверждения.

Таблица 3-77. Параметры сведений об уровне

Параметр	Описание
Имя	<p>Введите имя.</p> <p>Название уровня отображается при просмотре запросов, на которые распространяется политика подтверждения.</p>
Описание	<p>Введите описание уровня, например CPU>4 для администратора виртуальной инфраструктуры.</p>
Когда требуется подтверждение?	<p>Выберите, время начала применения политики подтверждения.</p>
Всегда требуется	<p>Политика подтверждения срабатывает для каждого запроса.</p> <p>Если выбрать этот параметр и применить эту политику подтверждения к соответствующим службам, элементам каталога или действиям, относящимся к праву, до подготовки запроса его обязательно должен подтвердить определенный утверждающий. Например, все запросы должен подтверждать диспетчер запросившего пользователя.</p>

Таблица 3-77. Параметры сведений об уровне (продолжение)

Параметр	Описание
Требуется при определенных условиях	<p>Политика подтверждения основывается на одном или нескольких предложениях условий.</p> <p>Если выбрать этот параметр, необходимо создать условия. Если эта политика подтверждения применяется к соответствующим службам, элементам каталога или действиям, относящимся к праву, происходит оценка условий. При соответствии условиям прежде чем запрос будет подготовлен, его должен подтвердить определенный утверждающий. Если он не соответствует условиям, подготовка запроса происходит без подтверждения. Например, все запросы на виртуальную машину с 4 и более процессорами должен подтвердить администратор виртуальной инфраструктуры.</p> <p>Доступные поля, на основе которых формируются условия, зависят от выбранного типа политики подтверждения или элемента каталога.</p> <p>При вводе значения для условия учитывается регистр.</p> <p>Чтобы настроить несколько предложений условия, выберите для условий логическую операцию.</p> <ul style="list-style-type: none"> ■ Все из указанного. Подтверждение запускается, если запрос соответствует всем условиям. Между предложениями должен стоять логический оператор AND. ■ Что-нибудь из указанного. Уровень подтверждения применяется, если запрос соответствует по крайней мере одному предложению. Между предложениями должен стоять логический оператор OR. ■ Ничего из указанного. Уровень подтверждения запускается, если ни один запрос не соответствует условиям. Между предложениями должен стоять логический оператор NOT.
Утверждающие	Выберите способ подтверждения.
Определенные пользователи и группы	<p>Обеспечивает отправку запросов на подтверждение выбранным пользователям.</p> <p>Выберите пользователей или группы пользователей, которые должны подтвердить запрос на каталог служб, прежде чем он будет подготовлен или будет запущено действие. Например, запрос отправляется группе администраторов виртуальной инфраструктуры, если установлен параметр Подтвердить может кто угодно.</p>
Определить пользователей из запроса	<p>Обеспечивает отправку запроса на подтверждение пользователям в зависимости от определенного условия.</p> <p>Например, если необходимо применить политику подтверждения к бизнес-группам и потребовать подтверждения запросов их диспетчером, выберите Бизнес-группа > Потребитель > Пользователи > Диспетчер.</p>

Таблица 3-77. Параметры сведений об уровне (продолжение)

Параметр	Описание
Использовать подписку на события	<p>Обеспечивает обработку запросов на подтверждение на основе определенных подписок на события.</p> <p>Чтобы определить подписку на рабочий процесс, выберите Администрирование > События > Подписки.</p> <p>Соответствующие подписки на рабочие процессы используются перед подтверждением и после него.</p>
Подтвердить может кто угодно	<p>Прежде чем запрос будет обработан, его должен подтвердить один из утверждающих.</p> <p>При получении запроса на элемент каталога служб запросы на подтверждение отправляются всем утверждающим. Если один утверждающий подтвердит запрос, запрос будет считаться подтвержденным, после чего он будет удален из папок входящих запросов других утверждающих.</p> <p>Если первый утверждающий отклонит запрос, запрашивающий пользователь будет уведомлен об этом и запрос на подтверждение будет удален из папок входящих запросов других утверждающих.</p> <p>Если первый утверждающий подтвердит запрос, но при этом запрос на подтверждение будет открыт в консоли другого утверждающего, он не сможет отправить запрос. Будет считаться, что его подтвердил первый утверждающий.</p> <p>Если выбрать параметр Определенные пользователи и группы или Определить утверждающих из запроса при наличии нескольких утверждающих, этот параметр будет дополнительным. При наличии только одного утверждающего он не будет применяться.</p>
Подтвердить должны все	<p>Прежде чем запрос будет обработан, его должны подтвердить все утверждающие.</p> <p>Если выбрать параметр Определенные пользователи и группы или Определить утверждающих из запроса при наличии нескольких утверждающих, этот параметр будет дополнительным. При наличии только одного утверждающего он не будет применяться.</p>

Добавление свойств системы в параметры политики подтверждения

Вы выбрали свойства системы, которые требуется добавить в форму подтверждения и разрешить утверждающему изменять значение.

Например, для подтверждения виртуальной машины выберите ЦП, если вы хотите разрешить утверждающему изменить запрос и указать не 6 ЦП, а 4 ЦП.

Для выбора свойств системы откройте **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**. Выберите тип политики и нажмите кнопку **ОК**. На вкладке «Предварительное подтверждение» или «Последующее подтверждение» щелкните значок **Создать (+)** и перейдите на вкладку **Свойства системы**.

Таблица 3-78. Параметры свойств системы

Параметр	Описание
Свойства	<p>Список доступных системных свойств зависит от выбранного типа запроса или элемента каталога и наличия свойств системы для этого элемента.</p> <p>Некоторые свойства доступны, только если схема элементов настроена определенным образом. Например, должны быть настроены определенные параметры для процессоров. Для схемы элементов, к которой применяется политика подтверждения с использованием системного свойства центральных процессоров, должен быть задан диапазон. Например, минимальное количество процессоров — 2, а максимальное — 8.</p>

Добавление настраиваемых свойств в параметры политики подтверждения

Вы настраиваете свойства, которые требуется добавить в форму подтверждения, чтобы утверждающий мог изменять значение.

Например, для подтверждения виртуальной машины добавьте **VMware.VirtualCenter.Папка**, если вы хотите разрешить утверждающему указывать папку, к которой добавлен компьютер в vCenter Server.

Вы можете также добавить настраиваемое свойство, которое относится к данной форме политики подтверждения.

Для выбора свойств системы откройте **Администрирование > Политики подтверждения**. Нажмите кнопку **Создать**. Выберите тип политики и нажмите кнопку **ОК**. На вкладке «Предварительное подтверждение» или «Последующее подтверждение» щелкните значок **Создать (+)** и перейдите на вкладку **Настраиваемые свойства**.

Таблица 3-79. Настраиваемые свойства

Параметр	Описание
Имя	Введите имя свойства.
Метка	Введите метку, которая будет показана утверждающему в форме подтверждения.
Описание	<p>Введите подробную информацию для утверждающего.</p> <p>Она отображается в подсказке к полю в форме.</p>

Изменение политики подтверждения

Активную и неактивную политики подтверждения изменять нельзя. Необходимо создать копию исходной политики и заменить политику, которая не приносит требуемых результатов. Активная и неактивная политики подтверждения предназначены только для чтения. Политики подтверждения, которые находятся в состоянии черновика, допускают возможность изменения.


При копировании политики подтверждения новая политика создается на основе исходного типа политики. Можно изменять все атрибуты, кроме типа политики. Это требуется, если необходимо изменить уровни подтверждения для изменения, добавления или удаления уровней, а также добавления системных или настраиваемых свойств в формы.

Можно создать уровни предварительного и последующего подтверждения. Указания по созданию уровней подтверждения см. в разделе [Создание уровня подтверждения](#).

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.
2. Выберите строку политики подтверждения, которую необходимо копировать.
3. Щелкните значок **Копировать** .
- Теперь копия политики подтверждения создана.
4. Выберите новую политику подтверждения, которую необходимо изменить.
5. В текстовом поле **Имя** введите имя.
6. (дополнительно) В текстовом поле **Описание** введите описание.
7. Выберите состояние политики в раскрывающемся меню **Состояние**.

Параметр	Описание
Черновик	Сохранение политики подтверждения в состоянии с возможностью редактирования.
Активно	Сохранение политики подтверждения в состоянии с доступом только для чтения, которое можно использовать для права.
Неактивно	Сохранение политики подтверждения в состоянии с доступом только для чтения, которое нельзя использовать для права, пока не будет активирована политика.

8. Измените уровни до и после подтверждения.
9. Нажмите кнопку **ОК**.

Результаты

Создана новая политика подтверждения на основе существующей политики подтверждения.

Следующие шаги

Примените новую политику подтверждения в праве. См. [Предоставление пользователям права на использование службы, элементов каталога и действий](#).

Деактивация политики подтверждения

Если становится очевидным, что политика подтверждения устарела, ее можно деактивировать, чтобы она не использовалась во время подготовки.

Для деактивации политики подтверждения необходимо назначить новую политику для каждого права, к которому политика подтверждения применяется в настоящее время.

Впоследствии деактивированную политику подтверждения можно либо снова активировать, либо удалить.

Необходимые условия

Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.
2. Щелкните имя политики подтверждения.
3. Щелкните **Просмотреть связанные права**.
 - а) В раскрывающемся меню **Заменить все на** выберите новую политику подтверждения.

Если в списке содержится больше одного права, новая политика подтверждения будет применяться ко всем перечисленным правам.
 - б) Нажмите кнопку **ОК**.
4. Убедившись, что с политикой подтверждения никакие права не связаны, выберите **Неактивно** в меню «Состояние».
5. Нажмите кнопку **ОК**.
6. Для удаления политики подтверждения выберите строку с неактивной политикой.
 - а) Нажмите кнопку **Удалить**.
 - б) Нажмите кнопку **ОК**.

Результаты

Связи политики подтверждения со всеми правами, к которым она применяется, будут удалены, и политика деактивирована. Впоследствии данную политику можно повторно активировать и снова применить к элементам в праве.

Следующие шаги

Если политика подтверждения больше нужна, ее можно удалить. См. [Удаление политики подтверждения](#).

Удаление политики подтверждения

Если у вас есть ненужные политики подтверждения, которые вы деактивировали, их можно удалить из vRealize Automation.

Необходимые условия

- Отмените связь и деактивируйте политики подтверждения. См. [Деактивация политики подтверждения](#).
- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор подтверждения**.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.
2. Выберите строку, содержащую неактивную политику.
3. Щелкните элемент **Удалить**.
4. Нажмите кнопку **ОК**.

Результаты

Политика подтверждения удалена.

Сценарий: создание и применение CentOS с политиками подтверждения MySQL

Администратор арендатора может применить строгое управление запросами к элементам каталога для бизнес-группы разработки и проверки качества. Прежде чем пользователи смогут подготавливать элемент каталога CentOS с MySQL, может потребоваться, чтобы администратор виртуальной инфраструктуры vSphere подтвердил запрос к компьютеру, а также чтобы диспетчер ПО подтвердил запрос к программному обеспечению.

Создайте и примените одну политику для запроса каталога службы vSphere CentOS с MySQL, в которой требуется подтверждение компьютера от администратора виртуальной инфраструктуры vSphere на основе определенных условий, и другую политику подтверждения для компонента MySQL Программное обеспечение, требующую подтверждения каждого запроса менеджером программного обеспечения.

Администраторы подтверждения могут только создавать подтверждения, а менеджеры бизнес-группы могут применять их к правам. Администратор арендатора может не только создавать подтверждения, но и применять их к правам.

Необходимые условия

- Войдите в консоль vRealize Automation в качестве **администратора арендатора**. Как создавать, так и применять политики подтверждения может только администратор арендатора.
- Убедитесь, что элемент каталога CentOS с MySQL включен в службу. См. раздел [Сценарий: предоставление доступа к CentOS со схемой элементов приложения MySQL в каталоге служб](#).

Сценарий: создание CentOS с MySQL для политики подтверждения виртуальной машины

Администратор арендатора должен предоставить группе разработчиков и инженеров по контролю качества виртуальные машины, которые должным образом подготовлены для используемой среды. Поэтому ему нужно создать политику подтверждения, требующую предварительного подтверждения для соответствующих типов запросов.

Поскольку CentOS с MySQL для виртуальной машины потребляет ресурсы vCenter Server, для обеспечения рационального потребления ресурсов требуется, чтобы администратор виртуальной инфраструктуры vSphere подтверждал запросы, если запрашиваемый объем памяти превышает 2048 МБ или используется более 2 ЦП. Утверждающему также предоставляется возможность изменять запрашиваемые объемы ресурсов ЦП и памяти до подтверждения запроса.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.
2. Создайте политику подтверждения для подготовки виртуальной машины.
 - а) Выберите значок **Создать** (+).
 - б) Выберите **Выберите тип политики подтверждения**.
 - в) В списке последовательно выберите **Каталог служб: запрос на элемент каталога — Виртуальная машина**.
 - г) Нажмите кнопку **ОК**.
 - д) Настройте следующие параметры.

Параметр	Конфигурация
Имя	Введите CentOS on vSphere CPU or Memory VM .
Описание	Введите Requires VI Admin approval for CPU>2 or Memory>2048 .
Состояние	Выберите значение Активно .

3. На вкладке **Предварительное подтверждение** щелкните значок **Добавить** (+).
4. Настройте критерии запуска и действия подтверждения на вкладке **Сведения об уровне**.
 - а) В текстовом поле **Имя** введите **CPU>2 or Memory>2048 – VI Admin**.
 - б) В текстовом поле **Описание** введите **VI Admin approval for CPU and Memory**.
 - в) Выберите **Требуется при определенных условиях**.
 - г) В раскрывающемся списке «Предложение» выберите пункт **Что-нибудь из указанного**.
 - д) В новом раскрывающемся списке «Предложение» выберите пункт **ЦП** и настройте значения в предложении **ЦП > 2**.
 - е) Щелкните **Добавить выражение** и введите **Память (МБ) > 2048**, чтобы настроить значения в предложении.
 - ж) Выберите **Определенные пользователи и группы**.
 - з) В текстовом поле поиска введите имя администратора виртуальной инфраструктуры или группы администраторов vSphere, щелкните значок поиска (🔍).
 - и) Выберите пользователя или группу.
 - к) Выберите **Подтвердить может кто угодно**.
Требуется, чтобы один администратор виртуальной инфраструктуры проверил ресурсы и подтвердил запрос.

5. Щелкните вкладку **Свойства системы** и выберите свойства, которые позволяют утверждающему изменить запрашиваемые объемы ресурсов процессора и памяти до подтверждения запроса.

а) Установите флажки **ЦП** и **Память (МБ)**.

б) Нажмите кнопку **ОК**.

6. Нажмите кнопку **ОК**.

Результаты

Теперь политика подтверждения для запросов виртуальных машин создана, однако необходимо также создать подтверждение для компонента MySQL. Подтверждения запускаются только после применения политик к праву.

Сценарий: создание политики подтверждения для Программное обеспечение компонента MySQL

Менеджеры программного обеспечения могут обращаться к администратору арендатора с просьбой создать и применить политику подтверждения для установок MySQL для отслеживания использования лицензирования. Будет создана политика, которая будет уведомлять менеджера лицензий на программное обеспечение всякий раз, когда запрашивается Программное обеспечение компонент MySQL для виртуальных машин Linux.

Данный тип утверждения может потребоваться в некоторых средах, потому что лицензионные ключи должны быть предоставлены менеджеру программного обеспечения. В этом случае нужно, чтобы запрос отслеживался и подтверждался только менеджером программного обеспечения. После создания политики подтверждения она применяется к элементу каталога MySQL для виртуальных машин Linux. Эта политика подтверждения очень специфична и может быть применена только к Программное обеспечение компоненту MySQL для виртуальных машин Linux в правах.

Процедура

1. Выберите **Администрирование > Политики подтверждения**.

2. Создание политики подтверждения для Программное обеспечение компонента MySQL.

а) Выберите значок **Создать (+)**.

б) Выберите **Выберите элемент**.

в) Выберите **MySQL для виртуальных машин Linux**.


г) Нажмите кнопку **ОК**.

д) Настройте следующие параметры.

Параметр	Конфигурация
Имя	Введите Подтверждение отслеживания MySQL.
Описание	Введите Запрос на подтверждение отправлен менеджеру ПО.
Состояние	Выберите значение Активно .

3. На вкладке **Предварительное подтверждение** щелкните значок **Добавить (+)**.

4. Настройте критерии запуска и действия подтверждения на вкладке **Сведения об уровне**.

- а) В текстовое поле **Имя** введите **Уведомление о разворачивании программного обеспечения MySQL**.
- б) В текстовое поле **Описание** введите **Подтверждение установки программного обеспечения менеджером ПО**.
- в) Выберите **Требуется всегда**.
- г) Выберите **Определенные пользователи и группы**.
- д) Введите имя менеджера программного обеспечения в текстовом окне поиска и нажмите на значок поиска () , затем выберите пользователя.
- е) Выберите **Подтвердить может кто угодно**.
Запрос подтверждается одним менеджером программного обеспечения.
Нажмите кнопку **ОК**.

5. Нажмите кнопку **ОК**.

Результаты

Созданы политики подтверждения для виртуальных машин и компонентов Программное обеспечение для виртуальных машин MySQL для Linux. Подтверждения запускаются только после применения политик подтверждения к праву.

Сценарий: применение политик подтверждения к CentOS с компонентами MySQL

Администратор арендатора может создавать политики подтверждения и права. Можно изменить право для разработки и контроля качества, чтобы применять созданные политики подтверждения для запуска подтверждений, когда пользователь каталога служб запрашивает элемент.

Хотя может показаться, что проще выдать бизнес-группе права на всю службу каталога, это не даст вам возможность иметь такой же контроль и управление, как при создании отдельных прав на элементы каталога. Например, если предоставить пользователям права доступа к службе в целом, то они могут запросить любые элементы каталога, имеющиеся в службе, и все элементы, которые будут добавлены в службу в будущем. Это также означает, что можно будет использовать политики подтверждения лишь самого высокого уровня, которые применяются к каждому элементу каталога в службе и всегда требуют подтверждения от менеджера. Если будет принято решение выдавать права на элементы каталога по отдельности, то можно создавать и применять весьма специфические политики подтверждения для каждого элемента и жестко контролировать, кто какие элементы в службе может запрашивать. Если же вы решите выдавать права на отдельные компоненты каталога по отдельности, то получите еще больший контроль.

Если пока неизвестно, какие политики подтверждения необходимо применить к элементам в праве, можно вернуться позже и применить их. В этом сценарии различные политики подтверждения применяются к двум компонентам одной и той же схемы элементов опубликованного приложения.

Процедура

1. Выберите **Администрирование > Управление каталогом > Права**.

2. Выберите Право для разработки и контроля качества.

3. Откройте вкладку Элементы и подтверждения.

4. Добавьте CentOS с компьютером MySQL и примените политику подтверждения.

- а) Нажмите значок **Добавить элементы** (+) рядом с заголовком «Уполномоченные элементы».
- б) Установите флажок **CentOS с MySQL**.
- в) Щелкните стрелку раскрывающегося списка **Применить эту политику к выбранным элементам**.

Политика «ЦП и память» CentOS в vSphere отсутствует в списке.

- г) Выберите **Показать все** и щелкните стрелку вниз, чтобы просмотреть все политики подтверждения.
- д) Выберите **ЦП и память CentOS в vSphere** [каталог служб: запрос на элемент каталога, виртуальная машина].

Компьютер vSphere CentOS — схема элементов компьютера в схеме элементов приложения. Просмотрите имена политики и выберите наиболее подходящее для данного типа элемента каталога. Если применить неправильную политику, то политика подтверждения вызовет ошибку или будут создаваться запросы на подтверждение, основанные на неверных условиях.
- е) Нажмите кнопку **ОК**.

5. Добавьте MySQL в качестве элемента для компонента программного обеспечения виртуальных машин Linux и примените политику подтверждения к этому элементу.

- а) Нажмите значок **Добавить компоненты и элементы каталога** (+) рядом с заголовком «Уполномоченные компоненты и элементы каталога».
- б) В раскрывающемся меню **Добавить компоненты и элементы каталога** выберите **Нет**.

Компоненты программного обеспечения всегда связаны с компьютером. Они не доступны по отдельному запросу в каталоге служб.
- в) Установите флажок **MySQL для виртуальных машин Linux**.
- г) Щелкните стрелку раскрывающегося списка **Применить эту политику к выбранным элементам**.
- д) Выберите **Подтверждение отслеживания MySQL** [Каталог служб: запрос на элемент каталога, компонент программного обеспечения].

Дополнительные настройки не потребуются, потому что политика подтверждения была создана для этого конкретного программного компонента, который добавляется в виртуальную машину.

- е) Нажмите кнопку **ОК**.

6. Добавьте действия, которые пользователь может запускать на подготовленном компьютере.

Политики подтверждения не применимы к действиям в этом сценарии.

- а) Нажмите значок **Добавить действия** значок (+) рядом с заголовком «Уполномоченные действия».
- б) Выберите следующие действия.

Имя/тип	Описание
Создать моментальный снимок/виртуальная машина	Создание моментального снимка виртуальной машины вместе с установленным программным обеспечением. Это позволяет разработчикам создавать моментальные снимки, с которых можно выполнять восстановление в процессе разработки.
Удалить/развертывание	Удаление всей подготовленной схемы элементов, а не только компьютера. Используйте это действие для потерянных компонентов.
Выключить/компьютер	Выключение виртуальной машины.
Включить/компьютер	Включение виртуальной машины.
Восстановить из моментального снимка/виртуальная машина	Восстановление из ранее созданного моментального снимка.

- в) Нажмите кнопку **ОК**.

7. Щелкните элемент **Готово**.

Результаты

Это право позволяет запрашивать различные подтверждения в разных компонентах схемы элементов.

Следующие шаги

Запросите CentOS с элементом MySQL в каталоге служб в качестве члена бизнес-группы, чтобы убедиться в корректном выполнении подтверждений и права.

Запрос подготовки компьютера с помощью параметризованной схемы элементов

При запросе подготовки компьютера для схемы элементов компьютера vSphere, которая может включать профили компонентов размера и образа, указывается параметр подготовки посредством выбора доступного набора значений.

При запросе подготовки можно выбрать доступные параметры Size и Image. При выборе одного из наборов значений к запросу привязывается соответствующее значение свойства.

Набор значений профиля компонента применяется ко всем компьютерам vSphere в кластере.

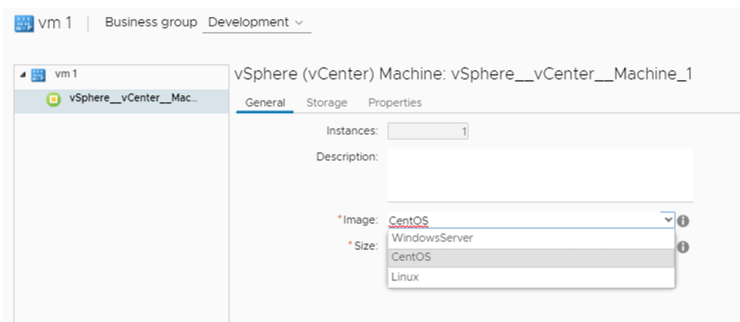
Сведения о настройке профиля компонентов см. в разделе [Общие сведения о параметризации схем элементов и ее использование](#).

Необходимые условия

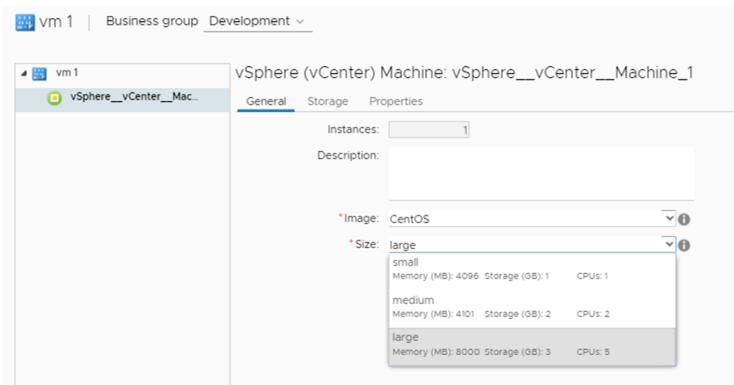
- Определите наборы значений для профилей компонентов **Size** или **Image**. См. и в *Справочник по настраиваемым свойствам*.
- Создайте схему элементов, содержащую компонент компьютера vSphere, в котором содержится профиль компонентов **Image** или **Size**. См. [Настройка схемы элементов компьютера](#) и [Настройки компонентов компьютера vSphere в vRealize Automation](#).
- Опубликуйте схему элементов в каталоге. См. раздел [Публикация схемы элементов](#).
- Настройте схему элементов в каталоге. См. [Контрольный список для настройки каталога служб](#) и [Примеры политик подтверждения, основанных на типе политики виртуальной машины](#).

Процедура

1. Щелкните элемент **Каталог**.
2. Выберите службу каталога, которую необходимо запросить, и щелкните элемент **Запросить**.
3. Выберите компонент компьютера vSphere, который необходимо подготовить, а также укажите количество экземпляров для подготовки.
4. Выберите в раскрывающемся меню **Образ** вариант набора значений для образа.



5. Выберите в раскрывающемся меню **Размер** вариант набора значений для размера.



6. Нажмите кнопку **Отправить**.

Следующие шаги

Наборы значений, указанные для профилей компонентов **Size** и **Image**, теперь доступны в раскрывающихся меню **Образ** и **Размер** на вкладке **Каталог** в форме запроса подготовки каталога.

Сценарий: предоставление доступа к CentOS со схемой элементов приложения MySQL в каталоге служб

По запросу администратора арендатора архитекторами схем элементов создается элемент каталога для MySQL на CentOS, на котором группа разработчиков и инженеров по контролю качества будет выполнять тестовые сценарии. Программный архитектор сообщил, что элемент каталога готов для пользователей. Чтобы предоставить бизнес-пользователям доступ к нему, необходимо связать схемы элементов и компонент Программное обеспечение со службой каталогов, а затем предоставить участникам бизнес-группы право на запрос элемента каталога.

Необходимые условия

- Войдите в службу vRealize Automation как **администратор арендатора** или **администратор каталога**.
- Опубликуйте схему элементов MySQL на виртуальной машине vSphere CentOS. Ознакомьтесь с процессами создания схем элементов компьютеров и программных компонентов в [Создание библиотеки проектов](#).
- При создании схем элементов в среде разработки выполните импорт схемы элементов в производственную среду. См. раздел [Экспорт и импорт схем элементов и содержимого](#).
- Создайте резервирование, чтобы выделить ресурсы vSphere для бизнес-группы, используемой для разработки и обеспечения качества. См. раздел [Создание резервирования для Hyper-V, KVM, SCVMM, vSphere или XenServer](#).

Процедура

1. Сценарий: создание службы каталога для разработки и проверки качества

Администратор арендатора может создать отдельную службу каталога для групп разработки и проверки качества, чтобы другие группы, такие как финансовый отдел и отдел кадров, не видели специализированные элементы каталога. Для публикации всех элементов каталога для нужд разработки и тестирования можно создать службу каталога под названием «Служба для разработки и контроля качества».

2. Сценарий: добавление CentOS с MySQL в службу, используемую для разработки или обеспечения качества

Нужно добавить CentOS с элементом каталога MySQL в службу, используемую для разработки и обеспечения качества, от имени администратора арендатора.

3. Сценарий: предоставление пользователям прав на запрос элементов службы для разработки и контроля качества в качестве элемента каталога

Администратор арендатора может создать право «Разработка и тестирование», а также и добавить элементы каталога и некоторые соответствующие действия, чтобы пользователи групп разработки и контроля качества могли выполнять запросы MySQL в элементе каталога CentOS, а также выполнять действия на компьютере и в развертывании.

Сценарий: создание службы каталога для разработки и проверки качества

Администратор арендатора может создать отдельную службу каталога для групп разработки и проверки качества, чтобы другие группы, такие как финансовый отдел и отдел кадров, не видели специализированные элементы каталога. Для публикации всех элементов каталога для нужд разработки и тестирования можно создать службу каталога под названием «Служба для разработки и контроля качества».

Процедура

1. Выберите **Администрирование > Управление каталогом > Службы**.
2. Выберите значок **Создать (+)**.
3. В текстовое поле **Имя** введите **Служба Dev и QE**.
4. В текстовое поле **Описание** введите описание **Служба для разработки и контроля качества элементов каталога приложений для тестирования**.
5. В раскрывающемся меню **Состояние** выберите значение **Активно**.
6. В качестве администратора каталога, который создает службу, можно использовать опцию поиска, чтобы добавить свое имя в качестве владельца.
7. Добавьте настраиваемую группу пользователей «Служба технической поддержки».

Например, добавьте настраиваемую группу пользователей, в которую входят разработчики архитектуры инфраструктуры как услуги и программные архитекторы, чтобы пользователи каталога служб могли к кому-нибудь обратиться в случае возникновения проблем в ходе подготовки элементов каталога.
8. Нажмите кнопку **ОК**.

Результаты

Была создана и запущена служба Dev и QE, однако в ней еще нет каких-либо элементов каталога.

Сценарий: добавление CentOS с MySQL в службу, используемую для разработки или обеспечения качества

Нужно добавить CentOS с элементом каталога MySQL в службу, используемую для разработки и обеспечения качества, от имени администратора арендатора.

Процедура

1. Выберите **Администрирование > Управление каталогом > Службы**.
2. В списке **Службы** выберите службу, используемую для разработки и обеспечения качества, и щелкните **Управление элементами каталога**.
3. Выберите значок **Создать (+)**.
4. Выберите вариант **CentOS с MySQL**.

В этом списке отображаются только опубликованные схемы элементов и компоненты, которые еще не связаны со службой. Если схема элементов не отображается, убедитесь, что она была опубликована и не входит в состав другой службы.

5. Нажмите кнопку **ОК**.
6. Нажмите кнопку **Заккрыть**.

Результаты

CentOS с элементом каталога MySQL опубликован в службе, используемой для разработки и обеспечения качества. Однако элемент не будет отображаться и его никто не сможет запросить, пока пользователям не будет предоставлено право на его использование или на использование службы.

Сценарий: предоставление пользователям прав на запрос элементов службы для разработки и контроля качества в качестве элемента каталога

Администратор арендатора может создать право «Разработка и тестирование», а также и добавить элементы каталога и некоторые соответствующие действия, чтобы пользователи групп разработки и контроля качества могли выполнять запросы MySQL в элементе каталога CentOS, а также выполнять действия на компьютере и в развертывании.

В этом сценарии можно назначить право для службы, так как необходимо, чтобы пользователи имели права на любые будущие элементы каталога, добавленные к этой службе. Также можно предоставить пользователям права на управление подготовленным ими развертыванием, для чего в право можно добавить такие действия, как включение и выключение, создание моментального снимка и удаление развертывания.

Процедура

1. Выберите **Администрирование > Управление каталогом > Права**.
2. Выберите значок **Создать (+)**.
3. Настройка сведений.
 - а) В текстовое поле **Имя** введите **Право «разработка и тестирование»**.
 - б) В раскрывающемся меню **Состояние** выберите **Активно**.
 - в) В раскрывающемся меню **Бизнес-группа** выберите группу **Разработка и тестирование**.

- г) Добавьте одного или нескольких пользователей в области «Пользователи и группы».

Добавьте только себя, если вы не уверены, что схема элементов работает так, как предполагалось. Если она работает правильно, то можно добавить отдельных пользователей и настраиваемые группы пользователей.

- д) Нажмите кнопку **Далее**.

4. Добавьте службу.

Несмотря на то, что элементы каталога CentOS и MySQL добавляются отдельно, добавление службы гарантирует, что любые добавляемые в службу элементы в дальнейшем будут доступны в каталоге служб членам бизнес-группы.

- а) Нажмите значок **Добавить службы** значок (+) рядом с заголовком «Уполномоченные службы».
- б) Выберите **Служба «Разработка и тестирование»**.
- в) Нажмите кнопку **ОК**.

Служба «Разработка и тестирование» добавляется в список «Уполномоченные службы».

5. Добавьте действия.

- а) Нажмите значок **Добавить действия** значок (+) рядом с заголовком «Уполномоченные действия».
- б) Щелкните заголовок столбца «Тип», чтобы отсортировать список по этому столбцу.

Выберите следующие действия в зависимости от типа. Эти действия полезны для пользователей группы разработки и контроля качества при работе с компьютерами для тестирования и являются единственными действиями, которые члены этой бизнес-группы могут выполнять.

Тип	Название действия
Компьютер	Включение
Компьютер	Выключение
Виртуальная машина	Создание моментального снимка
Виртуальная машина	Восстановить из моментального снимка
Среда	Удалить
	Действие удаления развертывания удаляет все развертывание, а не только виртуальную машину.

- в) Нажмите кнопку **ОК**.

В перечень «Уполномоченные действия» будут добавлены пять действий.

6. Щелкните элемент **Готово**.

Результаты

Элемент каталога CentOS с MySQL добавлен в новую службу каталога «Разработка и тестирование», членам бизнес-группы предоставлены права на запрос и управление элементом.

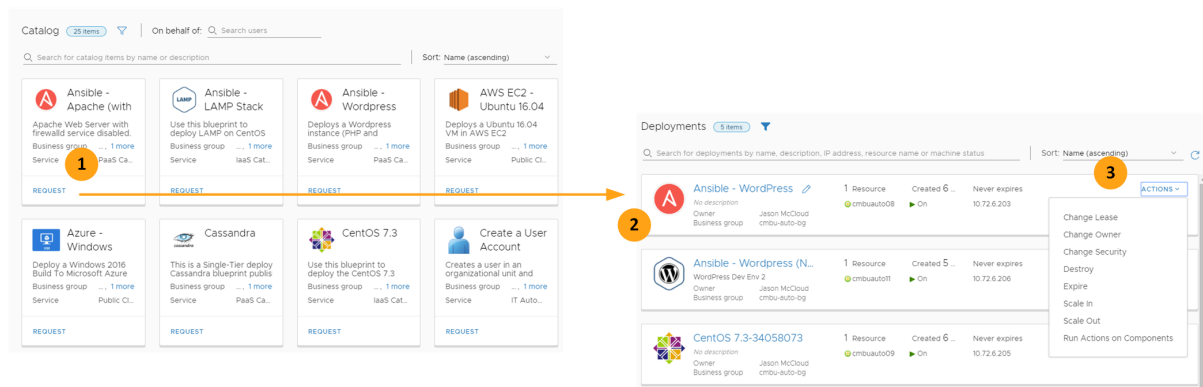
Следующие шаги

После проверки путем подготовки CentOS с элементом каталога MySQL в право можно добавлять пользователей, чтобы сделать элемент каталога доступным для пользователей групп разработки и контроля качества. Если в дальнейшем будет нужно управлять подготовкой ресурсов в среде, то можно создать политики подтверждения для Программное обеспечение компонента MySQL и CentOS на компьютере для тестирования программного обеспечения. См. [Сценарий: создание и применение CentOS с политиками подтверждения MySQL](#).

Использование каталога и управление развертываниями

4

Каталог представляет собой доступные схемы элементов, а развертывания — это подготовленные схемы элементов. Администратор формирует элементы каталога. Эти ресурсы можно запрашивать и затем управлять ими как развертываниями. В качестве одного из средств управления развертываниями для внесения изменений можно выполнять различные действия.



Следующий рабочий процесс начинается с каталога.

1. Пользователь запрашивает элементы каталога. Каталог содержит опубликованные схемы элементов, которым предоставлены права для бизнес-групп, в которые входит данный пользователь.
2. Подготовленные ресурсы управляются, как развертывания. Можно отслеживать процесс подготовки, управлять развертываниями и выполнять действия в отношении развертываний.
3. Используйте действия, чтобы внести изменения в готовое развертывание. Такие действия могут включать: увеличение объема памяти, уменьшение ресурсов ЦП или удаление развертывания, когда оно больше не нужно.

В эту главу входят следующие разделы:

- [Работа с каталогом](#)
- [Работа с развертываниями](#)
- [Работа с папкой "Входящие"](#)

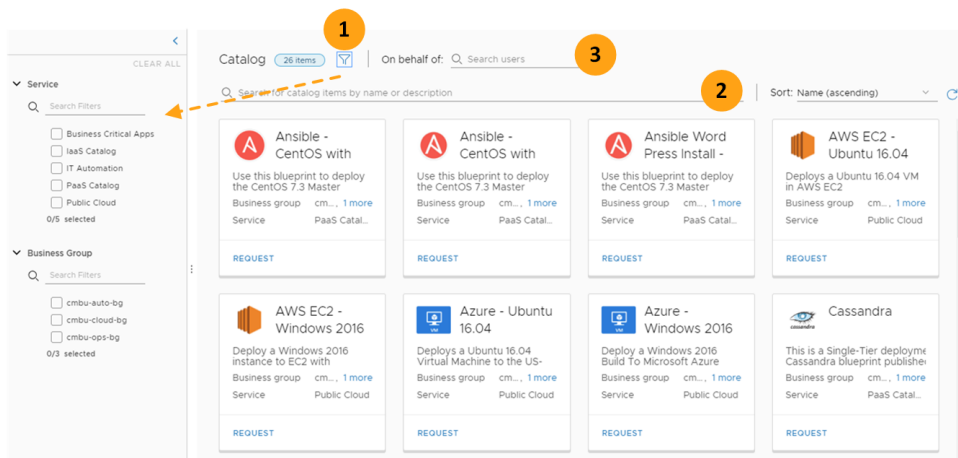
Работа с каталогом

Каталог представляет собой список схем элементов, которые можно развернуть. Архитектор схемы элементов определяет дизайн компонентов, какие настраиваемые параметры можно будет выбрать при запросе элемента и на какой из конечных точек vRealize Automation вашей организации этот элемент будет развернут.

Доступность элементов каталога определяется участием пользователя в одной или нескольких бизнес-группах и правами доступа этих бизнес-групп на подготовку схем элементов.

Поиск элементов каталога

В этом примере показан небольшой каталог. В средах больших предприятий каталог может занимать несколько страниц.

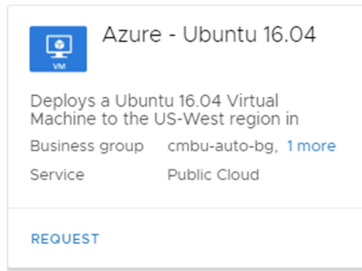


Для поиска схемы элементов, которую нужно развернуть, можно использовать следующие возможности.

1. **Фильтр** полного списка по нужным службам и бизнес-группам.
2. Функции **Поиск** и **Сортировка**, позволяющие найти и организовать элементы каталога.
3. Выберите режим **От имени** пользователя, чтобы ограничить количество элементов каталога, а затем создайте запросите элемент для этого пользователя. Можно развертывать только те схемы элементов, для которых открыт доступ бизнес-группам, в состав которых входит данный пользователь. При выборе имени пользователя список элементов каталога отображается в соответствии с членством в группах. Разрешение "От имени" могут использовать администраторы и диспетчеры бизнес-групп. Его можно предоставить одному или нескольким участникам бизнес-группы при ее настройке. См. раздел [Создание бизнес-группы](#).

Карточки каталога

Карточки каталога представляют собой схемы элементов, которые могут развертывать отдельные компьютеры или все приложение. Они также могут представлять рабочие процессы. Все как услуга, которые подготавливают ресурсы другими способами. Например, путем добавления пользователей в Active Directory.



Информация на карточке включает в себя бизнес-группы, у которых есть права запросить данный элемент каталога, и службу, с которой связан этот элемент.

Отправка запроса в каталог

При отправке запроса в каталог форма запроса для каждой схемы элементов может отличаться. Различия форм настраиваются в конструкторе схем элементов.

Возможности вариации форм зависят от широты прав на настройку запросов. У администратора может быть несколько параметров для выбора при настройке запроса, а может не быть ни одного такого параметра.

Например, архитектор схемы элементов может составить проект схемы, и администратор может выбрать определенное количество процессоров или большую, среднюю или малую ВМ, каждая из которых предусматривает определенное количество процессоров. Или наоборот, схема элементов может быть ограничивающей, запрещая внесение каких-либо изменений перед отправкой запроса.

После того, как запрос успешно подготовлен, развернутая рабочая нагрузка или служба будут готовы для управления.

Необходимые условия

- Для этого необходимо быть членом бизнес-группы, которой предоставлен доступ к одному или нескольким элементам каталога. См. раздел [Создание прав](#).
- Если развертывание проводится от имени другого пользователя, в его бизнес-группе необходимо назначить роль поддержки. См. раздел [Создание бизнес-группы](#).

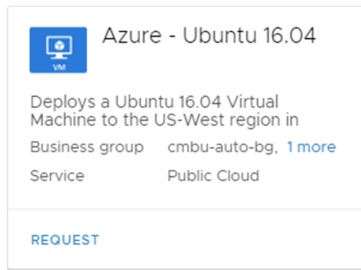
Процедура

1. Щелкните элемент **Каталог**.
2. Если администратор назначает роли поддержки в одной или нескольких бизнес-группах, а затем развертывание выполняется от имени других участников группы, но нужно ввести имя пользователя или настраиваемой группы в поле поиска **От имени**.

Список элементов каталога ограничивается элементами, к которым открыт доступ для бизнес-группы, в которую входит выбранный пользователь или группа.

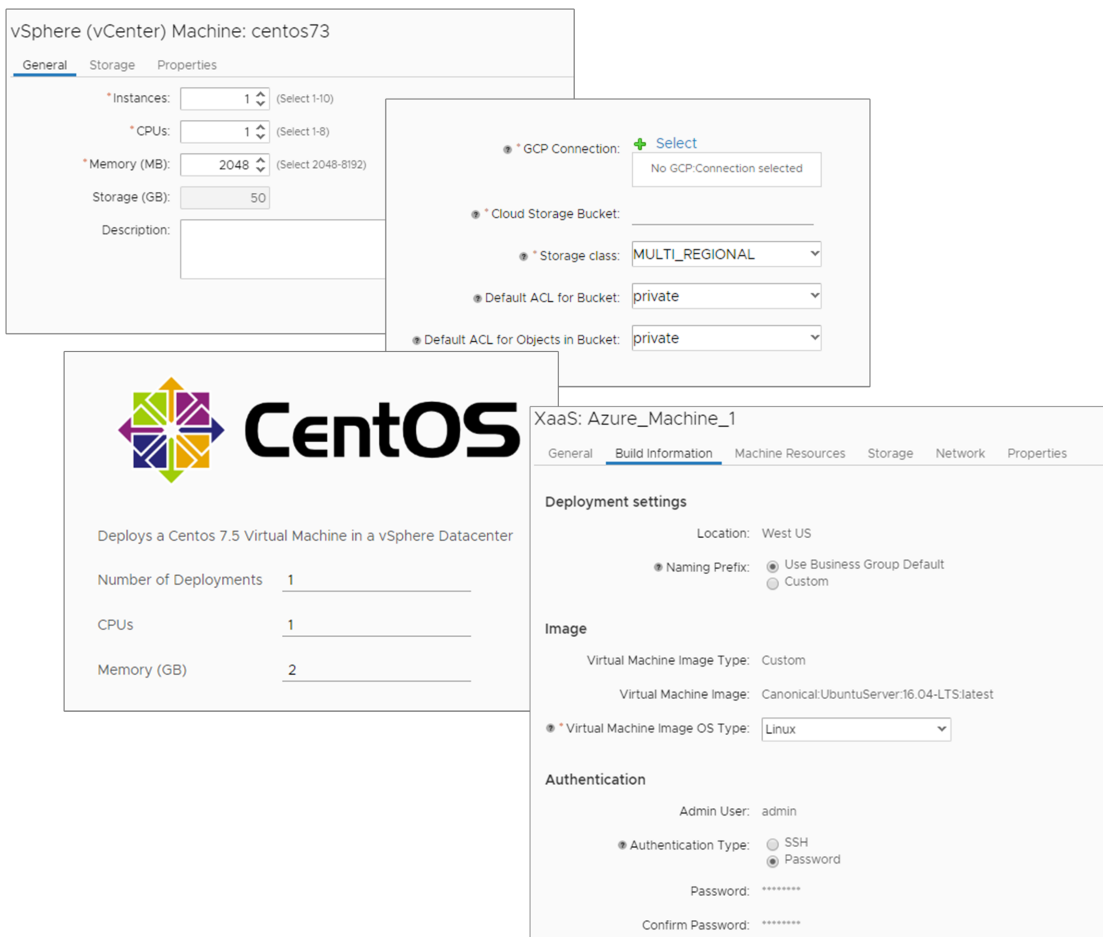
Если пользователь не выбран, запрос отправляется от имени текущего администратора.

- Используйте параметры поиска и сортировки, чтобы найти элемент, который нужно развернуть, и нажмите **Запрос**.



- Если вы участник более чем одной бизнес-группе, которым открыт доступ к данной схеме элементов, выберите бизнес-группу, которую нужно связать с этим развертыванием.
- В форме запроса задайте значения для всех обязательных и дополнительных параметров.

Формы могут изменяться в зависимости от настройки схемы элементов. Ниже приведены примеры, от простых до более сложных с несколькими вкладками.



- Нажмите кнопку **Отправить**.

Результаты

Запрос отправляется для подготовки, и открывается вкладка «Развертывания», на которой можно отслеживать ход выполнения запроса.

Следующие шаги

Проверьте, выполнен ли ваш запрос. См. раздел [Мониторинг запросов на подготовку](#).

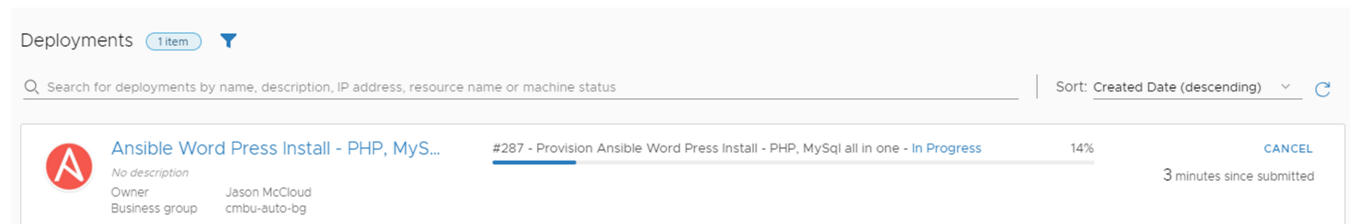
Работа с развертываниями

Развертывания — это подготовленные схемы элементов, запрошенные из каталога. В процессе подготовки можно отслеживать состояние отправленных запросов, вести мониторинг развернутых ресурсов и управлять этими ресурсами с помощью действий.

Мониторинг состояния запросов

Запросы, которые выполняются в данный момент, отображаются на вкладке «Развертывания». Используйте карточки, чтобы отслеживать процесс подготовки до самого завершения.

В случае ошибки процесса подготовки можно просмотреть сообщение об этой ошибке и соответствующие события, чтобы определить, где в запросе произошел сбой, и устранить возникшую проблему. См. раздел [Тестирование и устранение неполадок неудачных запросов на подготовку](#).



Управление развернутыми ресурсами

Можно управлять запросами на вкладке «Развертывания».

Управление включает в себя проверку того, что развертывание запущено. Оно также включает в себя изменение развертывания в соответствии с потребностями пользователя путем увеличения или уменьшения масштаба. Кроме того, пользователю может потребоваться просмотреть сведения о развертывании.

Дополнительные сведения см. в разделе [Управление развернутыми элементами каталога](#).

Мониторинг запросов на подготовку

Развертывания можно использовать для отслеживания хода выполнения запроса, созданного в каталоге. Если ресурс успешно подготовлен, можете управлять этим развернутым ресурсом.

Если вы не видите запрос, который выполняется в настоящее время, это значит, что он не был отправлен или он уже завершен.

Мониторинг запросов

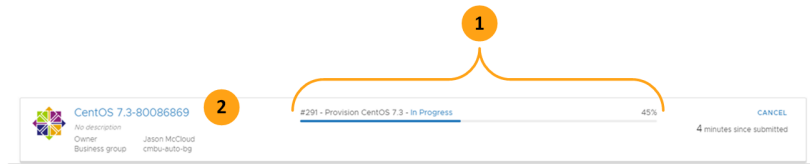
Чтобы отслеживать запросы каталога, выберите **Развертывания**.

Отслеживайте статус запроса в списке развертываний.

- 1 Отслеживайте состояние запроса на карточке развертывания (1). Если это происходит при первом запросе элемента каталога, то в строке состояния ход выполнения отображается без численного значения в процентах. После первого развертывания последующие запросы выдают расчетный процент завершения.

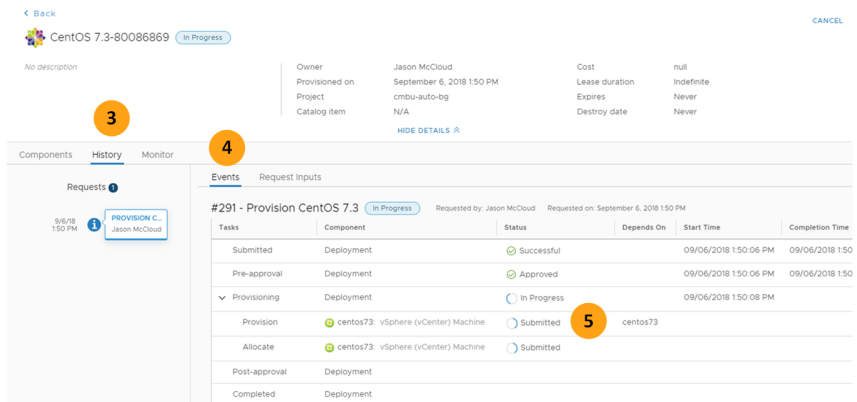
При выполнении действия на развернутом ресурсе в строке состояния показывается состояние выбранного изменения.

- 2 Чтобы просмотреть подробные сведения об идущем процессе, нажмите строку состояния развертывания (1) или имя развертывания (2).



Можно просмотреть параметры подготовки в процессе развертывания.

- 1 Вкладка журнал (3) предоставляет информацию о событиях развертывания, а также входные значения этих событий.
- 2 Вкладка «События» (4) предоставляет подробные сведения о запросе на подготовку.
- 3 Можно просмотреть процесс подготовки (5), чтобы определить, какие компоненты развертываются в настоящее время.



Если запрос не завершит процесс подготовки, см. раздел [Тестирование и устранение неполадок неудачных запросов на подготовку](#).

Отмена выполняемых запросов

Если отменить уже отправленный запрос, то процесс подготовки останавливается, и все развернутые ресурсы откатываются и очищаются.

Если отмена процесса занимает слишком много времени, можно попросить администратора отменить его принудительно. Администратор может отменить запрос, который находится в состоянии отмены. При принудительной отмене запроса откат ресурсов может быть не полным, тогда будет необходимо вручную очистить ресурсы на целевой системе.

Устранение неполадок при сбое запросов каталога

При выполнении запроса элемента каталога по нескольким причинам могут произойти ошибки. Это может произойти из-за сетевого трафика, недостаточных ресурсов конечной точки или ошибок в спецификации схемы элементов. Кроме того, запрос на подготовку может быть выполнен успешно, но развертывание не работает правильно. При помощи vRealize Automation можно изучить развертывание, просмотреть сообщения об ошибках и определить, произошла ли ошибка в среде, где ее можно устранить.

Если у вас нет прав администратора, и ваша роль в vRealize Automation — клиент каталога, то в качестве начального шага устранения неполадок можно использовать следующий рабочий процесс. Для проведения дополнительного более глубокого анализа может потребоваться помощь соответствующего специалиста.

Возможные состояния ошибки

В случае ошибки запроса на подготовку выдается сообщение об одном из следующих состояний.

- **Не выполнено.** Ошибка запроса может произойти по нескольким причинам. Одна причина заключается в том, что процесс подготовки мог не сработать из-за нехватки ресурсов на целевой конечной точке, недостаточного количества ресурсов для выполнения требований схемы элементов или неправильно составленной схемы элементов, которую нужно исправить. Другая причина заключается в том, что запросу требовалось подтверждение от кого-либо в вашей организации, и утверждающий отклонил этот запрос. Также может быть, что не удалось выполнить действие, запущенное пользователем для данного развертывания. Такая ошибка может быть вызвана уже упомянутыми причинами среды развертывания или утверждения запроса.

Чтобы установить причину проблемы, используйте следующий рабочий процесс устранения неполадок. Если можно устранить возникшую проблему, воспользуйтесь действиями **Отменить** и **Отправить повторно**. См. раздел [Пункты меню «Действие» для подготовленных ресурсов](#).

- **Частично успешно.** Запрос может быть выполнен частично, то есть некоторые компоненты были развернуты, но не все действия подготовки были выполнены успешно.

Чтобы определить, какие компоненты были развернуты только частично, и установить причину проблемы, используйте следующий рабочий процесс устранения неполадок. Если можно устранить возникшую проблему, воспользуйтесь действиями **Отменить** и, возможно, **Отправить повторно**. См. [Пункты меню «Действие» для подготовленных ресурсов](#) и [Как работает действие «Возобновить»](#).

Рабочий процесс устранения неполадок для клиентов каталога

Этот рабочий процесс можно использовать как первый этап анализа неудачного развертывания. Если ваш анализ обнаруживает, что ошибка была связана с временной проблемой среды развертывания, можно устранить эту проблему и повторно отправить запрос. Если проблема связана со спецификацией запроса, то, возможно, потребуется связаться с разработчиком данной схемы элементов.

Таблица 4-1. Как начать устранение неполадок

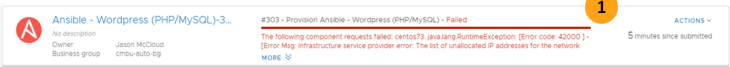
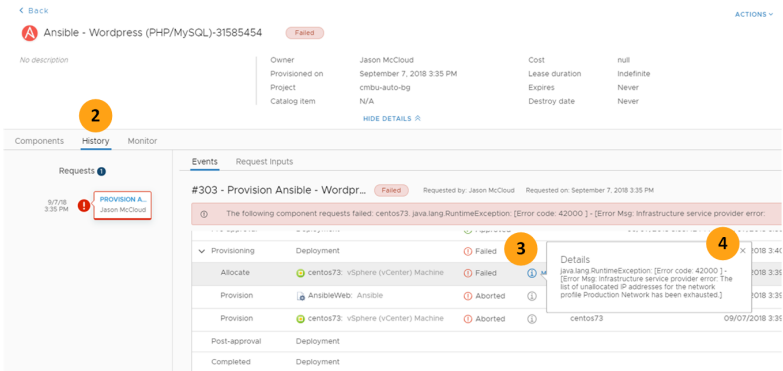
Рабочий процесс	Этап устранения неполадок	Пример
1	На вкладке Развертывания неудачные развертывания указываются в строке состояния. Данная карточка включает в себя последнее сообщение об ошибке. Для получения дополнительной информации нажмите имя развертывания или индикатор хода выполнения.	
2	На вкладке Журнал сведений о развертывании можно использовать рабочий процесс событий, чтобы определить, где в процессе подготовки произошла ошибка. Этот рабочий процесс также полезен, если выполнялось действие для развертывания, но произошла ошибка.	

Таблица 4-1. Как начать устранение неполадок (продолжение)

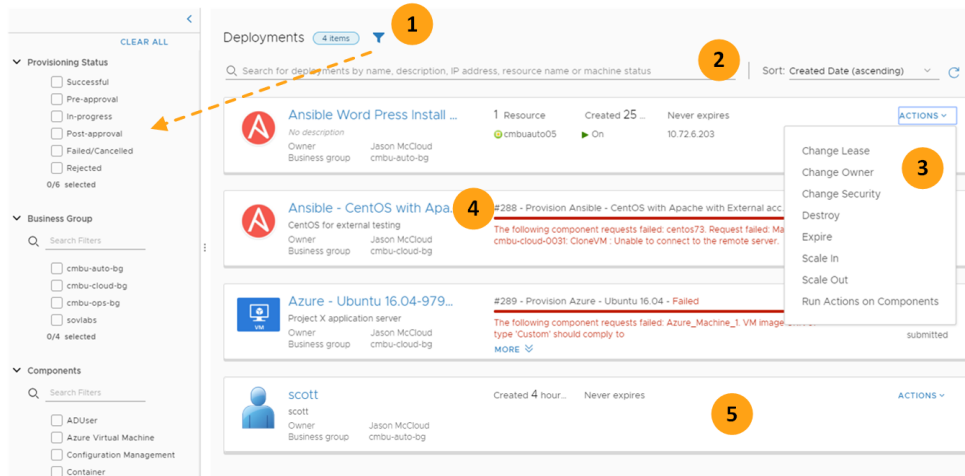
Рабочий процесс	Этап устранения неполадок	Пример
3	Состояние ошибки указывает, где произошел сбой рабочего процесса.	
4	<p>Данная информация предоставляет собой более подробное сообщение об ошибке.</p> <p>Если этих сведений в табличке с информацией недостаточно для определения причин проблемы и их устранения, можно дополнительно проанализировать журналы событий.</p> <p>Чтобы просмотреть журналы событий, необходимо иметь необходимые права пользователя.</p> <p>Разработчик схемы элементов и администратор могут оказать дополнительную помощь в устранении неполадок. См. раздел Тестирование и устранение неполадок неудачных запросов на подготовку.</p>	

Управление развернутыми элементами каталога

Владелец развертывания или администратор, который помогает другим пользователям, могут использовать сведения о развертывании для управления жизненным циклом развернутых элементов. Сведения о развертывании содержат актуальную информацию о каждом компоненте и используют журнал для отслеживания последующих изменений. При работе с развертываниями можно изменять развернутые элементы, используя действия. Некоторые параметры можно изменить, не используя действия.

Управление развертываниями с помощью карточек

Список карточек развертывания дает общее представление о развертываниях. Были они успешно выполнены? Запущены ли они?



Используйте следующие возможности для поиска развернутых ресурсов и управления ими в среде vRealize Automation.

1. Примените **фильтр** к данному списку по текущему состоянию запроса, по бизнес-группе, для которой сделано развертывание, по включенным компонентам, по владельцу или по датам подготовки или срока действия. Фильтры по состоянию инициализации и номеру запроса применяются только к процессу начальной подготовки. К возможным последующим действиям они не применимы. Другие фильтры применяются к развертыванию в целом.
2. Выполните **поиск** и **сортировку**, чтобы находить и организовывать нужные развертывания.
3. Для управления развертыванием нажмите **Действия**. Это запускает настроенные действия уровня развертывания. Чтобы выполнить действия с отдельными компонентами, нужно открыть подробные сведения о развертывании. Это могут быть стандартные действия, настроенные для схем элементов, либо настраиваемые действия для ресурсов Все как услуга, созданные и назначенные пользователем для схемы элементов Все как услуга. Дополнительные сведения о стандартных действиях см. в разделе [Выполнение действий с развернутыми ресурсами](#).
4. Для просмотра и управления подробными сведениями о развертывании, включая события предоставления, журналы и действия на уровне компонентов, нажмите имя нужного развертывания. Первые три — это запросы на начальную подготовку для стандартных схем элементов.
5. Можно также управлять запросами на развертывания Все как услуга, которые запускают рабочие процессы. Рабочие процессы могут привести к запуску ресурсов или рабочих процессов во внешних системах. В этом примере элемент Все как услуга добавил пользователя к домену Active Directory.

Управление развертыванием с помощью подробных сведений о развертывании

Сведения о развертывании позволяют управлять следующими данными.

- **Сведения.** Основные сведения, содержащиеся на данной карточке. Также можно изменять имя и описание развертывания и выполнять действия на уровне развертывания.
- **Вкладка «Компоненты».** Полная конфигурация каждого компонента. Можно выполнять действия на уровне компонентов.

- Вкладка «Журнал». Полный журнал изменений, внесенных в данное развертывание. Содержит также дополнительные сведения о размещении и о входных значениях, введенных при каждом изменении.
- **Вкладка «Мониторинг».** При интеграции с vRealize Operations Manager предоставляются показатели мониторинга и оповещения для развертывания и компонентов.
- **Действия.** Используя эти сведения, можно выполнять действия на уровне развертывания или действия на уровне компонентов.

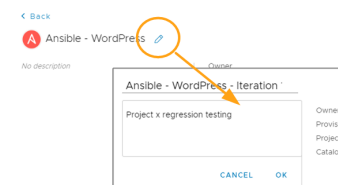
Использование сведений о развертывании

Сведения о развертывании предоставляют более полные сведения в дополнение к базовой информации на карточке. Здесь также можно изменять имя и описание развертывания и выполнять действия уровня развертывания и компонентов.

Просмотрите базовые сведения о развертывании, включая схему элементов, на основании которой оно было развернуто, а также стоимость.

Изменение имени развертывания

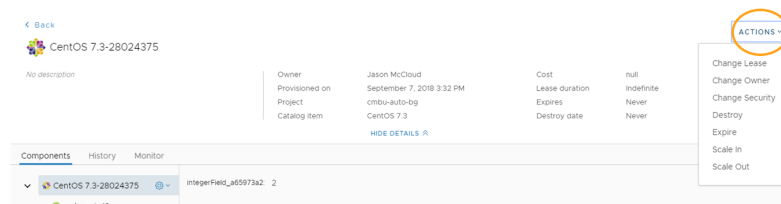
Развертывание получает имя на основании имени схемы элементов. Это имя не всегда удобно для работы с развертыванием. Можно изменить имя и описание, чтобы они отвечали требованиям пользователей.



1. Выделите имя и нажмите значок карандаша.
2. Измените имя и описание нужным образом.

Выполнение действий на уровне развертывания

Действия на уровне развертывания могут включать только изменения, применимые ко всему развертыванию. Набор доступных действий зависит от прав бизнес-группы пользователя на их использование.

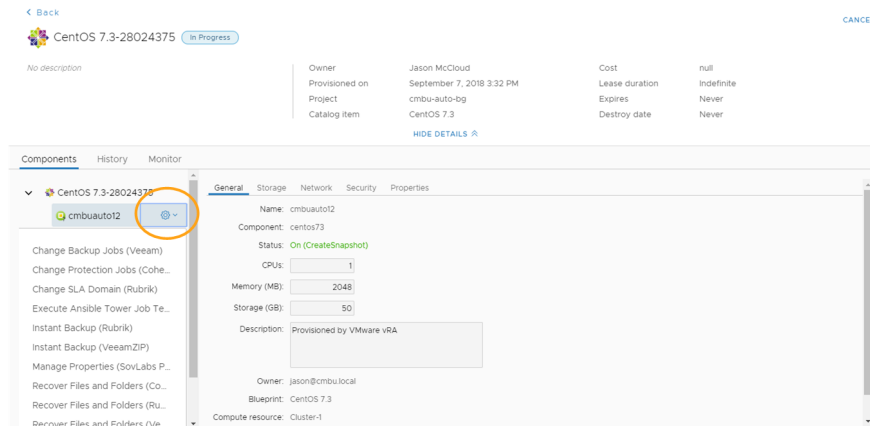


Компоненты развертывания

На вкладке "Компоненты" в подробных сведениях о развертывании приведены все параметры конфигурации для всех компонентов развертывания. Там можно просмотреть, как настроены компьютеры и сети. Можно также выполнять там действия на уровне компонентов для изменения конфигурации.

Просмотр сведений о компоненте позволяет оценить предоставленное развертывание и помогает при устранении неполадок с экземпляром.

Все изменения, сделанные с помощью действий, отображаются в этих сведениях.



Выполнение действий на уровне компонентов

Действия на уровне компонентов различаются в зависимости от компонента. Набор доступных действий зависит от прав на их использование, предоставленных вашей бизнес-группе. Если администратор не предоставил пользователю права выполнять действия, на его экране не будут отображаться значок шестеренки и список действий.

Журнал развертывания

Вкладка "Журнал" в сведениях о развертывания содержит все записи журнала развертывания с этапа начальной подготовки. Он включает все изменения, внесенные с помощью одного или нескольких действий. Полный журнал подготовки позволяет узнать, когда что-либо изменялось и какие значения параметров были введены.

Просмотрите подробный журнал, если необходимо определить, изменилось ли что-нибудь или если нужно устранить проблемы с экземпляром. Журнал также можно использовать для устранения неполадок в случае неудачного развертывания. См. раздел [Тестирование и устранение неполадок неудачных запросов на подготовку](#).

CentOS 7.3-28024375 In Progress

No description

Owner: Jason McCloud
Provisioned on: September 7, 2018 3:32 PM
Project: cmbu-auto-big
Catalog item: CentOS 7.3

Cost: null
Lease duration: Indefinite
Expires: Never
Destroy date: Never

Components **History** **Monitor**

Requests

- 9/10/18 4:01 PM **CREATE SNA...** Jason McCloud
- 9/10/18 3:42 PM **REBOOT CMB...** Jason McCloud
- 9/7/18 3:32 PM **PROVISION C...** Jason McCloud

Events **Request Inputs**

#316 - Create Snapshot cmbuauto... In Progress Requested by: Jason McCloud Requested on: September 10, 2018 4:01 PM

Tasks	Component	Status	Depends On	Start Time	Completion Time
Submitted	Deployment	Successful		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Pre-approval	Deployment	Approved		09/10/2018 4:01:09 PM	09/10/2018 4:01:09 PM
Create Snapshot	Deployment	In Progress		09/10/2018 4:01:11 PM	
Post-approval	Deployment				
Completed	Deployment				

Request Inputs

Machine Name: cmbuauto12
Snapshot name: cmbuauto12 (Monday, September 10, 2018 10:01:02 PM +00:00)
Snapshot description:
Include memory?: No

Мониторинг развертывания при помощи vRealize Operations Manager

vRealize Automation может отображать данные vRealize Operations Manager о развертываниях.

- Оповещения уровня развертывания
- Показатели уровня компьютера

Просмотр отфильтрованного набора оповещений и показателей непосредственно в vRealize Automation избавляет от необходимости открывать и выполнять поиск в vRealize Operations Manager. Хотя контекстный запуск в vRealize Operations Manager невозможен, можно в любой момент войти в систему и использовать vRealize Operations Manager для получения необходимых дополнительных данных.

Включение данных vRealize Operations Manager

Чтобы в vRealize Automation отображались данные vRealize Operations Manager, нужно сначала настроить параметры и адаптеры.

Настройте необходимые действия в vRealize Operations Manager и vRealize Automation.

Необходимые условия

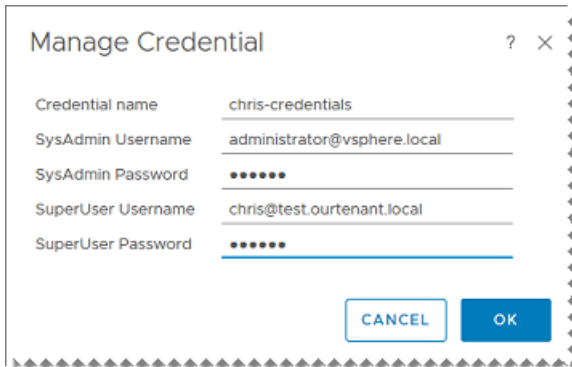
Проверьте, что используется vRealize Operations Manager версии 6 или более новой.

Процедура

1. В vRealize Operations Manager перейдите в меню **Администрирование > Решения**.
2. В разделе **Решения** проверьте, установлено ли **решение vRealize Automation** и поступают ли в него данные.
 - а) Выберите решение vRealize Automation.
 - б) На панели инструментов над этим решением щелкните значок настройки в виде шестеренки.

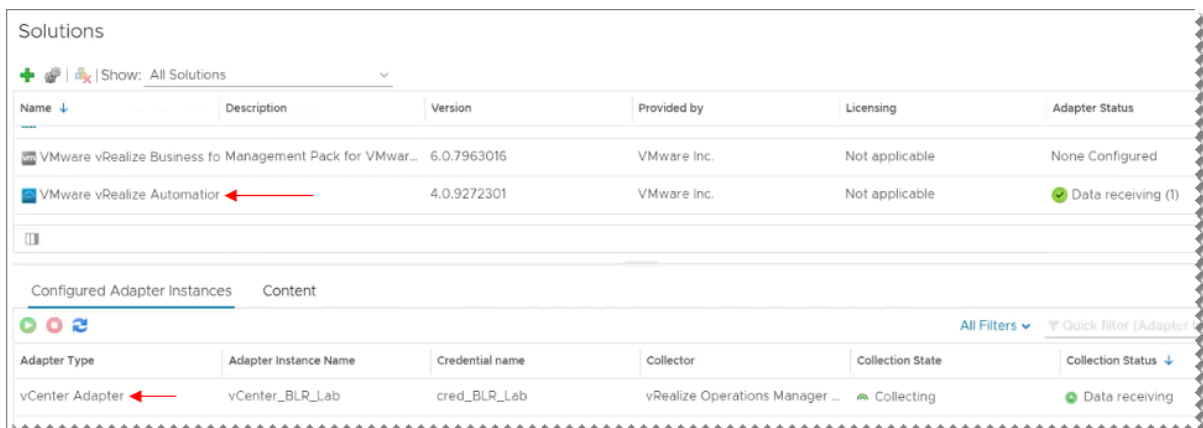
- в) На странице **Параметры экземпляра** перейдите к разделу **Учетных данных** и нажмите зеленый значок «+», чтобы добавить учетные данные.

Название учетных данных	Описание набора учетных данных
SysAdmin	Имя пользователя и пароль администратора арендатора vRealize Automation по умолчанию, обычно administrator@vsphere.local
SuperUser	Имя пользователя и пароль для доступа к учетной записи с расширенными правами для рабочего арендатора vRealize Automation



- г) Сохраните учетные данные и проверьте возможность подключения с ними.
3. В разделе **Настроенные экземпляры адаптера** убедитесь, что настроен **адаптер vCenter** для конечной точки vSphere, в которой выполняет подготовку vRealize Automation, и что на адаптер поступают данные.

Рис. 4-1. Решения и адаптеры vRealize Operations Manager



4. В vRealize Operations Manager перейдите в меню: **Оповещения > Параметры оповещений**.

5. Убедитесь, что определения оповещений и симптомов генерируют правильные оповещения vRealize Automation.

Большинство пользователей vRealize Automation просто хотят убедиться, что развертывание будет работоспособным. Дополнительные оповещения с уровня виртуальной машины могут создавать очень большой поток данных и содержать сведения, которыми нельзя управлять с помощью vRealize Automation.

Для **оповещений vRealize Automation** общее развертывание выступает как родительский объект. Виртуальные машины в этом развертывании будут дочерними объектами. По умолчанию уровнем оповещения будет родительский уровень развертывания.

Можно свободно использовать vRealize Operations Manager для создания оповещений уровня развертывания с информацией о дополнительных конкретных симптомах. Например может потребоваться показывать для развертывания все проблемы SQL Server.

6. В vRealize Automation перейдите в меню: **Администрирование > Реорганизация > Источник показателей**.
7. Выберите **Конечная точка vRealize Operations Manager**.
8. Введите URL-адрес vRealize Operations Manager `https://master-node-FQDN-or-IP/suite-api/` и учетные данные пользователя vRealize Operations Manager с правами администратора.

Примечание При наличии нескольких источников проверки подлинности введите имя пользователя в формате `user@domain@source`, где `@source` — это источник импорта LDAP в vRealize Operations Manager. Для учетной записи пользователя требуется как минимум роль `ReadOnly` (только чтение) и права объекта для адаптера vCenter и облачного экземпляра vCenter Server.

9. Проверьте это подключение и сохраните его.
10. Нажмите **Развертывания**, выберите нужное развертывание и убедитесь, что открывается вкладка мониторинга.

Вкладка «Мониторинг» отображается только при выборе vRealize Operations Manager в качестве источника показателей.

Оповещения, предоставляемые vRealize Operations Manager

При включенном режиме мониторинга vRealize Automation загружает оповещения vRealize Operations Manager о соответствующих развертываниях.

Для доступа к средству мониторинга нажмите нужное развертывание и откройте вкладку **Мониторинг**. Если такая вкладка отсутствует, см. раздел [Включение данных vRealize Operations Manager](#).

Чтобы просмотреть оповещения, выделите имя данного развертывания в верхней части дерева компонентов в левой части окна.

- В оповещениях можно просмотреть уровень важности и текст.
- Чтобы легче находить нужные оповещения, используйте фильтрацию и сортировку данных в столбцах.
- Отображаются только оповещения о работоспособности. Другие типы оповещений, например эффективность или риск, не поддерживаются.

Components	History	Monitor
<div> <div>VC-65-DND Deployme...</div> <div>VC-65-DND</div> </div>		
Alerts	Total VMs	Total CPUs
5	1	4
Total Memory	Total Storage	
16384 MB	270 GB	
Criticality	Alert	Created On
Warning	One or more VM's of Deployment is not having memory ballooning	7/26/18, 7:47 PM
Critical	One or more VM's Disk usage is above 70%	7/26/18, 7:47 PM
Immediate	One or more VM is having CPU in idle state	7/26/18, 7:47 PM
Critical	Most deployment resources have health issues	7/26/18, 7:47 PM
Critical	One or more VM of Deployment is running out of Guest file system disk space	7/26/18, 7:47 PM

Показатели, предоставляемые vRealize Operations Manager

При включенном режиме мониторинга vRealize Automation получает показатели vRealize Operations Manager о развертываниях.

Для доступа к средству мониторинга нажмите нужное развертывание и откройте вкладку **Мониторинг**. Если такая вкладка отсутствует, см. раздел [Включение данных vRealize Operations Manager](#).

Чтобы просмотреть показатели, разверните дерево компонентов в левой части экрана и выберите нужную виртуальную машину.

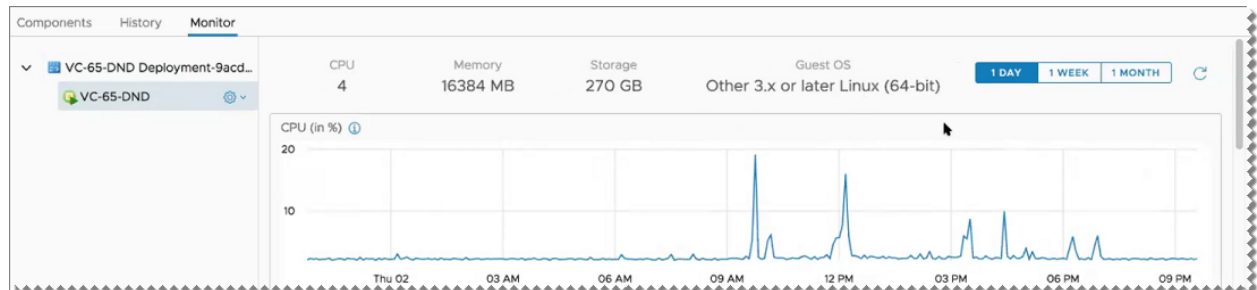
- Показатели не кэшируются. Они передаются непосредственно из vRealize Operations Manager, и этот процесс может занять несколько минут.
- Отображаются только показатели виртуальной машины. Показатели других компонентов, например vCloud Director, программного обеспечения или любого ресурса как услуги не поддерживаются.
- Отображаются только показатели виртуальной машины vSphere. Другие поставщики облачных служб, например AWS или Azure, не поддерживаются.

Показатели отображаются как графики на временной шкале, на которых показаны минимальные и максимальные значения для следующих измеряемых свойств.

- ЦП
- Память

- Число операций ввода-вывода системы хранения
- Пропускная способность сети в Мбит/с

Чтобы отобразить имя определенного показателя, нажмите синий значок сведений в верхнем левом углу временной шкалы.



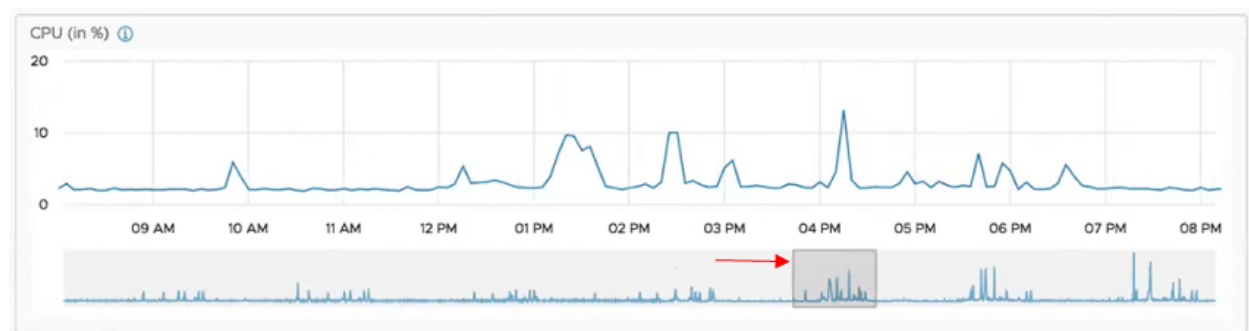
Реакция на данные, предоставляемые vRealize Operations Manager

Когда показатели, предоставляемые vRealize Operations Manager, указывают на какую-либо проблему, можно прямо в vRealize Automation предпринять некоторые корректирующие действия.

Для просмотра показателей, предоставляемых vRealize Operations Manager, нажмите нужное развертывание и откройте вкладку **Мониторинг**. Если такая вкладка отсутствует, см. раздел [Включение данных vRealize Operations Manager](#).

Поиск проблем

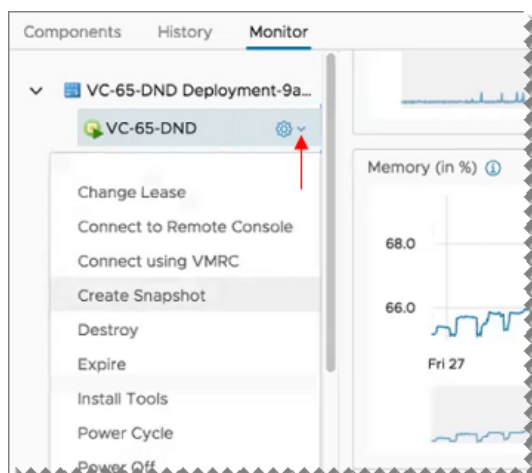
Предоставляются показатели за последний день, неделю и месяц. Чтобы подробнее увидеть нужный интервал времени, выберите соответствующую область в нижней затененной части графика какого-либо показателя:



Внесение изменений

При возникновении проблемы можно предпринять некоторые корректирующие действия прямо в том же интерфейсе.

Например, если на графике использования памяти видны регулярные пики, можно увеличить объем памяти. В дереве компонентов в левой части экрана нажмите раскрывающееся меню для данной виртуальной машины и выберите нужный пункт в контекстном меню, чтобы выполнить действие по обслуживанию или изменить конфигурацию.



Выполнение действий с развернутыми ресурсами

Действия, которые можно выполнять с развернутым ресурсом, зависят от типа ресурса, параметров действия, способа доступа к нему подготовленных элементов, а также рабочего состояния элемента.

Настроенные действия, доступные для развертывания или для компонента развертывания, отображаются в меню **Действия** при выборе определенного развертывания или компонента.

Список доступных действий определяется правами бизнес-группы пользователя для данного развертывания и компонента, а также типом компьютера данного компонента. Доступность действия зависит от типа или состояния компьютера.

Если элемент подготовлен на основе схемы элементов Все как услуга, действия ресурсов нужно создавать и публиковать в службе, использованной для подготовки элемента. Кроме того, права на их использование нужно также назначать в этой службе. Список доступных действий зависит от типа и текущего состояния элемента.

В частности, для элемента, подготовленного в качестве компьютера Инфраструктура как услуга, могут быть доступны действия ресурсов Все как услуга, если действия сопоставляются с элементом.

Пункты меню «Действие» для подготовленных ресурсов

Действия — это изменения, производимые с подготовленными ресурсами. Действия vRealize Automation используются для управления жизненным циклом ресурсов.

Набор команд в меню **Действие** зависит от того, как диспетчер бизнес-группы или администратор арендатора настроил право, распространяющееся на ресурс, с которым выполняются действия. Доступность элемента меню зависит также от типа ресурса, а также от рабочего состояния элемента.

В один момент времени можно запускать не более одного действия. Чтобы выполнить второе действие с данным ресурсом, дождитесь завершения первого.

Таблица 4-2. Команды в меню «Действие»

Действие	Тип ресурса	Описание
Связать плавающий IP-адрес	Компьютер (OpenStack)	Связывание плавающего IP-адреса с компьютером OpenStack.
Отмена	Компьютер	<p>Отмена выполняющегося действия перенастройки.</p> <p>Пользователи могут отменить только действия, позволяющие выполнить откат к предыдущему состоянию.</p> <p>Если действие не поддерживает откат к предыдущему состоянию (например, «выключение»), то запрос может отменить только пользователь с привилегиями администратора арендатора.</p>
Изменить аренду	Развертывание и компьютер	Изменение количества оставшихся дней аренды для конкретного компьютера или всех ресурсов, включенных в развертывание. Если не указывать значение, аренда станет бессрочной.
Изменить правила NAT	Сеть NAT	Добавьте новые правила переадресации портов NAT, измените или удалите существующие правила.
Изменить владельца	Развертывание	<p>Изменение владельца развертывания и всех содержащихся в нем ресурсов. Только диспетчеры бизнес-групп и пользователи службы поддержки могут менять право собственности на развертывание.</p> <p>Компьютер должен быть во включенном, выключенном или активном состоянии при инициировании смены владельца. В противном случае данное действие завершится сбоем с таким сообщением:</p> <p>Это действие недопустимо для компьютера.</p>
Изменить параметры безопасности	Развертывание	<p>Можно добавить или удалить существующие группы безопасности NSX и теги безопасности. Также можно удалить группы безопасности по требованию.</p> <p>Дополнительные сведения см. в разделе Добавление и удаление элементов системы безопасности в развертывании.</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Подключить с помощью VMRC	Компьютер	<p>Подключение к виртуальной машине с помощью приложения VMRC 8.x.</p> <p>Чтобы использовать это действие, приложение VMRC необходимо установить на локальную систему пользователя каталога служб, начавшего выполнение данного действия.</p> <p>Инструкции по установке и инструкции пользователя см. в документации по VMware Remote Console. Сведения о загрузке см. в разделе Загрузка VMware Remote Console.</p> <p>VMRC 8.x заменяет предыдущую консоль VMware Remote Console.</p>
Подключение к удаленной консоли	Компьютер	<p>Подключение к выбранному компьютеру с помощью VMware Remote Console.</p> <p>Консоль виртуальной машины появляется в браузере. VMRC 8.x заменяет консоль VMware Remote Console.</p>
Подключиться с помощью билета консоли	Компьютер (OpenStack и KVM)	Подключение к виртуальной машине OpenStack или KVM с помощью билета консоли для подключения к VMware Remote Console.
Подключиться с помощью ICA	Компьютер (Citrix)	Подключение к компьютеру Citrix с помощью Independent Computing Architecture.
Подключиться с помощью RDP	Компьютер	Подключение к компьютеру с помощью Microsoft Remote Desktop Protocol.
Подключиться с помощью SSH	Компьютер	<p>Подключение к выбранному компьютеру с помощью SSH.</p> <p>Для включения параметра Подключиться с помощью SSH в браузере должен быть установлен подключаемый модуль, который поддерживает SSH, например терминал-клиент FireSSH SSH для Mozilla Firefox и Google Chrome. Если имеется такой подключаемый модуль, при выборе параметра Подключиться с помощью SSH отображается консоль SSH и запрашиваются учетные данные администратора.</p> <p>Чтобы использовать это действие, в компоненте компьютера схемы элементов, в группе свойств или отдельном настраиваемом свойстве должно быть задано настраиваемое свойство Machine.SSH.</p>
Подключиться с помощью виртуального рабочего стола	Компьютер	Подключение к выбранному компьютеру с помощью виртуального рабочего стола Microsoft.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Создание моментального снимка	Виртуальная машина	Создайте моментальный снимок виртуальной машины. Если разрешается создать только два моментальных снимка и они уже созданы, эта команда станет доступной только после удаления одного моментального снимка.
Удалить моментальный снимок	Виртуальная машина	Удаление моментального снимка виртуальной машины.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Удалить	Развертывание, компьютер и группа безопасности по требованию	<p>Немедленное удаление подготовленного ресурса. Не рекомендуется удалять компоненты развертывания (за исключением Все как услуга). Используйте действие по уменьшению масштаба для снижения количества компьютеров в развертывании или удаления всего развертывания.</p> <p>Это действие необходимо выполнить для удаления ресурсов Все как услуга, даже если они являются частью удаляемого развертывания. Прочие ресурсы удаляются по истечении срока действия аренды или периода архивного хранения.</p> <p>Действие «Удалить» недоступно для следующих развертываний:</p> <ul style="list-style-type: none"> ■ развертывания физических компьютеров; ■ развертывания с существующей сетью NSX или существующим ресурсом безопасности NSX; ■ развертывания с ресурсом подсистемы балансировки нагрузки по требованию NSX. <p>Так как подсистема балансировки нагрузки NSX относится к среде NSX Edge, при удалении решения NSX Edge подсистема балансировки нагрузки также удаляется, а ресурсы высвобождаются. При удалении уровня компьютеров, для которых выполняется балансировка нагрузки, уровень удаляется из пула подсистемы балансировки нагрузки на соответствующем экземпляре NSX Edge.</p> <p>Примечание В ответ на действие «Удалить» может появиться сообщение об успешном выполнении даже в том случае, если развертывание компьютера не удалено из конечной точки. Например, если компьютер vSphere находится в хранилище данных, отличном от vSAN, и его файл VMX содержит поврежденные или недопустимые данные. Даже если сообщение об удалении указывает на успешное выполнение действия, можно обратиться к журналу запросов для получения дополнительной информации. При принудительном удалении компьютера в этом состоянии он может остаться запущенным в конечной точке и вызвать конфликты, связанные с IP-адресами. Если проблема устранена в конечной точке (за пределами vRealize Automation), можно повторить действие «Удалить».</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
		<p>Администраторы бизнес-групп могут принудительно удалить развертывание после сбоя запроса на удаление. В случае принудительного удаления vRealize Automation игнорирует отказы в удалении отдельных ресурсов во время удаления развертывания. Дополнительные сведения о принудительном удалении см. в разделе Принудительное удаление развертывания после неудачного запроса на удаление.</p> <hr/> <p>Примечание Хранилище и память, назначенные подготовленному компьютеру путем резервирования, освобождаются, когда компьютер, которому они назначены, удаляется в vRealize Automation. Хранилище и память не освобождаются, если компьютер удален в vCenter Server.</p> <hr/> <p>При удалении развертывания, содержащего компьютер Amazon, можно за один раз удалить несколько томов EBS в зависимости от того, как был настроен параметр Удалить тома в схеме элементов. Дополнительные сведения см. в разделе Настройки компонентов компьютера Amazon.</p> <hr/> <p>При уничтожении развертывания, в котором содержится компонент компьютера Amazon, все тома EBS, добавленные на компьютер во время его жизненного цикла, отделяются, а не уничтожаются. vRealize Automation не предоставляет параметр для уничтожения объемов EBS.</p> <hr/>
Отменить связь плавающего IP-адреса	Компьютер (OpenStack)	Удаление плавающего IP-адреса с компьютера Openstack.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Заккрыть	Не указан тип ресурса. Не удалось выполнить запрос на начальную подготовку или указанное действие.	<p>Выполняется отклонение запроса с ошибкой.</p> <p>Выполняется отмена выполняемого запроса.</p> <ul style="list-style-type: none"> ■ Если отклоненный запрос — это запрос на развертывание, отклонение удаляет развертывание, завершившееся сбоем, из списка развертываний. ■ Если отклоненный запрос — это действие, отклонение удаляет из карточки запрос на действие, завершившийся сбоем, и оставляет развертывание в предыдущем состоянии. <p>Необходимо отклонить запрос на действие, завершившийся сбоем, чтобы видеть выполнение других действий в связанном развертывании. Также необходимо отклонить действия, завершившиеся сбоем, чтобы пользователи развертывания могли видеть журнал компьютера.</p> <p>Нельзя запустить команду «отклонить» для запросов, отправленных API-интерфейсом, и она не блокирует действия, отправленные API-интерфейсом.</p> <p>Это действие доступно для всех невыполненных запросов начальной подготовки. Какие-либо права не требуются.</p>
Выполнить перенастройку	Компьютер	Сразу же перенастройте компьютер или запланируйте действие перенастройки на более позднее время.
Срок действия	Развертывание и компьютер	Завершить развертывание или аренду компьютера для всех ресурсов, включенных в развертывание.
Экспорт сертификата	Компьютер	Экспорт сертификата из облачного компьютера.
Напомнить об окончании срока действия	Компьютер	Загрузка файла событий календаря для текущего срока действия аренды.
Установить VMware Tools	Компьютер	Установить VMware Tools на виртуальной машине vSphere
Цикл электропитания	Компьютер	Выключение компьютера с последующим повторным включением.
Выключение	Компьютер	Компьютер выключается без завершения работы гостевой операционной системы.
Включение	Компьютер	Включите компьютер. Если работа компьютера была приостановлена, нормальное функционирование будет возобновлено с той точки, в которой оно было приостановлено.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Перезагрузка	Компьютер	Перезагрузка гостевой операционной системы на виртуальной машине vSphere. Чтобы использовать это действие, необходимо установить VMware Tools на компьютере.
Перенастроить	Компьютер	<p>Диспетчер бизнес-групп, пользователь поддержки или владелец компьютера могут выполнять следующие операции по изменению настроек выбранной виртуальной машины vSphere:</p> <ul style="list-style-type: none"> ■ изменить описание; ■ изменить параметры ЦП, памяти, сети и диска; ■ Добавление, редактирование и удаление пользовательских свойств и групп свойств ■ Добавить, изменить, изменить порядок или удалить сетевой адаптер для правил переадресации портов NAT ■ перенастроить выключение. ■ изменить владельца компьютера (только для диспетчеров бизнес-групп и пользователей службы поддержки) <p>Нельзя изменить политику резервирования места для хранения, если при этом может измениться профиль хранения на диске.</p> <p>Дополнительные сведения см. в разделе Задание параметров перенастройки компьютера и рекомендации по перенастройке.</p> <p>Если выбран параметр Распространять обновления на существующие развертывания на странице Настройки схем элементов в исходной схеме элементов, любое увеличение или расширение минимальных и максимальных параметров ЦП, памяти или хранилища в схеме элементов автоматически отражается в активных развертываниях, подготовленных на основе этой схемы элементов. Дополнительные сведения см. в разделе Настройки свойств схемы элементов.</p> <p>Не работайте с объектами NSX под управлением vRealize Automation за пределами vRealize Automation. Например, если изменить порт-участник развернутой подсистемы балансировки нагрузки в NSX, а не в vRealize Automation, то сбор данных NSX прерывается. Операции горизонтального и вертикального масштабирования также выполняются с непредсказуемым результатом.</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Перенастроить	Подсистема балансировки нагрузки	<p>Уполномоченный владелец компьютера, пользователь поддержки, администратор арендатора или диспетчер бизнес-групп может изменить любой из параметров на виртуальном сервере, а также добавить или удалить виртуальные серверы в подсистеме балансировки нагрузки NSX:</p> <p>Дополнительные сведения см. в разделе Перенастройка подсистемы балансировки нагрузки в развертывании.</p> <p>Сведения о параметрах виртуального сервера в подсистеме балансировки нагрузки см. в разделе Добавление компонента «Подсистема балансировки нагрузки по требованию».</p> <p>Не работайте с объектами NSX под управлением vRealize Automation за пределами vRealize Automation. Например, если изменить порт-участник развернутой подсистемы балансировки нагрузки в NSX, а не в vRealize Automation, то сбор данных NSX прерывается. Операции горизонтального и вертикального масштабирования также выполняются с непредсказуемым результатом.</p>
Регистрация VDI	Виртуальная машина (XenServer)	Регистрация образа виртуального диска для элементов XenServer.
Удалить из каталога	Развертывания	Удаление подготовленных ресурсов XaaS из каталога. Эту операцию можно выполнить в отношении существующих объектов и объектов, которые больше не находятся в иерархии Orchestrator.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Повторно подготовить	Компьютер	<p>Компьютер удаляется, а затем запускается рабочий процесс подготовки для создания компьютера с таким же именем.</p> <p>Как известно, существует проблема, из-за которой при запросе на повторную подготовку компьютера в каталоге в vRealize Automation может отображаться состояние «Завершено», хотя в действительности должно отображаться состояние «Выполняется». После отправки запроса на повторную подготовку компьютера можно использовать любую из следующих последовательностей для проверки состояния заново подготовленных элементов.</p> <ul style="list-style-type: none"> ■ Инфраструктура > Управляемые компьютеры; ■ Вкладка Развертывания ■ Администрирование > События > Журналы событий. <hr/> <p>Примечание Повторная подготовка компьютера Amazon не допускается.</p> <hr/> <p>Дополнительные сведения см. в статье базы знаний VMware «Задачи для компьютера после повторной подготовки» ... (2065873) на странице http://kb.vmware.com/kb/2065873.</p>
Отправить повторно	Не указан тип ресурса. Не удалось выполнить запрос на начальную подготовку.	<p>Отправьте запрос на подготовку, завершившийся сбоем, еще раз. При повторной отправке запроса процесс подготовки повторяется с начала с использованием ранее введенных значений.</p> <p>Если при обработке запроса произошел сбой и вы можете устранить данную проблему, то можно не создавать новый запрос, а повторно отправить существующий. Если ошибка возникла из-за неправильных значений, например указано хранилище данных, не поддерживающее данный запрос, то необходимо создать новый запрос с новыми значениями.</p> <p>Это действие доступно для всех невыполненных запросов начальной подготовки. Какие-либо права не требуются.</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Продолжить	Развертывание	<p>Возобновите частично выполненный запрос на подготовку. Процесс возобновляется с той точки, где произошла ошибка.</p> <p>В случае сбоя развертывания во время процесса подготовки из-за временных проблем со средой или инфраструктурой, превышения времени ожидания или иных проблем, устранение которых не затрагивает выполнение запроса, можно возобновить процесс подготовки, а не создавать новый запрос на подготовку. Если причиной сбоя являются ошибки в схеме элементов, возобновление не выполняется. В этом случае не следует пытаться возобновить процесс — необходимо создать запрос на новое развертывание.</p> <p>Если запрос развертывания выполнен частично и вы можете устранить возникшую проблему, можно использовать действие возобновления. Обработка запроса возобновляется с той точки, где произошла ошибка.</p> <p>Дополнительные сведения см. в разделе Как работает действие «Возобновить».</p>
Откат моментальных снимков	Виртуальная машина	<p>Восстановление из предыдущего моментального снимка для этого компьютера. Для использования этого действия требуется наличие существующего моментального снимка.</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Уменьшить масштаб	Развертывание	<p>Удаление ненужных экземпляров компьютеров в развертывании в соответствии с требованиями по уменьшению емкости. Будут удалены компоненты компьютера и установленные на них компоненты программного обеспечения. Зависимые компоненты программного обеспечения, а также компоненты сети и безопасности обновляются в соответствии с новой конфигурацией развертывания. Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операций масштабирования.</p> <p>Можно попытаться исправить частично успешные операции, выполнив повторное масштабирование. Однако нельзя выполнить масштабирование развертывания до его текущего размера, и исправление частично успешного масштабирования таким образом не отменит выделение обособленных ресурсов. Можно просмотреть окно со сведениями о выполнении запроса и понять, какие задачи и на каких узлах дали сбой. Это поможет решить, стоит ли исправлять частично успешное масштабирование с помощью новой операции масштабирования. Неудачные и частично успешные операции масштабирования не влияют на функциональность исходного развертывания, вы можете продолжать использовать элементы каталога во время устранения неполадок.</p>

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Увеличить масштаб	Развертывание	<p>Подготовьте дополнительные экземпляры компьютеров в своем развертывании, чтобы обеспечить соответствие требованиям увеличенной емкости. Будут подготовлены компоненты компьютера и установленные на них компоненты программного обеспечения. Зависимые компоненты программного обеспечения, а также компоненты сети и безопасности обновляются в соответствии с новой конфигурацией развертывания. Компоненты Все как услуга не подлежат масштабированию и не обновляются во время операций масштабирования.</p> <p>Можно попытаться исправить частично успешные операции, выполнив повторное масштабирование. Однако нельзя выполнить масштабирование развертывания до его текущего размера, и исправление частично успешного масштабирования таким образом не отменит выделение обособленных ресурсов. Можно просмотреть окно со сведениями о выполнении запроса и понять, какие задачи и на каких узлах дали сбой. Это поможет решить, стоит ли исправлять частично успешное масштабирование с помощью новой операции масштабирования. Неудачные и частично успешные операции масштабирования не влияют на функциональность исходного развертывания, вы можете продолжать использовать элементы каталога во время устранения неполадок.</p> <p>Если выбран параметр Распространять обновления на существующие развертывания на странице Настройки схем элементов в исходной схеме элементов, любое увеличение минимальных и максимальных параметров ЦП, памяти или хранилища в схеме элементов автоматически отражается в активных развертываниях, подготовленных на основе этой схемы элементов. Дополнительные сведения см. в разделе Настройки свойств схемы элементов.</p>
Завершение	Компьютер	Завершение работы гостевой операционной системы и выключение компьютера. Чтобы использовать это действие, необходимо установить VMware Tools на компьютере.
Приостановить	Компьютер	Приостановка работы компьютера, чтобы его невозможно было использовать и он не потреблял никакие системные ресурсы, кроме используемых в настоящее время ресурсов хранилища.

Таблица 4-2. Команды в меню «Действие» (продолжение)

Действие	Тип ресурса	Описание
Отменить регистрацию	Компьютер	Исключите компьютер из иерархии, не удаляя его. Незарегистрированные компьютеры не используются.
Отменить регистрацию	Сеть	Исключить сеть из иерархии, не удаляя ее. Незарегистрированные сети недоступны для использования.
Отмена регистрации VDI	Виртуальная машина (XenServer)	Отмена регистрации образа виртуального диска для элементов XenServer.

Поиск и устранение неполадок из-за отсутствия действий в меню «Действия ресурсов»

Для владельца компьютера или ресурсов отображаются не все уполномоченные действия для подготовленного элемента.

Проблема

Если известно, что пользователю или бизнес-группе предоставлено право на использование действия в среде, ожидается, что при выборе элемента в списке **Развертывание** будут отображаться все действия.

Причина

Доступность действий зависит от типа подготовленного ресурса, его рабочего состояния, параметров и способа, которым к нему можно получить доступ. В списке ниже приведены некоторые причины, по которым могут отображаться не все настроенные действия.

- Действие неприменимо при текущем состоянии подготовленного ресурса. Например, действие «Выключить» доступно, только если компьютер включен.
- Действие неприменимо к выбранному типу элемента. Если элемент не поддерживает действие, оно не отображается в списке. Например, действие «Создать моментальный снимок» недоступно для физического компьютера, а «Подключиться посредством RDP» — в случае, если в качестве элемента выбран компьютер Linux.
- Действие применимо к типу подготовленного ресурса, но оно деактивировано в схеме элементов инфраструктуры. Если действие деактивировано, оно не отображается в списке доступных действий ни для одного элемента, подготовленного с использованием схемы элементов.
- На действие не распространяется право, использованное для подготовки элемента, с которым нужно выполнить это действие. В меню «Действия» могут отображаться только уполномоченные действия. Они могут отображаться как компоненты схемы элементов Инфраструктура как услуга или действия ресурса Все как услуга.
- Действие создается в виде действия ресурса Все как услуга, но на него не распространяется право, использованное для подготовки элемента, с которым нужно выполнить это действие. В меню «Действия» отображаются только уполномоченные действия.
- Возможность выполнения действия может быть ограничена в зависимости от настроенных целевых критериев для действий ресурсов Все как услуга или сопоставлений ресурсов с подготовленными компьютерами Инфраструктура как услуга.

Решение

- ◆ Убедитесь, что действие применимо к подготовленному элементу или к состоянию подготовленного элемента.
- ◆ Убедитесь, что действие настроено и на него распространяется право, использованное для подготовки элемента.

Создание моментального снимка виртуальной машины

Возможность создания моментального снимка виртуальной машины зависит от того, как администраторы настроили рабочую среду. Моментальный снимок — это образ виртуальной машины в определенный момент времени. Это компактная копия исходного образа виртуальной машины. С помощью моментальных снимков можно легко восстановить систему в случае повреждения, потери данных или угроз безопасности. Создав моментальный снимок виртуальной машины, можно применить его и сбросить параметры системы до момента, когда был сделан моментальный снимок.

При создании моментального снимка памяти фиксируется состояние параметров питания виртуальной машины и (при необходимости) память виртуальной машины. Если фиксируется состояние памяти виртуальной машины, операция создания моментального снимка занимает больше времени. Также может возникнуть кратковременная задержка ответа сети.

Необходимые условия

- Существующая виртуальная машина во включенном, отключенном или приостановленном состоянии.
- Если виртуальная машина настроена для одного или нескольких независимых дисков, выключите ее перед созданием моментального снимка. Когда она включена, создать моментальный снимок невозможно. Сведения о конфигурации диска см. в таблице *Настраиваемые свойства V*.
- Администратор арендатора или диспетчер бизнес-групп должен предоставить право на выполнение действий с моментальными снимками.

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит компьютер, для которого нужно сделать моментальный снимок, и нажмите имя этого развертывания.
3. На вкладке **Компоненты** выберите эту виртуальную машину и нажмите значок действий (шестеренка).
Откроется меню действий для данного компонента.
4. В меню «Действия» выберите пункт **Создать моментальный снимок**.
5. Введите имя и, при необходимости, описание.
6. Если необходимо создать моментальный снимок состояния памяти и параметров питания компьютера, выберите **Добавить память**.
7. Нажмите кнопку **Отправить**.

Удаленное подключение к компьютеру

С помощью консоли vRealize Automation можно осуществлять удаленное подключение к компьютеру.

Если для подключения используется VMware Remote Console, см. инструкции в статье базы знаний [Устранение неполадок при подключении по VMRC в vRealize Automation \(2114235\)](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, администратора арендатора** или **диспетчера бизнес-групп**.
- Убедитесь, что установлены инструменты VMware Tools.

VMware Tools должны быть установлены в клиенте vRealize Automation, так как они обеспечивают поддержку полностью функционального доступа при подключении с помощью VMware Remote Console. Если инструменты VMware Tools не установлены, при работе будут возникать неполадки. Например, после подключения к целевому компьютеру могут не работать указатель и кнопки мыши. Дополнительные сведения о поддерживаемых версиях VMware Tools см. в [таблице совместимости решений с vRealize Automation в документации по vRealize Automation](#).

- Убедитесь, что подготовленный компьютер включен.
- Разрешите прохождение сетевого трафика между устройствами vRealize Automation и сервером ESXi по порту 902.
- Разрешите прохождение сетевого трафика между устройствами vRealize Automation и браузером клиента по порту 8444.
- Разрешите прохождение сетевого трафика между Windows-серверами веб-компонента инфраструктуры как услуги и связанными конечными точками vSphere через порт 443.

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит компьютер, к которому нужно подключиться, и нажмите имя этого развертывания.
3. На вкладке **Компоненты** выберите этот компьютер и нажмите значок действий (шестеренка).
Откроется меню действий для данного компонента.
4. Выберите метод удаленного подключения.
 - Чтобы подключиться по протоколу RDP, выберите элемент **Подключение по протоколу RDP**.
 - Выберите элемент **Подключение к удаленной консоли**, чтобы подключиться с помощью VMware Remote Console.

Обработайте все запросы.
5. Нажмите кнопку **Подключить** и войдите в систему компьютера, следуя инструкциям.
6. По завершении выйдите из системы и закройте окно браузера.

Настройка удаленных консолей для vSphere с ненадежными сертификатами SSL

Если в вашем развертывании vRealize Automation используются ненадежные сертификаты, то перед применением удаленных консолей с помощью VMware Remote Console необходимо задать в клиентском браузере доверие к этому сертификату. Эта процедура может отличаться в зависимости от браузера.

Если устройство vRealize Automation настроено с доверенным сертификатом SSL для вашей среды, то в VMware Remote Console дополнительная настройка в клиентских браузерах не требуется. Если сертификат устройства vRealize Automation заменяется и является доверенным сертификатом, обновлять сведения о сертификате для клиентского браузера не нужно.

Если необходимо заменить сертификат, ознакомьтесь с разделом о замене сертификата Устройство vRealize Automation в документе *Администрирование системы* для vRealize Automation.

Для защиты удаленных подключений с помощью VMware Remote Console для компьютеров, подготовленных в vSphere, применяются сертификаты устройства vRealize Automation через консоль прокси-сервера. Для VMware Remote Console требуется поддержка WebSockets в браузере, а браузеры должны доверять сертификату устройства vRealize Automation. Для получения сертификата можно перейти в виртуальное устройство корневого уровня по адресу формы <https://vra-va.eng.mycompany.com/>.

Сведения о требованиях к поддержке для браузеров и vSphere см. в разделе *Матрица поддержки vRealize Automation*.

Настройка в Firefox доверия к сертификатам для устройства vRealize Automation

Ненадежные сертификаты устройства vRealize Automation необходимо вручную импортировать в клиентские браузеры для поддержки VMware Remote Console в клиентах, подготовленных в среде vSphere.

Сведения о поддерживаемых версиях браузера Firefox см. в разделе *Матрица поддержки VMware vRealize* в vRealize Automation [Информационном центре](#).

Примечание Если устройство vRealize Automation настроено с доверенным сертификатом SSL для вашей среды, то в VMware Remote Console дополнительная настройка в клиентских браузерах не требуется.

Процедура

1. В браузере Firefox выполните вход в устройство vRealize Automation.
Появляется сообщение о том, что сертификат не является доверенным.
2. Выберите **Открыть меню > Параметры**.
3. Щелкните **Конфиденциальность и безопасность**, затем щелкните **Просмотреть сертификаты**.
4. В диалоговом окне «Диспетчер сертификатов» выберите **Серверы**, затем щелкните **Добавить исключение**.
5. Добавьте URL-адрес устройства vRealize Automation с портом 8444.

Например, <https://your-vra-fqdn-domain:8444>.

6. Щелкните **Получить сертификат**, затем щелкните **Подтвердить исключение безопасности**.

7. Нажмите кнопку **ОК**.

Результаты

Вы можете подключаться к удаленной консоли без ошибок сертификата.

Настройка в Internet Explorer доверия к сертификату для устройства vRealize Automation

Недоверенные сертификаты Устройство vRealize Automation необходимо вручную импортировать в клиентские браузеры для поддержки VMware Remote Console в клиентах, подготовленных в среде vSphere.

Примечание Если устройство vRealize Automation настроено с доверенным сертификатом SSL для вашей среды, то в VMware Remote Console дополнительная настройка в клиентских браузерах не требуется.

Операции в этой процедуре применяются для самозаверяющих сертификатов и сертификатов, выданных центром сертификации.

Сведения о поддерживаемых версиях Internet Explorer см. в разделе *Таблица поддержки VMware vRealize* на веб-сайте VMware.

Процедура

1. В браузере Internet Explorer выполните вход в Устройство vRealize Automation.
2. Щелкните **Просмотреть сертификат** в сообщении об ошибке сертификата, которое появляется в адресной строке браузера.
3. Перейдите на вкладку **Общие** в окне «Сведения о сертификате».
4. Убедитесь, что сведения о сертификате являются корректными и щелкните **Установить сертификат**.
5. Установите флажок **Поместить все сертификаты в следующее хранилище** в диалоговом окне «Хранилище сертификатов».
6. Щелкните **Обзор**, чтобы найти хранилище сертификатов.
7. Установите флажок **Доверенный корневой центр сертификации** и нажмите **ОК**.
8. Нажмите **Далее** в диалоговом окне «Хранилище сертификатов».
9. Нажмите **Да** в диалоговом окне «Предупреждение системы безопасности», чтобы установить сертификат.
10. Перезапустите браузер.

Результаты

Вы можете подключаться к удаленной консоли без ошибок сертификата.

Настройка в Chrome доверия к сертификатам для устройства vRealize Automation

Недоверенные сертификаты Устройство vRealize Automation необходимо вручную импортировать в клиентские браузеры для поддержки VMware Remote Console в клиентах, подготовленных в среде vSphere.

Дополнительные сведения о поддерживаемых версиях Chrome см. в *таблице совместимости решений с vRealize Automation* в [документации по vRealize Automation](#).

Примечание Если устройство vRealize Automation настроено с доверенным сертификатом SSL для вашей среды, то в VMware Remote Console дополнительная настройка в клиентских браузерах не требуется.

В ОС Windows браузеры Chrome и Internet Explorer используют одно и то же хранилище сертификатов. Это означает, что сертификаты, которым доверяет Internet Explorer, также доверяет Chrome. Для установления доверенных сертификатов для Chrome импортируйте их с помощью Internet Explorer. Описание этой процедуры см. в разделе [Настройка в Internet Explorer доверия к сертификату для устройства vRealize Automation](#).

По окончании данной процедуры перезапустите Chrome.

Для обеспечения постоянного доверия к сертификату в операционной системе Macintosh загрузите файл сертификата и установите сертификат как доверенный в средстве управления сертификатами.

Процедура

1. В браузере Chrome выполните вход в Устройство vRealize Automation.
2. Щелкните значок *Сведения о сайте* рядом с адресной строкой браузера, затем щелкните значок **Сертификат**, чтобы посмотреть информацию о сертификате.
3. Сохраните сертификат.
4. Запустите приложение Keychain Access, которое обычно размещено в подпапке «Служебные программы» (Utilities) в папке «Приложения» (Applications).
5. Выберите **Файл > Импортировать элементы**.
6. На экране Keychain Access выберите ранее сохраненный файл сертификата.
Для параметра **Ключ назначения** установите значение **Система**.
7. Щелкните **Открыть**, чтобы импортировать сертификат.
8. Перезапустите браузер.

Задание параметров перенастройки компьютера и рекомендации по перенастройке

Платформами vSphere, vCloud Air и vCloud Director поддерживается перенастройка существующих компьютеров в развертывании для изменения таких спецификаций, как ЦП, память и хранилище.

Запросы на перенастройку подлежат утверждению на основе прав, политик и действий, включенных для компонента компьютера в схеме элементов.

Перенастройка виртуальной машины, назначенной сети по требованию, не поддерживается. Нельзя перенастроить сетевой адаптер, подключенный к сети по требованию. При попытке перенастроить сеть NAT по требованию или маршрутизируемую сеть появится сообщение об ошибке Original network [`<network>`] is not selected in the machine's reservation., а сети и IP-адреса на компьютере не изменятся.

Если имеется право на действия «Отмена перенастройки (компьютера)» и «Запуск перенастройки (компьютера)», то можно отменить изменение конфигурации или повторить неудавшуюся перенастройку.

Расширение диска на виртуальной машине, которая была подготовлена с использованием схемы элементов связанного клона, не поддерживается.

С помощью профилей компонентов **Size** и **Image** компьютеры перенастроить нельзя. Диапазон ресурсов ЦП, памяти и хранилища из рассчитывается из профиля и остается доступным при выполнении действий по перенастройке. Например, можно использовать следующие наборы значений **Size**: малый (1 ЦП, объем памяти — 1024 МБ, объем хранилища — 10 ГБ), средний (3 ЦП, объем памяти — 2048 МБ, объем хранилища — 12 ГБ) и большой (5 ЦП, объем памяти — 3072 МБ памяти, объем хранилища — 15 ГБ) . При перенастройке компьютера доступны следующие диапазоны ресурсов: количество ЦП — от 1 до 5, объем памяти — от 1024 до 3072 ГБ, объем хранилища — от 1 до 15 ГБ.

Во время развертывания vRealize Automation создает моментальный снимок схемы элементов. Если в развертывании возникли проблемы перенастройки при обновлении свойств компьютера, таких как ЦП и ОЗУ, см. в статье базы знаний 2150829 [Создание моментального снимка схемы элементов vRA 7.x](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, пользователя поддержки, пользователя бизнес-группы с ролью коллективного доступа** или **диспетчера бизнес-групп**.
- Компьютер, который необходимо перенастроить, должен быть во включенном или выключенном состоянии и не быть в активном состоянии перенастройки.
- Тип компьютера должен быть таким: vSphere, vCloud Air или vCloud Director, хотя параметры NSX применяются только к vSphere.
- Убедитесь, что у вас есть право на перенастройку компьютера.

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит компьютер, который нужно перенастроить, и нажмите имя этого развертывания.
3. На вкладке **Компоненты** выберите эту виртуальную машину и нажмите значок действий (шестеренка).
Откроется меню действий для данного компонента.
4. Выберите **Перенастроить**.
5. Выберите вкладку, соответствующую параметрам, которые необходимо перенастроить.

Таблица 4-3. Изменения, требующие запроса на перенастройку

Вкладка	Тема
Общие	Перенастройка процессоров и памяти
Хранилище	Изменение параметров хранилища

Таблица 4-3. Изменения, требующие запроса на перенастройку (продолжение)

Вкладка	Тема
Сеть	Изменение параметров сети Сведения об изменении правил NAT см. в разделе Изменение правил NAT в развертывании .
Безопасность	Сведения о перенастройке параметров безопасности см. в разделе Добавление и удаление элементов системы безопасности в развертывании .
Свойства	Изменение параметров настраиваемых свойств и группы свойств

Следующие шаги

[Выполнение запрошенной перенастройки компьютера](#) .

Перенастройка процессоров и памяти

Можно изменить количество ЦП или объем памяти и хранилища, используемых подготовленным компьютером, в пределах, установленных схемой элементов подготовки.

Для подготовленных развертываний Amazon можно изменить все тома хранилища в развертывании, за исключением корневого тома.

Расширение диска на виртуальной машине, которая была подготовлена с использованием схемы элементов связанного клона, не поддерживается.

Необходимые условия

[Задание параметров перенастройки компьютера и рекомендации по перенастройке](#).

Процедура

1. Откройте вкладку **Общие**.
2. В текстовом поле **Количество ЦП** введите количество ЦП.
3. В текстовом поле **Память (МБ)** введите объем памяти.
4. В текстовом поле **Хранилище (ГБ)** введите объем хранилища.

Следующие шаги

Задайте дополнительные параметры перенастройки компьютера. Завершив изменение параметров компьютера, запустите запрос на его перенастройку. См. раздел [Выполнение запрошенной перенастройки компьютера](#) .

Изменение параметров хранилища

Томы хранилища подготовленной виртуальной машины можно добавлять и удалять, а также изменять их размер.

Нельзя перенастроить том хранилища для диска типа IDE.

Хранилище и память, назначенные подготовленному компьютеру путем резервирования, освобождаются, когда компьютер, которому они назначены, удаляется в vRealize Automation. Хранилище и память не освобождаются, если компьютер удален в vCenter Server.

Например, нельзя удалить резервирование, которое связано с компьютерами в существующем развертывании. При перемещении или удалении развернутых компьютеров в vCenter Server вручную vRealize Automation по-прежнему распознает развернутые компьютеры как существующие и не даст удалить связанные резервирования.

После подготовки и развертывания компьютера можно изменить отдельные параметры, например политику резервирования емкости и хранилища.

На этапе подготовки для гостевого агента применяются значения **Буква диска/путь монтирования** и **Метка**. Эти значения не обновляются после подготовки и, следовательно, могут быть неактуальны. Для сбора и отображения данных текущих значений можно создать и запустить настраиваемый рабочий процесс vRealize Orchestrator.

Необходимые условия

[Задание параметров перенастройки компьютера и рекомендации по перенастройке.](#)

Для подготовленных развертываний Amazon можно изменить все тома хранилища в развертывании, за исключением корневого тома.

Процедура

1. Откройте вкладку **Хранилище**.
2. При необходимости просмотрите или измените параметры хранилища.

- Добавьте новый том, если это возможно.
- Удалите том, если это возможно.

Значок невозможности выбора обозначает том, который нельзя удалить, например том связанного клона.

- Измените размер тома, если это возможно.

Размер существующих томов нельзя уменьшить. Размер тома ограничен общим объемом хранилища, указанным в схеме элементов. Он меньше объема, выделенного для других томов.

Следующие шаги

Задайте дополнительные параметры перенастройки компьютера. Завершив изменение параметров компьютера, запустите запрос на его перенастройку. См. раздел [Выполнение запрошенной перенастройки компьютера](#).

Изменение параметров сети

Можно добавить, удалить или изменить сетевой адаптер.

Во время перенастройки компьютера возможны следующие действия по изменению параметров сети.

- Добавление или удаление сетевых адаптеров.

- Выделение или освобождение IP-адресов для существующих сетевых адаптеров.
- Назначение новых IP-адресов сетевым адаптерам, при этом сеть не должна быть сетью NAT по требованию или маршрутизируемой сетью по требованию.

Перенастроить сеть NAT по требованию или маршрутизируемую сеть по требованию невозможно.

Для перенастройки сети необходимо, чтобы исходная и целевая сети были выбраны в резервировании.

При добавлении сетевых адаптеров IP-адреса выделяются. При удалении сетевых адаптеров IP-адреса освобождаются.

При изменении параметров сети с учетом резервирования и сведений профиля сети для vRealize Automation будет назначен новый IP-адрес сети, но на уже развернутом компьютере на конечной точке не будут обновлены сведения о новом IP-адресе. Необходимо вручную назначить новый IP-адрес таким компьютерам после завершения процесса перенастройки.



Перенастройка виртуальной машины, назначенной сети по требованию, не поддерживается. Нельзя перенастроить сетевой адаптер, подключенный к сети по требованию. При попытке перенастроить сеть NAT по требованию или маршрутизируемую сеть появится сообщение об ошибке `Original network [<network>] is not selected in the machine's reservation.`, а сети и IP-адреса на компьютере не изменятся.

Изменение параметров сети NSX не поддерживается для развертываний, которые были обновлены или перенесены из vRealize Automation 6.2.x в этот выпуск vRealize Automation.

Необходимые условия



[Задание параметров перенастройки компьютера и рекомендации по перенастройке.](#)

Процедура

1. Перейдите на вкладку **Сеть**.
2. (дополнительно) Добавьте сетевой адаптер.
 - а) Щелкните **Новый сетевой адаптер**.
 - б) В раскрывающемся меню **Сетевой путь** выберите сеть.
Все сети, выбранные в резервировании компьютера, доступны.
 - в) В текстовом поле **Адрес** введите статический IP-адрес для сети.
Этот IP-адрес должен быть не выделенным в сетевом профиле, назначенном резервированию.
 - г) Щелкните значок **Сохранить** (.
3. (дополнительно) Удалите сетевой адаптер.
 - а) Найдите сетевой адаптер.
 - б) Щелкните значок **Удалить** (.

Нельзя удалить сетевой адаптер O.

4. (дополнительно) Измените сетевой адаптер.

- а) Найдите сетевой адаптер.
- б) Щелкните значок **Изменить** ().
- в) В раскрывающемся меню **Сетевой путь** выберите сеть.
- г) Щелкните значок **Сохранить** (.

Следующие шаги

Задайте дополнительные параметры перенастройки компьютера. Завершив изменение параметров компьютера, запустите запрос на его перенастройку. См. раздел [Выполнение запрошенной перенастройки компьютера](#).

Изменение параметров настраиваемых свойств и группы свойств

На развернутом компьютере можно изменять, добавлять и удалять настраиваемые свойства.

Настраиваемые свойства нельзя использовать для ввода номера, емкости, метки или политики резервирования хранилища диска тома. Необходимо ввести эти значения, добавив или изменив том в таблице томов хранилища. См. раздел [Изменение параметров хранилища](#).

Необходимые условия

[Задание параметров перенастройки компьютера и рекомендации по перенастройке.](#)

Процедура

1. Перейдите на вкладку **Свойства**.
2. Чтобы добавить свойство, нажмите кнопку **Создать свойство**.
3. В текстовом поле **Имя** введите имя свойства.
4. В текстовом поле **Значение** введите значение свойства.
5. Установите флажок **Зашифровано**, чтобы зашифровать значение.
6. Установите флажок **Запросить пользователя**, чтобы запрашивать у пользователей значение при запросе доступа к компьютеру.
7. Добавьте еще одно свойство, измените существующее свойство или удалите его.

Следующие шаги

Задайте дополнительные параметры перенастройки компьютера. Завершив изменение параметров компьютера, запустите запрос на его перенастройку. См. раздел [Выполнение запрошенной перенастройки компьютера](#).

Выполнение запрошенной перенастройки компьютера

Запрошенную перенастройку компьютера можно начать сразу или можно запланировать ее запуск на определенный день и время. Кроме того, прежде чем перенастроить компьютер, можно указать параметр его питания.

Необходимые условия

Задание параметров перенастройки компьютера и рекомендации по перенастройке.

Процедура

1. Если видна вкладка **Выполнение**, можно выбрать ее, чтобы указать дополнительные параметры перенастройки. Если она недоступна, нажмите кнопку **Отправить**, чтобы начать перенастройку компьютера.
2. Если вкладка **Выполнение** доступна, нажмите кнопку **Выполнение**, чтобы запланировать действие перенастройки.
3. (дополнительно) Выберите пункт в раскрывающемся меню **Выполнить запрос**.

Параметр	Описание
Текущий момент	После подтверждения как можно скорее запустите перенастройку.
По расписанию	Запустите перенастройку в указанные дату и время. Введите дату и время в появившихся текстовых полях.

Запланированное время — это местное время, соответствующее параметрам расположения веб-сервера vRealize Automation. Если раскрывающееся меню **Выполнить запрос** недоступно, перенастройка запустится сразу.

4. (дополнительно) В раскрывающемся меню **Действие с питанием** выберите действие с питанием.

Параметр	Описание
Перезагрузить, если потребуется	(По умолчанию) При необходимости перезапустите компьютер перед его перенастройкой.
Перезагрузить	Перезапустите компьютер перед его перенастройкой независимо от того, требуется ли перезапуск.
Не перезагружать	Не перезапускайте компьютер перед перенастройкой, даже если требуется перезапуск.

Перезапуск компьютера перед перенастройкой требуется в следующих ситуациях:

- изменение ЦП, после которого не поддерживается или деактивировано «горячее» добавление ЦП;
- изменение памяти, после которого «горячее» добавление памяти не поддерживается или деактивировано;
- изменение хранилища, после которого «горячее» добавление хранилища деактивировано.

Если компьютер находится в состоянии отключения, его нельзя перезапустить.

Примечание Параметр «горячего» добавления vSphere можно деактивировать с помощью настраиваемого свойства `VirtualMachine.Reconfigure.DisableHotCpu`.

5. Нажмите кнопку **ОК**.

Следующие шаги

За ходом перенастройки можно следить, наблюдая за состоянием рабочих процессов, которые отображаются в пользовательском интерфейсе. См. раздел [Состояния рабочего процесса операций перенастройки](#).

Состояния рабочего процесса операций перенастройки

На странице изменения можно наблюдать за ходом выполнения рабочего процесса перенастройки.

Таблица 4-4. Состояния рабочего процесса операций перенастройки

Состояние	Описание
Ожидание перенастройки	Создана операция состояния.
По расписанию	Для Distributed Execution Manager создан запланированный рабочий процесс.
Перенастройка	Выполняется рабочий процесс, зависящий от интерфейса.
Не удалось выполнить перенастройку. Ожидание повторной попытки.	Не удалось выполнить перенастройку. Ожидание запроса владельца на повторную попытку. Если владелец компьютера имеет права на перенастройку или отмену действий по перенастройке, он может повторить перенастройку или отменить ее.
Сбой перенастройки	Не удалось выполнить перенастройку. Ожидание выполнения следующего действия рабочим процессом.
Перенастройка успешно выполнена	Перенастройка выполнена успешно. Ожидание выполнения следующего действия рабочим процессом.
Отменен	Пользователь отменил перенастройку. Владельцы компьютеров, которым предоставлены права, могут отменить перенастройку.
Комплексное	Рабочий процесс завершения устанавливает это состояние после завершения очистки, чтобы рабочий процесс мог перейти к очистке операций состояния и подтверждений. Состояние «Завершено» означает, что запрос из vRealize Automation завершен, но это не означает, что перенастройка компьютера успешно завершена.

Перенастройка подсистемы балансировки нагрузки в развертывании

Можно добавить, изменить или удалить виртуальный сервер в развертывании подсистемы балансировки нагрузки NSX.

Следующая информация относится к развертываниям, основанным на vRealize Automation 7.2 или более ранних версиях.

- Перенастройка подсистем балансировки нагрузки возможна только для развертываний, содержащих одну подсистему балансировки нагрузки.
- На странице сведений об элементах для любой подсистемы балансировки нагрузки в развертывании отображаются виртуальные серверы, используемые всеми подсистемами балансировки нагрузки в развертывании. Дополнительные сведения см. в [статье базы знаний 2150276](#).
- Операция «Перенастройка подсистемы балансировки нагрузки» не поддерживается для развертываний, которые были обновлены или перенесены из vRealize Automation 6.2.x в этот выпуск vRealize Automation.

Если используются обновленные подсистемы балансировки нагрузки и подсистемы балансировки нагрузки, развернутые в текущей версии vRealize Automation, не редактируйте и не добавляйте виртуальный сервер в одном и том же запросе. Дополнительные сведения см. в [статье базы знаний 2150240](#).

Примечание Действие **Перенастройка** не доступно для подсистем балансировки нагрузки NSX-T.

При отправке запроса на перенастройку подсистемы балансировки нагрузки во время выполнения другого действия в развертывании, например при осуществлении в развертывании операции увеличения масштаба, происходит сбой перенастройки с сопутствующим сообщением. В этом случае можно дождаться завершения действия, а затем отправить запрос на перенастройку.

Примечание Если схема элементов, связанная с развертыванием, импортируется из файла YAML, в котором в поле имени используемой по требованию подсистемы балансировки нагрузки содержится не такое значение, как в поле идентификатора, действие **Перенастройка** завершается сбоем. Чтобы включить перенастройку подсистемы балансировки нагрузки в развертывании, основанном на импортированной схеме элементов, выполните следующие операции в схеме элементов. Это позволит действиям, осуществляемым после подготовки, выполняться в отношении компонентов подсистемы балансировки нагрузки в будущих развертываниях.

1. Выберите схему элементов в консоли vRealize Automation.
2. Щелкните **Изменить** и измените имя схемы элементов. После этого имя и встроенный идентификатор станут одинаковыми.
3. Выберите компонент балансировки нагрузки в схеме элементов.
4. Щелкните **Изменить** и еще раз введите имя компонента. После этого имя и встроенный идентификатор станут одинаковыми.
5. Повторите это действие для всех компонентов балансировки нагрузки в схеме элементов.
6. Сохраните схему элементов.

Когда с помощью измененной схемы элементов будет подготавливаться новое развертывание, действие по перенастройке подсистемы балансировки нагрузки выполнится успешно. Чтобы избежать этой проблемы, перед импортом каждого файла YAML необходимо убедиться, что значения имени и идентификатора у всех компонентов подсистемы балансировки нагрузки, сети и системы безопасности совпадают.

Не работайте с объектами NSX под управлением vRealize Automation за пределами vRealize Automation. Например, если изменить порт-участник развернутой подсистемы балансировки нагрузки в NSX, а не в vRealize Automation, то сбор данных NSX прерывается. Операции горизонтального и вертикального масштабирования также выполняются с непредсказуемым результатом.

Дополнительные сведения о параметрах, которые доступны при добавлении или изменении виртуального сервера, см. в разделе [Добавление компонента «Подсистема балансировки нагрузки по требованию»](#).

При перенастройке подсистемы балансировки нагрузки в vRealize Automation некоторые из параметров, настроенных в NSX и не доступных в качестве параметров в vRealize Automation, возвращаются к своим значениям по умолчанию. После выполнения действия перенастройки подсистемы балансировки нагрузки в vRealize Automation проверьте и при необходимости обновите следующие параметры в NSX.

- Insert-X-Forwarded для заголовка HTTP
- URL-адрес перенаправления HTTP
- Расширение монитора служб

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, пользователя поддержки, пользователя бизнес-группы с ролью коллективного доступа или диспетчера бизнес-групп**.
- Убедитесь, что у вас имеется право на перенастройку подсистем балансировки нагрузки в развертывании. Требуется право «Перенастройка (подсистема балансировки нагрузки)» для каталога.

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит подсистему балансировки нагрузки, которую нужно перенастроить, и нажмите имя этого развертывания
3. На вкладке **Компоненты** выберите нужную подсистему балансировки нагрузки и нажмите значок действий (шестеренка).

Откроется меню действий для данного компонента.

4. Выберите **Перенастроить**.
5. Добавьте, измените или удалите виртуальные серверы.

Virtual servers:

Protocol	Port	Description	Member Protocol	Member Port	Health Check Protocol	Health Check Port
HTTP	80		HTTP	80	HTTP	80
HTTP	81		HTTP	81	HTTP	81

6. Нажмите кнопку **Отправить**.

Изменение правил NAT в развертывании

В развернутой сети NAT «один ко многим» можно добавлять, редактировать и удалять существующие правила NAT NSX.

Можно также изменять порядок обработки правил NAT.

Примечание Если исходная схема элементов развертывания импортируется из файла YAML, содержащего компонент сети NAT, а значения имени и идентификатора сетевого компонента NAT не совпадают, при выполнении действия **Изменить правила NAT** происходит сбой. Чтобы разрешить действие **Изменить правила NAT** для развертывания, выполняемого на основе импортированной схемы элементов, перед выполнением развертывания выполните следующие действия со схемой элементов.

1. Запустите vRealize Automation, перейдите на вкладку «Проектирование» и откройте схему элементов.
2. Щелкните **Изменить** и измените имя схемы элементов. После этого имя и встроенный идентификатор станут одинаковыми.
3. Выберите компонент сети NAT в схеме элементов.
4. Щелкните **Изменить** и еще раз введите имя компонента. После этого имя и встроенный идентификатор станут одинаковыми.
5. Повторите это для всех компонентов сети NAT в схеме элементов.
6. Сохраните схему элементов.

Чтобы избежать этой проблемы, перед импортом каждого файла YAML необходимо убедиться, что значения имени и идентификатора для всех схем элементов и компонентов подсистемы балансировки нагрузки, сети и системы безопасности совпадают.

Дополнительные сведения см. в разделах [Создание и использование правил NAT для NSX for vSphere](#) и [Добавление компонента «Сеть NAT по требованию» или «Маршрутизируемая сеть по требованию» в vRealize Automation](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, пользователя поддержки, пользователя бизнес-группы с ролью коллективного доступа** или **диспетчера бизнес-групп**.
- Убедитесь в наличии необходимых разрешений для изменения правил NAT в сети.
- Убедитесь, что сеть NAT настроена как сеть NAT «один ко многим». Это действие недоступно для сетей NAT «один к одному».

NSX for vSphere поддерживает сети NAT «один к одному» и «один ко многим», но NSX-T поддерживает только сети NAT «один ко многим».

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит сетевой компонент, который нужно перенастроить, и нажмите имя этого развертывания.

3. На вкладке **Компоненты** найдите сетевой компонент NAT.

В случае сети NAT по требованию, связанной со сторонним поставщиком управления IP-адресами, изменение этого компонента невозможно. Тем не менее можно вручную добавить новый IP-адрес назначения. При добавлении нового IP-адреса назначения значение компонента обнуляется. Новый IP-адрес назначения и обнуленный идентификатор компьютера обрабатываются при отправке запроса на изменение конфигурации.

4. Нажмите значок действий (шестеренка).

Откроется меню действий для данного компонента.

5. Нажмите **Изменить правила NAT**.

6. Добавьте новые правила переадресации портов NAT, измените или удалите существующие правила.

7. Нажмите кнопку **Отправить**.

Отображение всех правил NAT для существующего объекта NSX Edge

Можно отобразить информацию о правилах NAT для объектов NSX Edge, которые используются в активном развертывании.

Правила NAT отображаются в представлении Edge как совокупность всех правил NAT, используемых в развертывании. В представлении Edge правила не обязательно отображаются в порядке их обработки.

Чтобы просмотреть и при необходимости изменить порядок обработки правил NAT в сети NAT «один ко многим», см. раздел [Изменение правил NAT в развертывании](#).

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, пользователя поддержки, пользователя бизнес-группы с ролью коллективного доступа** или **диспетчера бизнес-групп**.

Процедура

1. Нажмите **Развертывания**.

2. Найдите развертывание, которое содержит просматриваемый компонент NSX Edge, и нажмите имя этого развертывания.

3. На вкладке **Компоненты** найдите компонент NSX Edge.

4. Выберите объект NSX Edge, который необходимо просмотреть.

5. По завершении нажмите кнопку **Закрыть**.

Добавление и удаление элементов системы безопасности в развертывании

Можно добавить или удалить существующие группы безопасности NSX и теги безопасности для развертывания компьютера. Группы безопасности по требованию нельзя добавить. Поддерживается только их удаление.

Действие изменения параметров безопасности определяется компонентом или кластером компьютера. Например, если параметры безопасности связаны с кластером с именем AppTier2, который состоит из двух компьютеров, то операция изменения параметров безопасности выполняется в кластере AppTier2, а не на отдельных компьютерах в кластере.

Операция изменения параметров безопасности не поддерживается для развертываний, которые были обновлены или перемещены из среды vRealize Automation 6.2.x в среду версии vRealize Automation.

Необходимые условия

- Войдите в службу vRealize Automation в качестве **владельца компьютера, пользователя поддержки, пользователя бизнес-группы с ролью коллективного доступа или диспетчера бизнес-групп**.
- Убедитесь в наличии необходимых разрешений для изменения параметров безопасности в развертывании. Требуемые права для каталога: «Изменить параметры безопасности (развертывание)».

Процедура

1. Нажмите **Развертывания**.
2. Найдите развертывание, которое содержит группы безопасности и теги и нажмите имя этого развертывания.
3. На вкладке **Компоненты** выберите нужный компонент безопасности и нажмите значок действий (шестеренку).
Откроется меню действий для данного компонента.
4. Нажмите **Изменить параметры безопасности**.
5. Выберите компонент или кластер компьютера для развертывания, для которого необходимо добавить или удалить элементы безопасности.
6. При необходимости добавьте или удалите существующие группы безопасности и теги безопасности для каждого из компонентов или кластеров компьютера в развертывании.
7. При необходимости добавьте или удалите группы безопасности по требованию для каждого из компонентов или кластеров компьютера в развертывании.
8. (дополнительно) Перейдите на вкладку **Причина** и укажите причину для отправки запроса.
9. Нажмите кнопку **Отправить**.

Дополнительные методы управления развертываниями

Развернутыми ресурсами можно управлять с помощью уполномоченными действиями, но предусмотрены также дополнительные методы, которые не оформлены в виде действий.

Эти методы не доступны на вкладке «Развертывания», но их можно использовать изменения подготовленных ресурсов.

Реорганизация ресурсов в соответствии с показателями vRealize Operations Manager

Реорганизация помогает эффективно использовать ресурсы. Если для управления ресурсами в данной среде также используется vRealize Operations Manager, то можно настроить vRealize Automation на использование соответствующих показателей для определения возможностей реорганизации ресурсов развертывания.

Процедура

1. Настройка поставщика показателей

В vRealize Automation можно настроить использование показателей работоспособности и ресурсов vRealize Operations Manager для виртуальных машин vSphere.

2. Отправка запроса на реорганизацию

Можно просматривать развертывания и управлять ими, а также отправлять запросы на реорганизацию владельцам развертываний. Запрос на реорганизацию определяет продолжительность новой аренды в днях, количество времени, отведенное владельцу развертывания для ответа, и каким компьютерам требуется реорганизация.

3. Отслеживание запросов на реорганизацию

Можно отслеживать текущее состояние запросов на реорганизацию и другие сведения.

Настройка поставщика показателей

В vRealize Automation можно настроить использование показателей работоспособности и ресурсов vRealize Operations Manager для виртуальных машин vSphere.

Дополнительные сведения об эмблемах и показателях vRealize Operations Manager см. в документации по vRealize Operations Manager.

Необходимые условия

- Войдите в консоль vRealize Automation в качестве **администратора арендатора, диспетчера бизнес-групп** или **владельца компьютера**.

Реорганизации. Пользователям, создающим запросы на реорганизацию, нужна роль администратора арендатора, и учетная запись того же администратора арендатора должна входить по крайней мере в одну бизнес-группу арендатора.

Если учетная запись администратора арендатора не добавлена в бизнес-группу, при открытии вкладки **Реорганизация > Развертывания** происходит системное исключение.

- Создайте учетную запись пользователя vRealize Operations Manager с правами на просмотр и запрос показателей ресурсов для всех серверов vSphere, которые интегрируются с vRealize Automation.
- Создайте экземпляры адаптера vRealize Operations Manager для всех серверов vSphere, добавляемых как конечные точки в vRealize Automation. Сведения о создании экземпляров адаптеров см. в документации по vRealize Operations Manager.

Процедура

1. Выберите **Администрирование > Реорганизация > Поставщик показателей.**
2. Выберите поставщика показателей.

Параметр	Описание
Поставщик показателей vRealize Automation (по умолчанию)	Если у вас нет экземпляра vRealize Operations Manager, базовые показатели компьютера можно получить в vRealize Automation.
Конечная точка vRealize Operations Manager	Укажите сведения о подключении к экземпляру vRealize Operations Manager, который нужно использовать в качестве поставщика показателей для виртуальных машин vSphere.

3. Щелкните элемент **Проверить подключение.**
4. Нажмите кнопку **Сохранить.**

Результаты

Администраторы арендатора, владельцы компьютера и диспетчеры бизнес-групп, в которых размещен компьютер, могут видеть значки работоспособности и оповещения о работоспособности на страницах сведений об элементах виртуальных машин vSphere. Они также могут видеть показатели и значки работоспособности vRealize Operations Manager при фильтровании по типу платформы vSphere на странице реорганизации.

Следующие шаги

[Отправка запроса на реорганизацию.](#)

Отправка запроса на реорганизацию

Можно просматривать развертывания и управлять ими, а также отправлять запросы на реорганизацию владельцам развертываний. Запрос на реорганизацию определяет продолжительность новой аренды в днях, количество времени, отведенное владельцу развертывания для ответа, и каким компьютерам требуется реорганизация.

Необходимые условия

- Войдите в vRealize Automation в качестве **администратора арендатора.**
- (дополнительно) Чтобы увидеть значки работоспособности или просмотреть метрики, предоставляемые vRealize Operations Manager, см. раздел [Настройка поставщика показателей.](#)

Процедура

1. Выберите **Администрирование > Реорганизация > Развертывания.**


2. Найдите виртуальную машину, соответствующую критериям поиска.

Для отображения метрик, предоставляемых vRealize Operations Manager, нужно выбрать тип платформы vSphere.

- а) Нажмите стрелку вниз **Расширенный поиск**, чтобы открыть окно поиска.
- б) Введите или выберите одно или несколько искомых значений.

Параметр	Действие
Имя виртуальной машины содержит	В текстовом поле введите один или несколько символов, чтобы найти соответствующие имена виртуальных машин.
Имя владельца содержит	В текстовом поле введите имя, чтобы найти соответствующие имена владельцев.
Имя бизнес-группы содержит	В текстовом поле введите имя, чтобы найти соответствующие имена бизнес-групп.
Тип платформы	В раскрывающемся меню выберите тип платформы. Выберите vSphere, чтобы просмотреть метрики, предоставляемые vRealize Operations Manager. Требуется для vRealize Operations Manager.
Состояние питания	В раскрывающемся меню выберите значение состояния питания, чтобы найти виртуальные машины с соответствующим состоянием питания.
Дата завершения срока действия в диапазоне	Щелкая значки календаря, выберите начальную и конечную даты, чтобы найти срок действия в диапазоне.
Использование ЦП	В раскрывающемся меню выберите значение, чтобы найти виртуальные машины с соответствующим уровнем использования ЦП: «Высокий уровень использования ЦП» (выше 80%), «Низкий уровень использования ЦП» (ниже 5%), «Нет» или без значения. При запросе метрик vRealize Operations Manager нельзя использовать этот фильтр. Кроме того, невозможно сортировать результаты по уровню использования ЦП.
Использование памяти	В раскрывающемся меню выберите значение, чтобы найти виртуальные машины с высоким уровнем потребления памяти: «Высокий уровень потребления памяти» (выше 80%), «Низкий уровень потребления памяти» (ниже 10%), «Нет» или без значения. При запросе метрик vRealize Operations Manager нельзя использовать этот фильтр. Кроме того, невозможно сортировать результаты по уровню потребления памяти.
Использование дисков	В раскрывающемся меню выберите значение, чтобы найти виртуальные машины с соответствующим уровнем использования жесткого диска: «Низкий уровень использования жесткого диска» (менее 2 Кбайт/с), «Нет» или без значения. При запросе метрик vRealize Operations Manager нельзя использовать этот фильтр. Кроме того, невозможно сортировать результаты по уровню использования дисков.
Использование сети	В раскрывающемся меню выберите значение, чтобы найти виртуальные машины с соответствующим уровнем использования сети: «Низкий уровень использования сети» (менее 1 Кбайт/с), «Нет» или без значения.

Параметр	Действие
	При запросе метрик vRealize Operations Manager нельзя использовать этот фильтр. Кроме того, невозможно сортировать результаты по уровню использования сети.
Комплексная метрика	<p>В раскрывающемся меню выберите значение, чтобы найти виртуальные машины на основе комплексных метрик. Например, выберите значение «Простой», чтобы найти компьютеры, в которых значение использования ЦП, сети, памяти и дисков составляет менее 20%.</p> <p>При запросе метрик vRealize Operations Manager нельзя использовать этот фильтр.</p>

в) Щелкните значок поиска ()

3. На странице «Развертывания» выберите один или несколько компьютеров, родительское развертывание которых планируется реорганизовать.

Реорганизованы будут только выбранные компьютеры, которые отображаются на текущей странице результатов.

4. Нажмите кнопку **Реорганизовать**.

В запрос включаются развертывания, в которых содержатся виртуальные машины, выбранные на текущей странице.

Примечание На странице «Реорганизация развертывания» могут содержаться компьютеры, для которых невозможно выполнить реорганизацию, например, компьютеры с истекшим сроком аренды. Если указать компьютер, для которого невозможно выполнить реорганизацию, отобразится следующее сообщение об ошибке:

```
Selection Error: Virtual machine name is not in valid state for reclamation.
```

5. В текстовом поле **Продолжительность новой аренды (дн.)** введите продолжительность новой аренды.

Минимальная продолжительность — 1 день, максимальная — 365 дней, продолжительность по умолчанию — 7 дней.

6. В текстовом поле **Ожидание перед принудительным применением аренды (дн.)** введите количество дней, отведенных владельцу развертывания для ответа на запрос на реорганизацию.

По окончании этого срока развертыванию назначается новая аренда с новой продолжительностью. Минимальная продолжительность периода ожидания — 1 день, максимальная — 365 дней, продолжительность по умолчанию — 3 дня.

7. В текстовом поле **Причина запроса** укажите причину запроса.

8. Нажмите кнопку **Отправить**.

9. Нажмите кнопку **ОК**.

Результаты

После отправки запроса на реорганизацию он отобразится в разделе «Входящие» у владельца развертывания. Если владелец не отвечает на запрос в течение требуемого количества дней, развертыванию назначается новая аренда с определенной продолжительностью, если текущий срок действия аренды не короче нового срока. Если в запросе на реорганизацию владелец щелкнет **Элемент используется**, срок аренды развертывания не изменится. Если владелец щелкнет **Освободить для реорганизации**, срок аренды развертывания сразу истечет.

Следующие шаги

[Отслеживание запросов на реорганизацию.](#)

Отслеживание запросов на реорганизацию

Можно отслеживать текущее состояние запросов на реорганизацию и другие сведения.

Для проверки состояния запросов на организацию доступны следующие альтернативные методы.

- Откройте вкладку **Входящие** и выберите пункт **Запросы на реорганизацию**, чтобы просмотреть сведения о запросах на реорганизацию.
- Откройте вкладку **Запросы на реорганизацию**, чтобы просмотреть список последних запросов
- Нажмите **Развертывания**, чтобы просмотреть последние изменения развертываний.


Необходимые условия

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

Процедура

1. Выберите **Администрирование > Реорганизация > Запросы на реорганизацию**.
2. Найдите виртуальные машины, соответствующие критериям поиска.
 - а) Нажмите стрелку вниз **Расширенный поиск**, чтобы открыть окно поиска.
 - б) Введите или выберите одно или несколько искомых значений.

Параметр	Действие
Имя виртуальной машины содержит	В текстовом поле введите один или несколько символов, чтобы найти соответствующие имена виртуальных машин.
Имя владельца содержит	В текстовом поле введите один или несколько символов, чтобы найти соответствующие имена владельцев.
Причина запроса содержит:	В текстовом поле введите один или несколько символов, чтобы найти соответствующую причину запроса.
Состояние запроса	В раскрывающемся меню выберите значение состояния запроса, чтобы найти виртуальные машины с соответствующим состоянием запроса.

- в) Щелкните значок **Поиск**  или нажмите клавишу ВВОД, чтобы начать поиск.
- г) Нажмите стрелку вверх **Расширенный поиск**, чтобы закрыть окно поиска.

3. (дополнительно) Щелкните элемент **Обновить данные**, чтобы обновить отображение запросов на реорганизацию.

Изменение резервирования управляемого компьютера

Можно изменить параметры резервирования или хранения управляемого компьютера. Эта возможность используется при перемещении компьютера в соответствии с новым путем к хранилищу, который недоступен в текущем резервировании. При развертывании на одном компьютере можно также изменить бизнес-группу для компьютера.

Можно переместить компьютер в развертывание с одним компьютером в другой бизнес-группе, если владелец компьютера принадлежит к целевой бизнес-группе. Чтобы изменить данный параметр бизнес-группы, необходимо быть диспетчером исходной и целевой бизнес-групп.

Примечание Если компьютеру назначена политика резервирования, изменить его бизнес-группу невозможно.

Можно создавать дополнительные резервирования для связанного вычислительного ресурса с помощью пунктов меню **Администрирование > Вычислительный ресурс**.

Хранилище и память, назначенные подготовленному компьютеру путем резервирования, освобождаются, когда компьютер, которому они назначены, удаляется в vRealize Automation. Хранилище и память не освобождаются, если компьютер удален в vCenter Server.

Например, нельзя удалить резервирование, которое связано с компьютерами в существующем развертывании. При перемещении или удалении развернутых компьютеров в vCenter Server вручную vRealize Automation по-прежнему распознает развернутые компьютеры как существующие и не даст удалить связанные резервирования.

Если при изменении резервирования компьютер в vCenter Server будет перемещен в новый каталог хранилища, который не является частью резервирования этого компьютера в vRealize Automation, перед изменением резервирования компьютера убедитесь, что в целевом резервировании выбран целевой или новый каталог хранилища.

Необходимые условия

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

Процедура

1. Выберите **Инфраструктура > Управляемые компьютеры**.
2. Найдите компьютер с резервированием, которое необходимо изменить.
3. В раскрывающемся меню щелкните **Изменить резервирование**.

Чтобы просмотреть информацию об управляемом компьютере, например, связанную схему элементов и вычислительный ресурс, выберите в раскрывающемся меню пункт **Просмотр**.

4. (дополнительно) В раскрывающемся меню **Бизнес-группа** выберите нужную бизнес-группу.
5. (дополнительно) В раскрывающемся меню **Резервирование** выберите резервирование.

6. (дополнительно) В раскрывающемся меню **Хранение** выберите политику хранения.
7. Нажмите кнопку **ОК**.

Работа с папкой "Входящие"

В папку "Входящие" поступают внутренние уведомления о подтверждении запросов каталога, дополнительные запросы в процессе подготовки и сообщения о состоянии запросов реорганизации на основе каких-либо метрик vRealize Operations Manager.

Открывая все вкладки, можно просмотреть поступившие оповещения, требующие действий пользователя.

- **Подтверждения.** Можно отслеживать запросы каталога, требующие подтверждения. Если пользователь определен как лицо, утверждающее запросы каталога, он может отвечать на запросы на подтверждение. См. раздел [Добавление сведений об уровне в параметры политики подтверждения](#).
- **Действие пользователя, выполняемое вручную.** Некоторые запросы каталога требуют уточнений в процессе подготовки. Пользователь может ответить на такие уточняющие запросы. См. раздел [Интеграция vRealize Orchestrator в vRealize Automation](#).
- **Запросы на реорганизацию.** Если для определения возможности реорганизации ресурсов используется vRealize Operations Manager, то можно отслеживать такие запросы на реорганизацию. См. раздел [Отслеживание запросов на реорганизацию](#).