

Руководство по балансировке нагрузки vRealize Automation 8.4

15 апреля 2021 г.

vRealize Automation 8.4

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

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

Содержание

1	Балансировка нагрузки в vRealize Automation и vRealize Orchestrator	5
2	Основные принципы балансировки нагрузки	6
	Транзитный режим SSL	6
	Уведомления подсистемы балансировки нагрузки	6
	Топологии one-arm и multi-arm	7
3	Предварительные условия для настройки подсистем балансировки нагрузки для vRealize Automation	8
	Выполнение начальной установки vRealize Automation или vRealize Orchestrator	9
4	Настройка NSX-V	10
	Настройка глобальных параметров	10
	Настройка профилей приложений	12
	Настройка мониторинга служб	13
	Настройка пулов серверов	15
	Настройка виртуальных серверов	17
5	Настройка NSX-T	19
	Настройка профилей приложений NSX-T	19
	Настройка активного монитора работоспособности NSX-T	20
	Настройка пулов серверов NSX-T	23
	Настройка виртуальных серверов NSX-T	24
	Настройка подсистемы балансировки нагрузки	26
	Добавление виртуальных серверов в подсистему балансировки нагрузки	26
6	Настройка F5 Big-IP LTM	28
	Настройка мониторов	28
	Настройка пулов серверов F5	30
	Настройка виртуальных серверов F5	32
7	Настройка Citrix ADC (NetScaler ADC)	34
	Настройка мониторов Citrix	34
	Настройка групп служб Citrix	37
	Настройка виртуальных серверов Citrix	38
8	Устранение неполадок	40

Ошибки в процессе установки vRealize Automation при использовании NSX-V в качестве подсистемы балансировки нагрузки для Workspace ONE	40
Сбои предоставления при использовании OneConnect с F5 BIG-IP	41
Лицензия F5 BIG-IP ограничивает пропускную способность сети	41

Балансировка нагрузки в vRealize Automation и vRealize Orchestrator

1

В этом документе описывается конфигурация балансировки нагрузки vRealize Automation и vRealize Orchestrator в распределенном кластерном развертывании с параметрами высокой доступности с помощью VMware NSX, F5 Networks BIG-IP (F5) и Citrix NetScaler.

Этот документ является руководством не по установке, а по настройке балансировки нагрузки, дополняющим документы по установке и настройке vRealize Automation и vRealize Orchestrator, доступные в [документации по продукту VMware vRealize Automation](#) и [документации по продукту VMware vRealize Orchestrator](#).

Эта информация предназначена для следующих продуктов и версий.

Таблица 1-1.

Продукт	Версия
NSX-T	2.4, 2.5, 3.0
NSX-V	6.2.x, 6.3.x, 6.4.x
F5 BIG-IP LTM	11.x, 12.x, 13.x, 14.x, 15.x
Citrix NetScaler ADC	10.5, 11.x, 12.x, 13.x
vRealize Automation	8.0, 8.1, 8.2
vRealize Orchestrator	8.0, 8.1

Дополнительные сведения см. в разделе [Таблицы совместимости продуктов VMware](#).

Основные принципы балансировки нагрузки

2

Подсистемы балансировки нагрузки распределяют нагрузку между серверами в развертываниях с высокой доступностью. Системный администратор регулярно создает резервные копии подсистем балансировки нагрузки одновременно с резервным копированием других компонентов.

При резервном копировании подсистем балансировки нагрузки следуйте политике своей организации с учетом сохранения топологии сети и планов резервного копирования продуктов VMware.

В эту главу входят следующие разделы:

- [Транзитный режим SSL](#)
- [Уведомления подсистемы балансировки нагрузки](#)
- [Топологии one-arm и multi-arm](#)

Транзитный режим SSL

Транзитный режим SSL используется с конфигурациями балансировки нагрузки.

Транзитный режим SSL используется по следующим причинам.

- Простота развертывания
 - За счет того, что в подсистеме балансировки нагрузки не требуется развертывать сертификаты vRealize Automation и vRealize Orchestrator, упрощается процесс развертывания.
- Отсутствие операционных издержек
 - В момент обновления сертификата в конфигурацию подсистемы балансировки нагрузки не требуется вносить изменения.
- Простота обмена данными
 - Отдельные имена узлов компонентов со сбалансированной нагрузкой соответствуют полю альтернативного имени субъекта в сертификатах, за счет чего упрощается обмен данными между клиентом и узлами с балансировкой нагрузки.

Уведомления подсистемы балансировки нагрузки

Рекомендуется включать уведомления при любом отключении узла vRealize Automation или vRealize Orchestrator в пуле серверов.

В VMware NSX Data Center можно включить уведомления при появлении оповещений в vRealize Operations Manager и vRealize Network Insight. См. документацию по vRealize Operations Manager и vRealize Network Insight.

Для NetScaler настройте специальные ловушки SNMP и диспетчер SNMP для отправки оповещений. Сведения о конфигурации SNMP см. в документации по NetScaler.

Чтобы настроить уведомление по электронной почте с помощью F5, используйте следующие методы.

- [Настройка системы BIG-IP для доставки создаваемых локально сообщений электронной почты](#)
- [Создание настраиваемых ловушек SNMP](#)
- [Настройка оповещений для отправки уведомлений по электронной почте](#)

Топологии one-arm и multi-arm

Развертывания типа one-arm и multi-arm по-разному маршрутизируют трафик подсистемы балансировки нагрузки.

В развертывании типа one-arm подсистема балансировки нагрузки физически не находится в канале трафика. Это значит, что входящий и исходящий трафик подсистемы балансировки нагрузки проходит через один и тот же сетевой интерфейс. Трафик с клиента проходит через подсистему балансировки нагрузки с преобразованием сетевых адресов (NAT), где подсистема балансировки нагрузки является исходным адресом. Узлы отправляют обратный трафик в подсистему балансировки нагрузки перед тем, как вернуть его в клиент. Без этого обратного потока пакетов обратный трафик будет пытаться достичь клиента напрямую, вызывая сбой подключения.

В конфигурации multi-arm трафик маршрутизируется через подсистему балансировки нагрузки. Как правило, для конечных устройств подсистема балансировки нагрузки является шлюзом по умолчанию.

Наиболее распространенным типом развертывания является конфигурация one-arm. Те же принципы применяются к развертываниям multi-arm. Оба типа работают с F5 и NetScaler.

В этом документе рассматривается развертывание компонентов vRealize Automation и vRealize Orchestrator в конфигурации one-arm. Развертывания multi-arm также поддерживаются, и их настройка почти аналогична описанной для конфигурации one-arm.

Конфигурация типа one-arm:



Предварительные условия для настройки подсистем балансировки нагрузки для vRealize Automation

3

Перед настройкой подсистем балансировки нагрузки должны быть выполнены следующие предварительные условия.

- NSX-V/T. Прежде чем начать реализацию высокой доступности для vRealize Automation или vRealize Orchestrator с использованием NSX-V/T в качестве подсистемы балансировки нагрузки, убедитесь, что настроена топология NSX-V/T и поддерживается соответствующая версия NSX-V/T. В этом документе рассматривается аспект конфигурации NSX-V/T, связанный с балансировкой нагрузки, и предполагается, что элемент NSX-V/T настроен и проверен для надлежащей работы в целевой среде и сетях. Чтобы убедиться, что используемая версия поддерживается, сверьтесь с [таблицей совместимости продукта](#).
- F5 BIG-IP LTM. Прежде чем начать реализацию высокой доступности для vRealize Automation и vRealize Orchestrator с использованием подсистемы балансировки нагрузки F5 LTM, убедитесь, что эта подсистема балансировки нагрузки установлена и лицензирована, а настройка DNS-сервера завершена.
- NetScaler. Прежде чем начать реализацию высокой доступности для vRealize Automation и vRealize Orchestrator с использованием подсистемы балансировки нагрузки NetScaler, убедитесь, что элемент NetScaler установлен и для него есть лицензия как минимум уровня Standard Edition.
- Сертификаты. Запросите сертификат, заверенный центром сертификации, в котором указано полное доменное имя подсистемы балансировки нагрузки и имена узлов кластера в разделе SubjectAltNames. Эта конфигурация позволяет подсистеме балансировки нагрузки обслуживать трафик без ошибок SSL.
- Поставщик удостоверений. Начиная с vRealize Automation 8.0, предпочтительным поставщиком удостоверений является решение Workspace ONE Access, которое развертывается отдельно от устройств и кластера vRealize Automation.

Подробную информацию об установке и настройке см. в документации по vRealize Automation на веб-сайте docs.vmware.com.

При необходимости для работы с системой vRealize Automation можно настроить внешний кластер vRealize Orchestrator. Это можно сделать после запуска системы vRealize Automation. При этом конфигурация vRealize Automation с высокой доступностью уже включает в себя встроенный кластер vRealize Orchestrator.

В эту главу входят следующие разделы:

- [Выполнение начальной установки vRealize Automation или vRealize Orchestrator](#)

Выполнение начальной установки vRealize Automation или vRealize Orchestrator

Перед выполнением начальной установки vRealize Automation или vRealize Orchestrator необходимо настроить подсистему балансировки нагрузки.

Во время процесса установки vRealize Automation или vRealize Orchestrator подсистема балансировки нагрузки, как правило, перенаправляет половину трафика на дополнительные узлы, которые еще не настроены, что приводит к сбою установки. Чтобы избежать этих ошибок и завершить начальную установку vRealize Automation или vRealize Orchestrator, необходимо выполнить следующие действия.

Процедура

1. Настройте подсистему балансировки нагрузки F5, NSX или NetScaler. См. разделы [Глава 6 Настройка F5 Big-IP LTM](#), [Глава 5 Настройка NSX-T](#) и [Глава 7 Настройка Citrix ADC \(NetScaler ADC\)](#).
2. Отключите мониторы работоспособности или временно измените их на ICMP по умолчанию и убедитесь, что трафик по-прежнему перенаправляется на основные узлы.
3. Отключите все дополнительные узлы от пулов подсистемы балансировки нагрузки.
4. Установите и настройте все компоненты системы, как описано в документации по установке и настройке vRealize Automation или vRealize Orchestrator.
5. После установки всех компонентов включите все дополнительные узлы в подсистеме балансировки нагрузки.
6. Настройте подсистему балансировки нагрузки, включив все мониторы проверки работоспособности.
После завершения этой процедуры обновите монитор, созданный на этапе [Настройка мониторов](#).
7. После установки убедитесь, что все узлы находятся в ожидаемом состоянии с включенным монитором работоспособности в подсистеме балансировки нагрузки. Пул, группы служб и виртуальный сервер узлов виртуального устройства должны быть доступны и запущены. Все узлы виртуальных устройств должны быть доступны, запущены и включены.

Настройка NSX-V

4

Можно развернуть новый шлюз служб NSX-V Edge или повторно использовать существующий. В любом случае он должен иметь сетевое подключение по направлению к компонентам vRealize, для которых выполняется балансировка нагрузки, и от них.

Примечание Чтобы настроить поставщика удостоверений с параметрами высокой доступности для vRealize Automation, см. документацию по балансировке нагрузки для [VMware Workspace ONE](#).

В эту главу входят следующие разделы:

- [Настройка глобальных параметров](#)
- [Настройка профилей приложений](#)
- [Настройка мониторинга служб](#)
- [Настройка пулов серверов](#)
- [Настройка виртуальных серверов](#)

Настройка глобальных параметров

Настройте глобальные параметры, выполнив следующие действия.

Процедура

1. Войдите в NSX-V, выберите **Диспетчер > Параметры, Интерфейсы**.
2. Выберите нужное устройство Edge из списка.
3. Щелкните **номер виртуального сетевого адаптера vNIC** внешнего интерфейса, в котором размещены виртуальные IP-адреса, и нажмите значок **Изменить**.

4. Выберите соответствующий сетевой диапазон для NSX-V Edge и нажмите значок **Изменить**.

Edit Interface | nic0

Basic Advanced

vNIC# 0

Name * nic0

Type ☐ Internal ☒ Uplink ☐ Trunk

Connected To * Prod-01

Connectivity Status ☒ Connected

Configure Subnets

+ ADD DELETE Search

<input type="checkbox"/>	Primary IP Address	Secondary IP Addresses	Subnet Prefix Length
<input type="checkbox"/>	192.168.208.102		24

1 items

CANCEL SAVE

5. Добавьте IP-адреса, назначенные виртуальным IP-адресам, и нажмите кнопку **Сохранить**.
6. Нажмите кнопку **ОК**, чтобы закрыть страницу настройки интерфейса.
7. Перейдите на вкладку **Подсистема балансировки нагрузки** и нажмите значок **Изменить**.
8. Установите при необходимости флажки **Включить подсистему балансировки нагрузки** и **Ведение журнала** и нажмите **Сохранить**.

Edit Load Balancer Global Configuration

Load Balancer ☒ Enable

Acceleration ☐ Disable

Logging ☒ Enable

Log Level

CANCEL SAVE

Настройка профилей приложений

Необходимо добавить профили приложений для vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

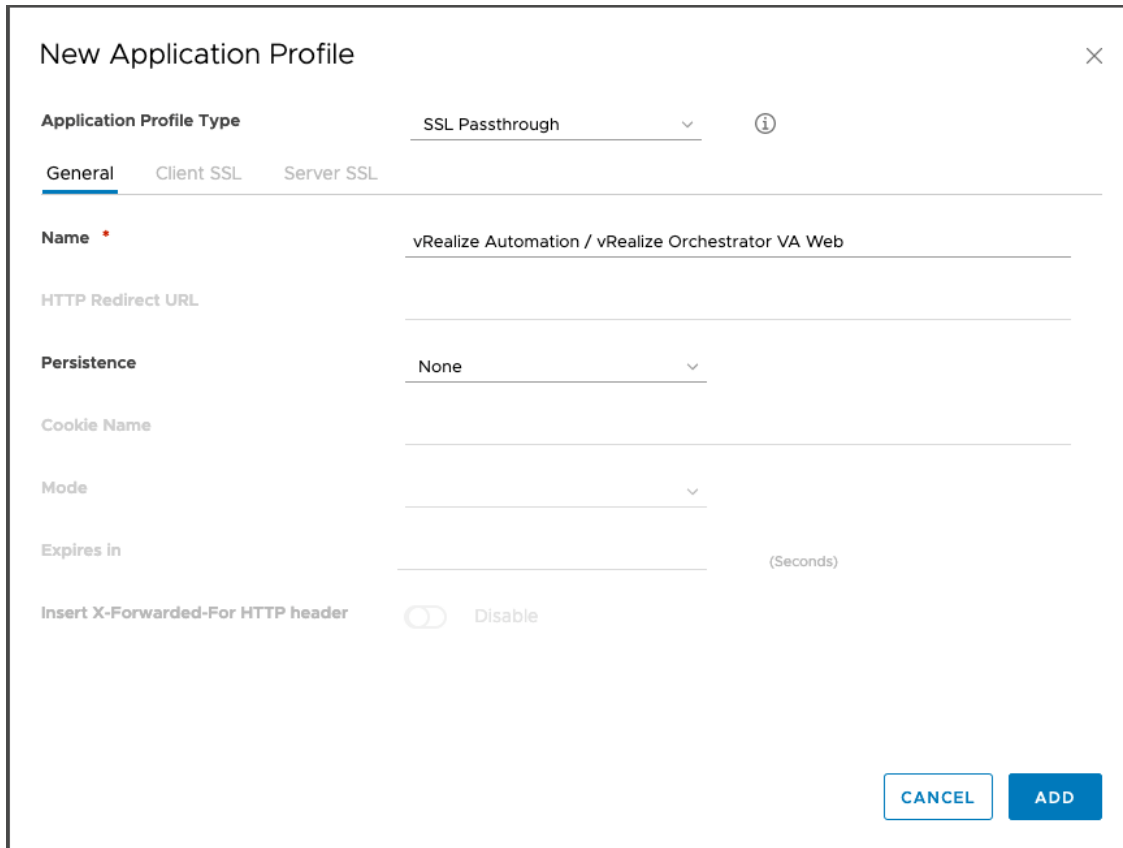
1. Щелкните **Профили приложений** на левой панели.
2. Щелкните значок **Добавить**, чтобы создать профили приложений, необходимые для данного продукта, в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 4-1. Профили приложений

Имя	Тип	Устойчивость	Срок действия истекает через
vRealize Automation	Транзитный режим SSL	Нет	Нет
vRealize Orchestrator	Транзитный режим SSL	Нет	Нет
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.			

Результаты

Конфигурация должна соответствовать следующему изображению:



New Application Profile [X]

Application Profile Type SSL Passthrough ⓘ

General Client SSL Server SSL

Name * vRealize Automation / vRealize Orchestrator VA Web

HTTP Redirect URL

Persistence None

Cookie Name

Mode

Expires in (Seconds)

Insert X-Forwarded-For HTTP header ☐ Disable

CANCEL **ADD**

Настройка мониторинга служб

Необходимо добавить мониторы служб для экземпляра vRealize Automation и внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. На левой панели нажмите **Мониторинг службы**.

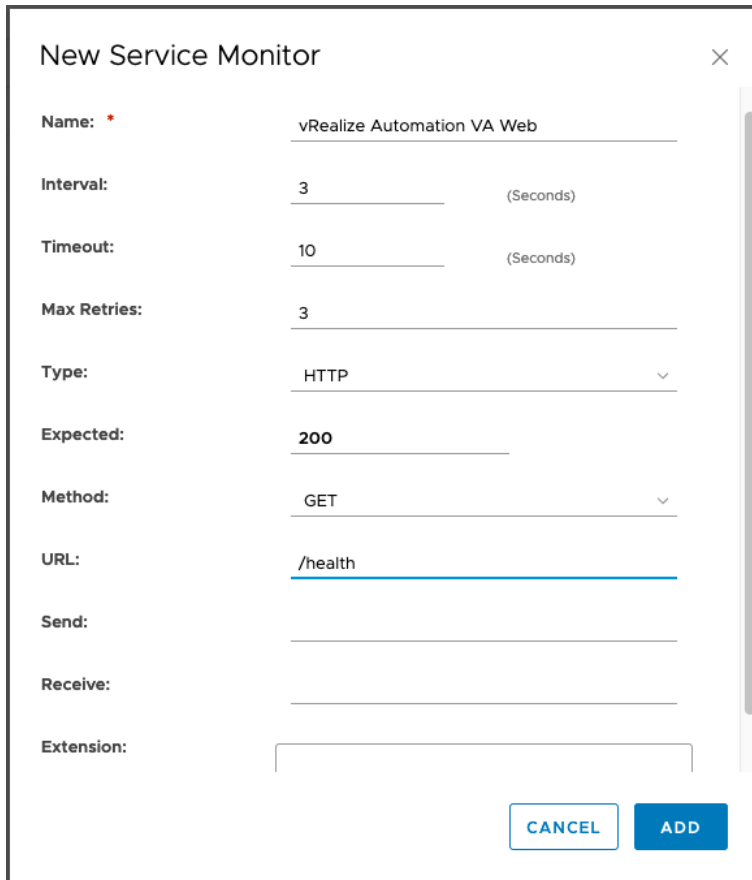
2. Нажмите значок **Добавить**, чтобы создать мониторы службы, необходимые для данного продукта, в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 4-2. Мониторинг службы

Имя	Интервал	Время ожидания	Количество попыток	Тип	Метод	URL-адрес	Получение	Ожидается
vRealize Automation	3	10	3	HTTP	GET	/health		200
vRealize Orchestrator	3	10	3	HTTP	GET	/health		200
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.								

Результаты

Конфигурация должна соответствовать следующему изображению:



New Service Monitor [X]

Name: * vRealize Automation VA Web

Interval: 3 (Seconds)

Timeout: 10 (Seconds)

Max Retries: 3

Type: HTTP

Expected: 200

Method: GET

URL: /health

Send:

Receive:

Extension:

CANCEL **ADD**

Настройка пулов серверов

Необходимо создать пулы серверов для экземпляра vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. На левой панели выберите **Пулы**.

2. Нажмите значок **Добавить**, чтобы создать пулы, необходимые для данного продукта, в соответствии с приведенной ниже таблицей.

Таблица 4-3. Пулы серверов

Имя пула	Алгоритм	Мониторы	Имя участника	IP-адрес или контейнер vCenter	Порт	Порт монитора
vRealize Automation	Минимальное число подключений	vRealize Automation	VA1 VA2 VA	IP-адрес	443	8008
vRealize Orchestrator	Минимальное число подключений	vRealize Orchestrator	VA1 VA2 VA3	IP-адрес	443	8008

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

Результаты

Конфигурация должна соответствовать следующему изображению:

New Pool

General

Members

+ ADD

EDIT

DELETE

	Name	IP Address / VC Container	Weight	Monitor Port	Port	Max Connections	Min Connections
<input type="radio"/>	vRA_VA_1	10.10.10.10	1	8008	443		
<input type="radio"/>	vRA_VA_3	10.10.10.12	1	8008	443		
<input type="radio"/>	vRA_VA_2	10.10.10.11	1	8008	443		

1 - 3 of 3 items

CANCEL

ADD

Настройка виртуальных серверов

Необходимо настроить виртуальные серверы для vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. На левой панели выберите **Виртуальные серверы**.
2. Нажмите значок **Добавить**, чтобы создать виртуальные серверы, необходимые для другого продукта, в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значения по умолчанию.

Таблица 4-4. Виртуальные серверы

Имя	Ускорение	IP-адрес	Протокол	Порт	Пул по умолчанию	Профиль приложения		
vRealize Automation	Отключено	IP-адрес	HTTPS	443	vRealize Automation	vRealize Automation		
vRealize Orchestrator	Отключено	IP-адрес	HTTPS	443	vRealize Orchestrator	vRealize Orchestrator		
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.								

Результаты

Конфигурация должна соответствовать следующему изображению.

New Virtual Server

Virtual Server *

☒ Enable

Acceleration *

☐ Disable

Application Profile:

vRealize Automation VA Web

Name: *

vs_vra-va-web_443

Description:

IP Address: *

10.10.10.8

Select IP Address

Protocol:

HTTPS

Port / Port Range: *

443

e.g.: 9000,9010-9020

Default Pool:

pool_vra-va-web_443

CANCEL

ADD

Настройка NSX-T

5

Перед настройкой NSX-T необходимо развернуть в среде, а шлюз уровня 1 с подсистемой балансировки нагрузки должен иметь доступ к компонентам vRealize по сети.

Примечание Чтобы настроить поставщика удостоверений с параметрами высокой доступности для vRealize Automation, см. документацию по балансировке нагрузки для [VMware Workspace ONE](#).

Примечание NSX-T версии 2.3 не поддерживает монитор HTTPS для пула виртуальных серверов FAST TCP. Монитор HTTPS поддерживается для NSX-T версии 2.4 и выше.

В эту главу входят следующие разделы:

- [Настройка профилей приложений NSX-T](#)
- [Настройка активного монитора работоспособности NSX-T](#)
- [Настройка пулов серверов NSX-T](#)
- [Настройка виртуальных серверов NSX-T](#)
- [Настройка подсистемы балансировки нагрузки](#)
- [Добавление виртуальных серверов в подсистему балансировки нагрузки](#)

Настройка профилей приложений NSX-T

В NSX-T можно добавить профиль приложения для запросов HTTPS.

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Профили**.
2. Выберите **Приложение** в качестве типа профиля.
3. Щелкните **Добавить профиль приложения** и выберите **Профиль Fast TCP**.
4. Введите имя профиля.

Результаты

Готовый профиль приложения для запроса HTTPS должен соответствовать следующему изображению.

The screenshot shows the 'PROFILES' tab in the vRealize Automation interface. Under 'Select Profile Type', 'APPLICATION' is selected. A button 'ADD APPLICATION PROFILE' is visible. Below is a table with columns: Name, Type, Idle Timeout (sec), and HA Flow Mirroring. The first row shows a profile named 'vRA_HTTPS' with Type 'Fast TCP' and Idle Timeout '1800'. The 'HA Flow Mirroring' toggle is 'Disabled'. Below the table, there are fields for 'Description' (with placeholder 'Enter Description'), 'Tags' (with 'Tag (Required)' and 'Scope (Optional)' sub-fields), and a 'Connection Close Timeout' field set to '8'. A note states 'Maximum 30 tags are allowed.' At the bottom are 'SAVE' and 'CANCEL' buttons.

Name	Type	Idle Timeout (sec)	HA Flow Mirroring
vRA_HTTPS	Fast TCP	1800	Disabled

Description: Enter Description

Tags: Tag (Required) Scope (Optional) ✓
Maximum 30 tags are allowed.

Connection Close Timeout: 8

SAVE CANCEL

Настройка активного монитора работоспособности NSX-T

Чтобы настроить активный монитор работоспособности для NSX-T, выполните следующие действия.

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Мониторы**.
2. Щелкните **Добавить активный монитор** и выберите **HTTP**.
3. Введите имя монитора работоспособности.

4. Настройте монитор работоспособности в соответствии с приведенной ниже таблицей:

Таблица 5-1. Настройка монитора работоспособности

Имя	Порт мониторинга	Интервал	Время ожидания	Счетчик падений	Тип	Метод	URL-адрес	Код ответа	Текст ответа
vRealize Automation	8008	3	10	3	HTTP	GET	/health	200	Нет
vRealize Orchestrator	8008	3	10	3	HTTP	GET	/health	200	Нет

Примечание
Используйте только для внешних экземпляров в vRealize Orchestrator.

Результаты

Конфигурация должна соответствовать следующему изображению.

The screenshot shows the 'MONITORS' tab in the vRealize Automation interface. A dialog box for adding an active monitor is displayed. The monitor is named 'vRealize Automation VA' and is configured with the following settings:

- Name:** vRealize Automation VA
- Protocol:** HTTP
- Monitoring Port:** 8008
- Monitoring Interval:** 3
- Timeout Period (sec):** 10
- Description:** Enter Description
- Fall Count:** 3
- Rise Count:** 3
- Tags:** Tag (Required), Scope (Optional), with a note 'Maximum 30 tags are allowed.'
- Additional Properties:**
 - HTTP Request:** Configure
 - HTTP Response:** Configure

At the bottom of the dialog are 'SAVE' and 'CANCEL' buttons.

HTTP Request and Response Configuration ×

Active Health Monitor -


HTTP Request Configuration HTTP Response Configuration

HTTP Method Get ▼

HTTP Request URL /health

HTTP Request Version 1.1 ▼

ADD

Header Name	Header Value
 Request Header not found	

HTTP Request Body

CANCEL

APPLY

HTTP Request and Response Configuration ×

Active Health Monitor -

HTTP Request Configuration HTTP Response Configuration

HTTP Response Code 200 ×

1 or more response codes

HTTP Response Body

Настройка пулов серверов NSX-T

Необходимо настроить пулы серверов для экземпляра vRealize Automation и внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Пулы серверов**.
2. Щелкните **Добавить пул серверов**.
3. Введите имя пула.
4. Настройте пул в соответствии с приведенной ниже таблицей:

Таблица 5-2. Настройка пулов серверов

Имя пула	Алгоритм	Активный монитор	Имя	IP-адрес	Порт
vRealize Automation	Минимальное число подключений	vRealize Automation	VA1 VA2 VA3	IP-адрес	443
vRealize Orchestrator	Минимальное число подключений	vRealize Orchestrator	VA1 VA2 VA3	IP-адрес	443

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

Результаты

Конфигурация должна соответствовать следующему изображению.

LOAD BALANCERS VIRTUAL SERVERS **SERVER POOLS** PROFILES MONITORS • About

ADD SERVER POOL

Name	Algorithm	Members/Group	Virtual Servers
pool_vra-va-web_443 *	Least Contr ▾	Select Members	

Description: Enter Description

SNAT Translation Mode: Automap ▾

> Additional Properties

SAVE CANCEL

Active Monitor: vra_htt

Configure Server Pool Members

Server Pool - pool_iaas-manager_443

☒ Enter individual members ☐ Select a group

ADD MEMBER

Search

Name	IP	Port	Weight	State	Backup Member	Max Concurrent Connections
		443	1	Enabled	● Disabled	
		443	1	Enabled	● Disabled	

CANCEL APPLY

Настройка виртуальных серверов NSX-T

Необходимо настроить виртуальные серверы для vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Виртуальные серверы**.
2. Щелкните **Добавить виртуальный сервер** и выберите **Уровень**.

3. Настройте виртуальные серверы в соответствии с приведенной ниже таблицей.

Таблица 5-3. Настройка виртуальных серверов

Имя	Тип	Профиль приложения	IP-адрес	Порт	Пул серверов	Профиль устойчивости
vRealize Automation	TCP уровня L4	vRealize Automation	IP-адрес	443	vRealize Automation	Нет
vRealize Orchestrator	TCP уровня L4	vRealize Orchestrator	IP-адрес	443	vRealize Orchestrator	Нет

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

Результаты

Конфигурация должна соответствовать следующему изображению.

The screenshot displays the 'VIRTUAL SERVERS' configuration page in the vRealize Automation interface. A table at the top lists the virtual server configuration:

Name	IP Address	Ports	Type	Load Balancer	Server Pool
vs_vra-va-web_443	10.10.10.10	443	L4 TCP	r34r3r4	pool_...

Below the table, the configuration details for the selected virtual server are shown:

- Description:** Enter Description
- Persistence:** Disabled
- Additional Properties:**
 - Max Concurrent Connections:** Unlimited
 - Max New Connection Rate:** Unlimited
 - Default Pool Member Ports:** 443
 - Access Log:** Disabled
- Admin State:** Enabled
- Tags:** Tag (Required), Scope (Optional)

Buttons for 'SAVE' and 'CANCEL' are located at the bottom left.

Настройка подсистемы балансировки нагрузки

Укажите подсистему балансировки нагрузки для каждого экземпляра vRealize Automation и внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Подсистемы балансировки нагрузки**.
2. Нажмите **Добавить подсистему балансировки нагрузки**.
3. Введите имя и выберите подходящий **размер подсистемы балансировки нагрузки** (зависит от размера кластера vRealize Automation).
4. Выберите **Логический маршрутизатор уровня 1**.

Примечание В NSX-T версии 2.4 проверки работоспособности монитора выполняются с использованием IP-адреса канала исходящей связи уровня 1 (или первого порта службы для автономного SR уровня 1) для всех пулов серверов подсистемы балансировки нагрузки. Убедитесь, что пулы серверов доступны с этого IP-адреса.

Результаты

Конфигурация должна соответствовать следующему изображению:

The screenshot displays the 'LOAD BALANCERS' section in the vRealize Automation interface. A table lists the configured load balancers. The first entry is 'vra75_lb' with a size of 'Small' and a 'Tier-1 Gateway' of 'vRA-LB-Tier-1-Router'. Below the table, the configuration details for 'vra75_lb' are shown, including a description field, tags, and the admin state, which is currently turned on.

Name	Size	Tier-1 Gateway	Virtual Servers
vra75_lb	Small	vRA-LB-Tier-1-Router	

Configuration details for vra75_lb:

- Description:** Enter Description
- Tags:** Tag (Required), Scope (Optional). Maximum 30 tags are allowed.
- Error Log Level:** Info
- Admin State:** On

Buttons: **SAVE**, **CANCEL**

Добавление виртуальных серверов в подсистему балансировки нагрузки

После настройки подсистемы балансировки нагрузки можно добавить виртуальные серверы.

Процедура

1. Перейдите в раздел **Сетевые подключения > Балансировка нагрузки > Виртуальные серверы**.
2. Измените настроенные виртуальные серверы.
3. Назначьте ранее настроенную подсистему балансировки нагрузки в качестве элемента **Подсистема балансировки нагрузки**.

Результаты

Конфигурация должна соответствовать следующему изображению:

Name	IP Address	Ports	Type	Load Balancer	Server
vs_vra-va-web_443 *	192.168.205.10 * <small>e.g. 10.10.10.10</small>	443 x <small>Enter Ports or Port Rang</small>	L4 TCP	vRA_LB (x) v	p
Description		Enter Description		Application Profile *	vRA_HTTPS
Persistence		Disabled v			
> Additional Properties					
<div>SAVE</div> <div>CANCEL</div>					

Настройка F5 Big-IP LTM

6

Прежде чем настраивать устройство F5, необходимо развернуть его в среде с доступом к компонентам vRealize по сети.

Примечание Чтобы настроить поставщика удостоверений с параметрами высокой доступности для vRealize Automation, см. документацию по балансировке нагрузки для [Workspace ONE](#).

Для настройки устройство F5 должно соответствовать следующим требованиям.

- Устройство F5 может быть либо физическим, либо виртуальным.
- Подсистему балансировки нагрузки модуля локального трафика F5 (LTM) можно развернуть в топологиях типа one-arm или multi-arm.
- LTM должен быть настроен и лицензирован как номинальный, минимальный или выделенный. Чтобы настроить LTM, перейдите в раздел **Система > Предоставление ресурсов**.

Если используется F5 LTM до версии 11.x, возможно, потребуется изменить параметры монитора работоспособности, связанные с отправляемой строкой. Дополнительные сведения о том, как настроить отправляемую строку монитора работоспособности для различных версий F5 LTM, см. в разделе [Сбои проверок работоспособности по HTTP могут происходить даже при правильном ответе узла](#).

В эту главу входят следующие разделы:

- [Настройка мониторов](#)
- [Настройка пулов серверов F5](#)
- [Настройка виртуальных серверов F5](#)

Настройка мониторов

Необходимо добавить мониторы для экземпляра vRealize Automation и внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Войдите в подсистему балансировки нагрузки F5 и перейдите в раздел **Локальный трафик > Монитор**.

2. Нажмите кнопку **Создать** и настройте монитор в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 6-1. Настройка мониторов

Имя	Тип	Интервал	Время ожидания	Отправляемая строка.	Получаемая строка.	Порт службы псевдонимов
vRealize Automation	HTTP	3	10	GET /health HTTP/1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
vRealize Orchestrator	HTTP	3	10	GET /health HTTP/1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.						

Результаты

Конфигурация должна соответствовать следующему изображению.

Local Traffic » Monitors » **New Monitor...**

General Properties

Name	vra_http_va_web
Description	
Type	HTTP
Parent Monitor	http

Configuration: Basic

Interval	3 seconds
Timeout	10 seconds
Send String	GET /health HTTP/1.0\r\n\r\n
Receive String	HTTP/1\.(0 1) (200)
Receive Disable String	
User Name	
Password	
Reverse	<input type="radio"/> Yes <input checked="" type="radio"/> No
Transparent	<input type="radio"/> Yes <input checked="" type="radio"/> No
Alias Address	* All Addresses
Alias Service Port	8008 Other: <input type="text"/>
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat Finished

Настройка пулов серверов F5

Необходимо настроить пулы служб для vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Войдите в подсистему балансировки нагрузки F5 и перейдите в раздел **Локальный трафик > Пулы**.

2. Нажмите кнопку **Создать** и настройте пул в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 6-2. Настройка пулов серверов

Имя	Мониторы работоспособности	Метод балансировки нагрузки	Имя узла	Адрес	Порт службы
vRealize Automation	vRealize Automation	Минимальное число подключений (участник)	VA1 VA2 VA3	IP-адрес	443
vRealize Orchestrator	vRealize Orchestrator	Минимальное число подключений (участник)	VA1 VA2 VA3	IP-адрес	443

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

3. Каждый участник пула должен вводиться как **Новый узел** и добавляться в группу **Новые участники**.

Результаты

Конфигурация должна соответствовать следующему изображению.

Local Traffic » Pools : Pool List » **pl_vra-va-00_443**

⚙ Properties Members Statistics

Load Balancing

Load Balancing Method: Least Connections (member)

Priority Group Activation: Disabled

Update

Current Members

<input checked="" type="checkbox"/>	<input type="checkbox"/> Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group
<input type="checkbox"/>		dz-vra8-node1.sof-mbu.eng.vmware.com:443	192.168.10.30	443		No	1	0 (Active)
<input type="checkbox"/>		dz-vra8-node2.sof-mbu.eng.vmware.com:443	192.168.10.31	443		No	1	0 (Active)
<input type="checkbox"/>		dz-vra8-node3.sof-mbu.eng.vmware.com:443	192.168.10.32	443		No	1	0 (Active)

Enable Disable Force Offline Remove

Настройка виртуальных серверов F5

Необходимо настроить виртуальные серверы для vRealize Automation и для внешнего экземпляра vRealize Orchestrator (необязательно).

Процедура

1. Войдите в подсистему балансировки нагрузки F5 и перейдите в раздел **Локальный трафик > Виртуальные серверы**.
2. Нажмите кнопку **Создать** и настройте виртуальный сервер в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 6-3. Настройка виртуальных серверов

Имя	Тип	Адрес назначения	Порт службы	Преобразование адреса источника	Пул по умолчанию	Профиль устойчивости по умолчанию
vRealize Automation	Производительность (уровень 4)	IP-адрес	443	Автоматическое сопоставление	vRealize Automation	Нет
vRealize Orchestrator	Производительность (уровень 4)	IP-адрес	443	Автоматическое сопоставление	vRealize Orchestrator	Нет

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

3. Для просмотра общих сведений и данных о состоянии виртуальных серверов выберите **Локальный трафик > Виртуальные серверы**.

Результаты

Конфигурация должна соответствовать следующему изображению:

General Properties

Name

vs_vra-va-00_443

Description

Type

Performance (Layer 4)

Source Address

Host

Address List

Destination Address/Mask

Host

Address List

192.168.10.33

Service Port

Port

Port List

443

HTTPS

Notify Status to Virtual Address

☒

State

Enabled

Configuration: Basic

Protocol

TCP

Protocol Profile (Client)

fastL4

HTTP Profile (Client)

None

HTTP Profile (Server)

(Use Client Profile)

HTTP Proxy Connect Profile

None

VLAN and Tunnel Traffic

All VLANs and Tunnels

Source Address Translation

Auto Map

Acceleration: Basic

iSession Profile

None

Rate Class

None

Resources

iRules

Enabled

<<

>>

Up

Down

Available

/Common

_sys_APM_ExchangeSupport_OA_BasicAuth

_sys_APM_ExchangeSupport_OA_NtimAuth

_sys_APM_ExchangeSupport_helper

_sys_APM_ExchangeSupport_main

Default Pool

+ pl_vra-va-00_443

Default Persistence Profile

None

Fallback Persistence Profile

None

Cancel

Repeat

Finished

vs_vra-va-00_443

STATS DIAGRAM

☐ List other virtual servers that share these pools ☐ List other pools that use these nodes

Virtual Server

Pools

Pool Members

vs_vra-va-00_443
192.168.10.33:443

pl_vra-va-00_443

dz-vra8-node1.sof-mbu.er
192.168.10.30
dz-vra8-node2.sof-mbu.er
192.168.10.31
dz-vra8-node3.sof-mbu.er
192.168.10.32

Настройка Citrix ADC (NetScaler ADC)

7

Перед настройкой Citrix ADC убедитесь, что устройство NetScaler развернуто в среде с доступом к компонентам vRealize.

Для настройки решение ADC Citrix должно соответствовать следующим требованиям.

- Можно использовать виртуальный или физический NetScaler.
- Подсистема балансировки нагрузки Citrix может быть развернута в топологиях типа one-arm (трафик не идет через подсистему балансировки нагрузки) или multi-arm (трафик идет через подсистему балансировки нагрузки).
- Включите подсистему балансировки нагрузки и модули SSL. Для этого перейдите в раздел **NetScaler > Система > Параметры > Настроить > Основные компоненты**.

В эту главу входят следующие разделы:

- [Настройка мониторов Citrix](#)
- [Настройка групп служб Citrix](#)
- [Настройка виртуальных серверов Citrix](#)

Настройка мониторов Citrix

Для настройки монитора Citrix следует выполнить следующие действия.

Процедура

1. Войдите в подсистему балансировки нагрузки NetScaler и перейдите в раздел **NetScaler > Управление трафиком > Балансировка нагрузки > Мониторы**.

2. Нажмите кнопку **Добавить** и настройте монитор в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 7-1. Настройка мониторов Citrix

Имя	Тип	Интервал	Время ожидания	Количество попыток	Успешных попыток	HTTP-запрос/строка отправки	Коды ответа	Строка получения	Порт назнач.	Защищенный
vRealize Automation	HTTP	5	4	3	1	GET / health	200	Нет	8008	Нет
vRealize Orchestrator	HTTP	5	4	3	1	GET / health	200	Нет	8008	Нет
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.										

Результаты

Конфигурация должна соответствовать следующему изображению.

← Create Monitor

Name*

vra_https_va_web

Type*

HTTP

>

Basic Parameters

Interval

5

Second

Response Time-out

4

Second

Response Codes

+

200

x

Custom Header

HTTP Request

GET /health

☐ Secure

Advanced Parameters

Destination IP

Destination Port

8008

Down Time

30

Second

TROFS Code

TROFS String

Dynamic Time-out

Deviation

Second

Dynamic Interval

Retries

3

Настройка групп служб Citrix

Для настройки групп служб выполните следующие действия.

Процедура

1. Войдите в подсистему балансировки нагрузки NetScaler и перейдите в раздел **NetScaler > Управление трафиком > Балансировка нагрузки > Группы служб**.
2. Нажмите кнопку **Добавить** и настройте группы служб в соответствии с приведенной ниже таблицей.

Таблица 7-2. Настройка групп служб

Имя	Мониторы работоспособности	Протокол	Участники групп служб	Адрес	Порт
vRealize Automation	vRealize Automation	Мост SSL	VA1 VA2 VA3	IP-адрес	443
vRealize Orchestrator	vRealize Orchestrator	Мост SSL	VA1 VA2 VA3	IP-адрес	443
Примечание Используйте только для внешних экземпляров vRealize Orchestrator.					

Результаты

Конфигурация должна соответствовать следующему изображению:

← Load Balancing Service Group

Basic Settings			
Name	pl_vra-va-00_443	Cache Type	SERVER
Protocol	SSL_BRIDGE	Cacheable	NO
State	ENABLED	Health Monitoring	YES
Effective State	● UP	AppFlow Logging	ENABLED
Traffic Domain	0	Monitoring Connection Close Bit	NONE
Comment		Number of Active Connections	0
		AutoScale Mode	DISABLED

Service Group Members	
3 Service Group Members	>

Settings			
SureConnect		Use Client IP	NO
Surge Protection	OFF	Client Keep-alive	NO
Use Proxy Port	YES	TCP Buffering	YES
Down State Flush	ENABLED	Client IP	DISABLED
		Header	
		AutoScale Mode	DISABLED

Monitors	
1 Service Group to Monitor Binding	>

Done

Настройка виртуальных серверов Citrix

Для настройки виртуальных серверов выполните следующие действия.

Процедура

1. Войдите в подсистему балансировки нагрузки NetScaler и перейдите в раздел **NetScaler > Управление трафиком > Балансировка нагрузки > Виртуальные серверы**.

2. Нажмите кнопку **Добавить** и настройте виртуальный сервер в соответствии с приведенной ниже таблицей. Если ничего не указано, используйте значение по умолчанию.

Таблица 7-3. Настройка виртуальных серверов

Имя	Протокол	Адрес назначения	Порт	Метод балансировки нагрузки	Привязка групп служб
vRealize Automation	Мост SSL	IP-адрес	443	Минимальное число подключений	vRealize Automation
vRealize Orchestrator	Мост SSL	IP-адрес	443	Минимальное число подключений	vRealize Orchestrator

Примечание
Используйте только для внешних экземпляров vRealize Orchestrator.

Результаты

Конфигурация должна соответствовать следующему изображению:

← Load Balancing Virtual Server

Load Balancing Virtual Server | [Export as a Template](#)

Basic Settings

Name

vs_vra-va-00_443

Protocol

SSL_BRIDGE

State

● UP

IP Address

10.71.226.23

Port

443

Traffic Domain

0

Listen Priority

-

Listen Policy Expression

NONE

Redirection Mode

IP

Range

1

IPset

-

RHI State

PASSIVE

AppFlow Logging

ENABLED

Retain Connections on Cluster

NO

Services and Service Groups

No Load Balancing Virtual Server Service Binding

1 Load Balancing Virtual Server ServiceGroup Binding

Traffic Settings

Health Threshold

0

Client Idle Time-out

180

Minimum Autoscale Members

0

Maximum Autoscale Members

0

ICMP Virtual Server Response

PASSIVE

Priority Queuing

Sure Connect

Down State Flush

ENABLED

Layer 2 Parameters

OFF

Trofs Persistence

ENABLED

Done

Устранение неполадок

8

В эту главу входят следующие разделы:

- Ошибки в процессе установки vRealize Automation при использовании NSX-V в качестве подсистемы балансировки нагрузки для Workspace ONE
- Сбои предоставления при использовании OneConnect с F5 BIG-IP
- Лицензия F5 BIG-IP ограничивает пропускную способность сети

Ошибки в процессе установки vRealize Automation при использовании NSX-V в качестве подсистемы балансировки нагрузки для Workspace ONE

Если в процессе установки vRealize Automation при использовании Workspace ONE в качестве подсистемы балансировки нагрузки возникают ошибки, выполните следующие действия для их устранения.

При использовании NSX-V в качестве подсистемы балансировки нагрузки для VMware Workspace ONE могут существовать определенные сетевые ограничения, которые приводят к ошибкам и превышению времени ожидания в процессе установки vRealize Automation, например:

```
2020-06-30 09:10:08.751+0000 INFO 16 --- [or-http-epoll-3]
com.vmware.identity.rest.RestClient : POST https://default-49-29.sqa.local/SAAS/API/1.0/oauth2/token?
grant_type=client_credentials
2020-06-30 09:10:08.755+0000 WARN 16 --- [or-http-epoll-3]
r.netty.http.client.HttpClientConnect : [id: 0x754860c7, L:/10.244.0.206:48686 !
R:default-49-29.sqa.local/10.198.49.29:443] The connection observed an error
reactor.netty.http.client.PrematureCloseException: Connection prematurely closed BEFORE response
```

Эти ошибки можно обойти, увеличив тайм-аут простоя подключения NSX-V до 5 минут вместо значения по умолчанию (1 сек.).

Сделать это можно с помощью правила приложения, содержащего следующие параметры.

```
timeout http-keep-alive 300s
```


Сбои предоставления при использовании OneConnect с F5 BIG-IP

При использовании компонента OneConnect с F5 BIG-IP в качестве виртуального сервера задачи предоставления иногда завершаются сбоем.

OneConnect обеспечивает мультиплексирование и повторное использование подключений подсистемы балансировки нагрузки к конечным серверам. Это снижает нагрузку на серверы и делает их более устойчивыми.

Использовать OneConnect с виртуальным сервером, на котором настроен транзитный режим SSL, не рекомендуется F5 и может приводить к ошибкам при попытке предоставления. Это происходит потому, что подсистема балансировки нагрузки пытается начать новый сеанс SSL во время существующего сеанса, а конечный сервер ожидает, что клиент закроет или возобновит существующий сеанс. Из-за этого происходит потеря подключения. Отключите OneConnect, чтобы устранить эту проблему.

1. Войдите в подсистему балансировки нагрузки F5 и перейдите в раздел **Локальный трафик > Виртуальные серверы > Список виртуальных серверов**.
2. Щелкните имя виртуального сервера, который требуется изменить.
3. В разделе **Ускорение** выберите **Нет** для **профиля OneConnect**.
4. Нажмите **Готово**.

Лицензия F5 BIG-IP ограничивает пропускную способность сети

Если сетевой трафик подсистемы балансировки нагрузки превышает лимит, предусмотренный лицензией F5 BIG-IP, возможно возникновение сбоев при предоставлении или проблем при загрузке страниц консоли vRealize Automation.

Как проверить, возникает ли эта проблема на платформе BIG-IP, описано в разделе [Механизм принудительного ограничения пропускной способности системой BIG-IP VE до предусмотренного лицензией](#).