

Lastausgleichshandbuch für vRealize Automation 8.1

14. April 2020.
vRealize Automation 8.1



vmware®

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese an:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Copyright © 2020 VMware, Inc. Alle Rechte vorbehalten. [Urheberrechts- und Markenhinweise](#).

Inhalt

- 1 Lastausgleich für vRealize Automation 8.0 5**
- 2 Lastausgleichskonzepte 6**
 - SSL-Passthrough 6
 - E-Mail-Benachrichtigungen für den Lastausgleichsdienst 7
 - Einarmige und mehrarmige Topologien 7
- 3 Voraussetzungen für die Konfiguration von Lastausgleichsdiensten für vRealize Automation 9**
 - Beenden der Erstinstallation 10
- 4 Konfigurieren von NSX-V 11**
 - Konfigurieren der globalen Einstellungen 11
 - Konfigurieren von Anwendungsprofilen 13
 - Konfigurieren der Dienstüberwachung 14
 - Konfigurieren von Serverpools 16
 - Konfigurieren von virtuellen Servern 18
- 5 Konfigurieren von NSX-T 20**
 - Konfigurieren von NSX-T-Anwendungsprofilen 20
 - Konfigurieren des Persistenzprofils für Workspace ONE Access 21
 - Konfigurieren der aktiven NSX-T-Integritätsüberwachung 21
 - Konfigurieren von NSX-T Serverpools 24
 - Konfigurieren von virtuellen NSX-T-Servern 25
 - Konfigurieren des Lastausgleichsdiensts 27
 - Hinzufügen von virtuellen Servern zum Lastausgleichsdienst 27
- 6 Konfigurieren von F5 BIG-IP LTM 29**
 - Konfigurieren des benutzerdefinierten Persistenzprofils für Workspace ONE Access 29
 - Konfigurieren von Überwachungen 30
 - Konfigurieren von F5-Serverpools 31
 - Konfigurieren von virtuellen F5-Servern 33
- 7 Konfigurieren von Citrix ADC (NetScaler ADC) 35**
 - Konfigurieren von Citrix-Überwachungen 35
 - Konfigurieren von Citrix-Dienstgruppen 38
 - Konfigurieren von virtuellen Citrix-Servern 39
 - Konfigurieren der Persistenzgruppe für Workspace ONE Access 41

8 Fehlerbehebung 42

[Bereitstellungsfehler bei der Verwendung von OneConnect mit F5 BIG-IP](#) 42

[F5 BIG-IP-Lizenzgrenzwerte für die Netzwerkbandbreite](#) 42

Lastausgleich für vRealize Automation 8.0

1

In diesem Dokument wird die Konfiguration der Lastausgleichsmodule von F5 Networks BIG IP Software (F5), Citrix NetScaler und NSX Load Balancer für vRealize Automation, vRealize Orchestrator und Workspace ONE Access in einer verteilten und hochverfügbaren Bereitstellung beschrieben.

In diesem Dokument handelt es sich nicht um ein Installationshandbuch, sondern um einen Konfigurationsleitfaden für den Lastausgleich, der die Installations- und Konfigurationsdokumentation für vRealize Automation und vRealize Orchestrator in der [VMware vRealize Automation-Produktdokumentation](#) und [VMware vRealize Orchestrator-Produktdokumentation](#) ergänzt.

Diese Informationen sind für die folgenden Produkte und Versionen vorgesehen.

Tabelle 1-1.

Produkt	Version
F5 BIG-IP LTM	11.x, 12.x, 13.x, 14.x, 15.x
NSX-V	6.2 x, 6.3.x, 6.4.x (weitere Informationen finden Sie in den VMware-Produktinteroperabilitätstabellen)
NSX-T	2,4
Citrix NetScaler ADC	10.5, 11.x, 12.x, 13.x
vRealize Automation	8.0
vRealize Orchestrator	8.0
Workspace ONE Access (früher VMware Identity Manager)	3.3.1

Weitere Informationen finden Sie in den [VMware-Interoperabilitätstabellen](#).

Lastausgleichskonzepte

2

Lastausgleichsdienste verteilen in Bereitstellungen mit Hochverfügbarkeit die Arbeitslast auf die Server. Der Systemadministrator sichert die Lastausgleichsdienste regelmäßig zusammen mit anderen Komponenten.

Halten Sie sich beim Sichern der Lastausgleichsdienste an Ihre Standortrichtlinien und achten Sie darauf, dass die Netzwerktopologie und der Sicherungsplan für VMware-Produkte eingehalten werden.

Dieses Kapitel enthält die folgenden Themen:

- [SSL-Passthrough](#)
- [E-Mail-Benachrichtigungen für den Lastausgleichsdienst](#)
- [Einarmige und mehrarmige Topologien](#)

SSL-Passthrough

SSL-Passthrough wird mit den Lastausgleichskonfigurationen verwendet.

SSL-Passthrough wird aus folgenden Gründen verwendet:

- Einfache Bereitstellung
 - Da keine Zertifikate für vRealize Automation, vRealize Orchestrator oder Workspace ONE Access an den Lastausgleichsdienst bereitgestellt werden müssen, wird die Bereitstellung vereinfacht und die Komplexität reduziert.
- Kein Betriebs-Overhead
 - Zum Zeitpunkt der Zertifikatsverlängerung sind keine Konfigurationsänderungen für den Lastausgleichsdienst erforderlich.
- Einfache Kommunikation
 - Die einzelnen Hostnamen der Komponenten mit Lastausgleich stehen im Feld für den alternativen Subjektnamen der Zertifikate, sodass der Client problemlos mit den Knoten mit Lastausgleich kommunizieren kann.

E-Mail-Benachrichtigungen für den Lastausgleichsdienst

Als bewährte Vorgehensweise kann eine E-Mail-Benachrichtigung für den Lastausgleichsdienst eingerichtet werden, damit jedes Mal E-Mails an den Systemadministrator gesendet werden, wenn ein Knoten von vRealize Automation, vRealize Orchestrator oder Workspace ONE Access ausfällt.

Zurzeit unterstützt NSX-V/T keine E-Mail-Benachrichtigung für ein solches Szenario.

Konfigurieren Sie für NetScaler spezifische SNMP-Traps und einen SNMP-Manager, um Warnungen zu senden. Weitere Informationen zur SNMP-Konfiguration finden Sie in der Dokumentation zu NetScaler.

Sie können die E-Mail-Benachrichtigung mit F5 mithilfe der folgenden Methoden einrichten:

- [Konfigurieren des BIG-IP-Systems für die Bereitstellung von lokal generierten E-Mail-Nachrichten](#)
- [Konfigurieren von benutzerdefinierten SNMP-Traps](#)
- [Konfigurieren von Warnungen zum Senden von E-Mail-Benachrichtigungen](#)

Einarmige und mehrarmige Topologien

Einarmige und mehrarmige Bereitstellungen leiten den Datenverkehr des Lastausgleichsdiensts unterschiedlich.

Bei einer einarmigen Bereitstellung befindet sich der Lastausgleichsdienst nicht physisch in der Linie des Datenverkehrs. Dies bedeutet, dass der eingehende und ausgehende Datenverkehr des Lastausgleichsdiensts die gleiche Netzwerkschnittstelle durchläuft. Der Datenverkehr vom Client über den Lastausgleichsdienst wird mit Netzwerkadressübersetzung (NAT) mit dem Lastausgleichsdienst als Quelladresse verarbeitet. Die Knoten senden ihren Rückverkehr an den Lastausgleichsdienst, bevor er an den Client zurückgegeben wird. Ohne diesen umgekehrten Paketfluss würde der Rückverkehr versuchen, den Client direkt zu erreichen, wodurch Verbindungen fehlschlagen.

Bei einer mehrarmigen Konfiguration wird der Datenverkehr über den Lastausgleichsdienst geleitet. Die Endgeräte verfügen in der Regel über den Lastausgleichsdienst als Standard-Gateway.

Die gängigste Bereitstellung ist eine einarmige Konfiguration. Die gleichen Grundsätze gelten für mehrarmige Bereitstellungen, und beide funktionieren mit F5 und NetScaler. Zu Zwecken dieses Dokuments werden die vRealize Automation-, vRealize Orchestrator- oder Workspace ONE Access-Komponenten als einarmige Konfiguration bereitgestellt. Mehrarmige Bereitstellungen werden ebenfalls unterstützt, und deren Konfiguration sollte der einarmigen Konfiguration gleichen.

Einarmige Konfiguration:



Voraussetzungen für die Konfiguration von Lastausgleichsdiensten für vRealize Automation

3

Führen Sie vor dem Konfigurieren von Lastausgleichsdiensten für vRealize Automation die folgenden erforderlichen Schritte durch.

- **NSX-V/T:** Vor dem Starten einer HA-Implementierung von vRealize Automation, vRealize Orchestrator oder Workspace ONE Access, die NSX-V/T als Lastausgleichsdienst verwendet, stellen Sie sicher, dass Ihre NSX-V/T-Topologie konfiguriert ist und dass Ihre Version von NSX-V/T unterstützt wird. In diesem Dokument wird der Lastausgleichsaspekt einer NSX-V/T-Konfiguration behandelt. Es wird davon ausgegangen, dass NSX-V/T konfiguriert und validiert ist, um in der Zielumgebung und den Netzwerken ordnungsgemäß zu funktionieren.

Informationen darüber, ob Ihre Version unterstützt wird, finden Sie in der Support-Matrix für vRealize Automation der aktuellen Version.

- **F5 BIG-IP LTM:** Bevor Sie eine HA-Implementierung von vRealize Automation, vRealize Orchestrator oder Workspace ONE Access mit einem F5 LTM-Lastausgleichsdienst starten, stellen Sie sicher, dass der Lastausgleichsdienst installiert und lizenziert ist und dass die Konfiguration des DNS-Servers abgeschlossen ist.
- **NetScaler:** Bevor Sie eine HA-Implementierung von vRealize Automation, vRealize Orchestrator oder Workspace ONE Access mit dem NetScaler-Lastausgleichsdienst starten, stellen Sie sicher, dass NetScaler installiert ist und mit mindestens einer Lizenz für die Standard Edition konfiguriert ist.
- **Zertifikate:** Fordern Sie ein von der Zertifizierungsstelle (CA) signiertes Zertifikat an, das den vollqualifizierten Domännennamen des Lastausgleichsdiensts und die Hostnamen der Clusterknoten im Abschnitt „SubjectAltNames“ enthält. Diese Konfiguration ermöglicht es dem Lastausgleichsdienst, Datenverkehr ohne SSL-Fehler zu bedienen.
- **Identitätsanbieter:** Ab vRealize Automation 8.0 ist der bevorzugte Identitätsanbieter Workspace ONE Access, der außerhalb der vRealize Automation-Appliance verwaltet wird.

Weitere Informationen zur Installation und Konfiguration finden Sie in der Dokumentation zu vRealize Automation auf docs.vmware.com.

Bei Bedarf kann der externe vRealize Orchestrator-Cluster für die Verwendung mit dem vRealize Automation-System konfiguriert werden. Dies ist nach der Inbetriebnahme des vRealize Automation-Systems möglich. Ein vRealize Automation-HA-Setup enthält jedoch bereits einen eingebetteten vRealize Orchestrator-Cluster.

Dieses Kapitel enthält die folgenden Themen:

- [Beenden der Erstinstallation](#)

Beenden der Erstinstallation

Sie müssen den Lastausgleichsdienst konfigurieren, bevor Sie die Erstinstallation von vRealize Automation, vRealize Orchestrator oder VMware Identity Manager abschließen.

Verfahren

- 1 Konfigurieren Sie den F5-, NSX- oder NetScaler-Lastausgleichsdienst. Weitere Informationen finden Sie unter „Konfigurieren von F5 BIG-IP“, „Konfigurieren von NSX“ und „Konfigurieren von Citrix NetScaler“.
- 2 Installieren und konfigurieren Sie alle Systemkomponenten wie in der [Installations-und Konfigurationsdokumentation](#) für vRealize Automation, vRealize Orchestrator und VMware Identity Manager beschrieben.
- 3 Stellen Sie sicher, dass sich alle Knoten im erwarteten Zustand befinden. Aktivieren Sie hierzu nach der Installation die Integritätsüberwachung im Lastausgleichsdienst. Der Pool, die Dienstgruppen und der virtuelle Server der Knoten der virtuellen Appliance müssen verfügbar sein und ausgeführt werden. Alle Knoten der virtuellen Appliance müssen verfügbar und aktiviert sein und ausgeführt werden.

Konfigurieren von NSX-V

4

Sie können ein neues NSX-V Edge Services Gateway bereitstellen oder ein vorhandenes wiederverwenden. Es muss jedoch über eine Netzwerkverbindung zu und von den vRealize-Komponenten verfügen, die vom Lastausgleichsdienst überwacht werden.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren der globalen Einstellungen](#)
- [Konfigurieren von Anwendungsprofilen](#)
- [Konfigurieren der Dienstüberwachung](#)
- [Konfigurieren von Serverpools](#)
- [Konfigurieren von virtuellen Servern](#)

Konfigurieren der globalen Einstellungen

Konfigurieren Sie die globalen Einstellungen mithilfe der folgenden Schritte.

Verfahren

- 1 Melden Sie sich bei NSX-V an, klicken Sie auf **Manager > Einstellungen** und wählen Sie **Schnittstellen** aus.
- 2 Wählen Sie Ihr Edge-Gerät aus der Liste aus.
- 3 Klicken Sie auf **vNIC#** für die externe Schnittstelle, die die virtuellen IP-Adressen hostet, und klicken Sie auf das Symbol **Bearbeiten**.

- 4 Wählen Sie den entsprechenden Netzwerkbereich für den NSX-V Edge aus und klicken Sie auf das Symbol **Bearbeiten**.

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 Fügen Sie die IP-Adressen hinzu, die den virtuellen IPs zugewiesen sind, und klicken Sie auf **Speichern**.
- 6 Klicken Sie auf **OK**, um die Schnittstellenkonfigurationsseite zu verlassen.
- 7 Navigieren Sie zur Registerkarte **Lastausgleichsdienst** und klicken Sie auf das Symbol **Bearbeiten**.
- 8 Wählen Sie **Lastausgleichsdienst aktivieren** und **Protokollierung**, falls erforderlich, und klicken Sie auf **Speichern**.

Edit Load Balancer Global Configuration

Load Balancer ☒ Enable

Acceleration ☐ Disable

Logging ☒ Enable

Log Level

CANCEL SAVE

Konfigurieren von Anwendungsprofilen

Anwendungsprofile müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) hinzugefügt werden.

Verfahren

- 1 Klicken Sie im linken Bereich auf **Anwendungsprofile**.
- 2 Klicken Sie auf das Symbol **Hinzufügen**, um die für das jeweilige Produkt erforderlichen Anwendungsprofile zu erstellen, wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 4-1. Anwendungsprofile

Name	Typ	Persistenz	Läuft ab in
vRealize Automation	SSL-Passthrough	Keine	Keine
vRealize Orchestrator	SSL-Passthrough	Keine	Keine
Hinweis Nur für externe vRealize Orchestrator-Instanzen.			
VMware Identity Manager	SSL-Passthrough	Quell-IP	36000

Ergebnisse

Die abgeschlossene Konfiguration sollte dem folgenden Bildschirm gleichen:

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**

Konfigurieren der Dienstüberwachung

Dienstüberwachungen müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) hinzugefügt werden.

Verfahren

- 1 Klicken Sie im linken Bereich auf **Dienstüberwachung**.

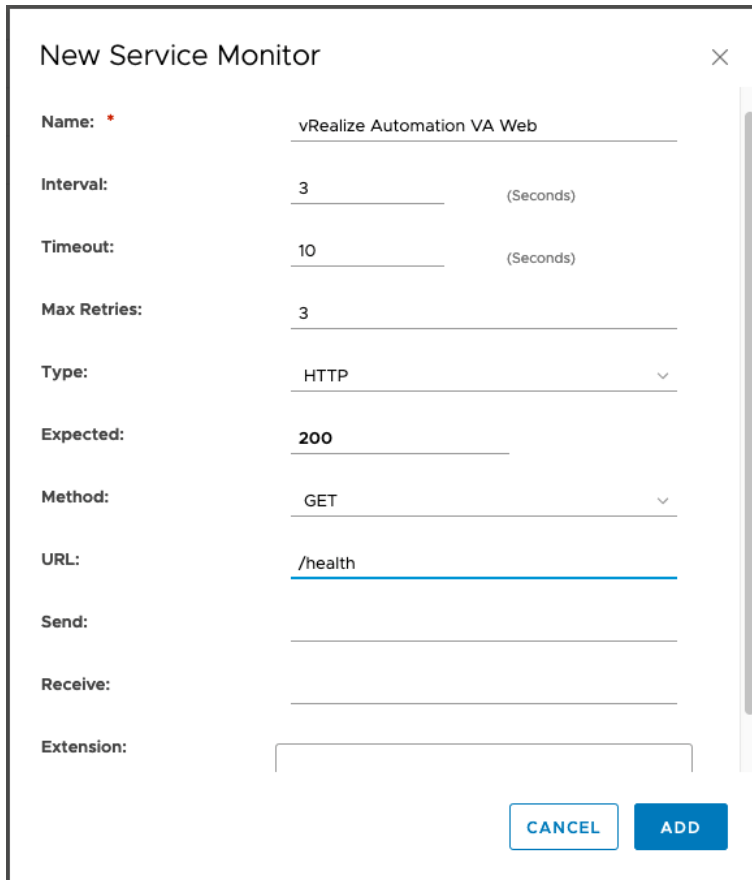
- 2 Klicken Sie auf das Symbol **Hinzufügen**, um die für das jeweilige Produkt erforderlichen Dienstüberwachungen zu erstellen, wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 4-2. Dienstüberwachung

Name	Intervall	Zeitüberschreitung	Wiederholungen	Typ	Methode	URL	Empfangen	Erwartet
vRealize Automation	3	10	3	HTTP	GET	/health		200
vRealize Orchestrator	3	10	3	HTTP	GET	/health		200
Hinweis Nur für externe vRealize Orchestrator-Instanzen.								
VMware Identity Manager	3	10	3	HTTPS	GET	/SAAS/API/1.0/REST/system/health/heartbeat	OK	200

Ergebnisse

Die abgeschlossene Konfiguration sollte dem folgenden Bildschirm gleichen:



The screenshot shows a 'New Service Monitor' dialog box with the following configuration:

- Name:** vRealize Automation VA Web
- Interval:** 3 (Seconds)
- Timeout:** 10 (Seconds)
- Max Retries:** 3
- Type:** HTTP
- Expected:** 200
- Method:** GET
- URL:** /health
- Send:** (empty field)
- Receive:** (empty field)
- Extension:** (empty field)

At the bottom right, there are two buttons: 'CANCEL' and 'ADD'.

Konfigurieren von Serverpools

Serverpools müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) erstellt werden.

Verfahren

- 1 Klicken Sie im linken Bereich auf **Pools**.

- 2 Klicken Sie auf das Symbol **Hinzufügen**, um die für das jeweilige Produkt erforderlichen Pools zu erstellen, wie in dieser Tabelle beschrieben.

Tabelle 4-3. Serverpools

Poolname	Algorithmus	Überwachung en	Mitgliedsnam e	IP-Adresse/ vCenter- Container	Port	Überwachungs port
vRealize Automation	Geringste Anzahl an Verbindungen	vRealize Automation	VA1 VA2 VA	IP-Adresse	443	8008
vRealize Orchestrator Hinweis Nur für externe vRealize Orchestrator- Instanzen.	Geringste Anzahl an Verbindungen	vRealize Orchestrator	VA1 VA2 VA3	IP-Adresse	443	8008
VMware Identity Manager	Geringste Anzahl an Verbindungen	VMware Identity Manager	VA1 VA2 VA3	IP-Adresse	443	8008

Ergebnisse

Die abgeschlossene Konfiguration sollte dem folgenden Bildschirm gleichen:

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

Konfigurieren von virtuellen Servern

Virtuelle Server müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) konfiguriert werden.

Verfahren

- 1 Klicken Sie im linken Bereich auf **Virtuelle Server**.

- 2 Klicken Sie auf das Symbol **Hinzufügen**, um die für das jeweilige Produkt erforderlichen virtuellen Server zu erstellen, wie in dieser Tabelle beschrieben. Verwenden Sie Standardwerte, wenn nichts angegeben ist.

Tabelle 4-4. Virtuelle Server

Name	Beschleunigung	IP-Adresse	Protokoll	Port	Standardpool	Anwendungsprofil
vRealize Automation	Deaktiviert	IP-Adresse	HTTPS	443	vRealize Automation	vRealize Automation
vRealize Orchestrator	Deaktiviert	IP-Adresse	HTTPS	443		
Hinweis Nur für externe vRealize Orchestrator-Instanzen.						
VMware Identity Manager	Deaktiviert	IP-Adresse	HTTPS	443	VMware Identity Manager	VMware Identity Manager

Ergebnisse

Die abgeschlossene Konfiguration sollte dem folgenden Bildschirm gleichen:

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

Konfigurieren von NSX-T

5

Vor dem Konfigurieren muss NSX-T in der Umgebung bereitgestellt werden, und das Gateway der Ebene 1 mit dem Lastausgleichsdienst muss über ein Netzwerk auf die vRealize-Komponenten zugreifen können.

Hinweis NSX-T Version 2.3 bietet keine Unterstützung für die HTTPS-Überwachung für den virtuellen FAST TCP-Serverpool. Die HTTPS-Überwachung wird für NSX-T Version 2.4 und höher unterstützt.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von NSX-T-Anwendungsprofilen](#)
- [Konfigurieren des Persistenzprofils für Workspace ONE Access](#)
- [Konfigurieren der aktiven NSX-T-Integritätsüberwachung](#)
- [Konfigurieren von NSX-T Serverpools](#)
- [Konfigurieren von virtuellen NSX-T-Servern](#)
- [Konfigurieren des Lastausgleichsdiensts](#)
- [Hinzufügen von virtuellen Servern zum Lastausgleichsdienst](#)

Konfigurieren von NSX-T-Anwendungsprofilen

Sie können ein Anwendungsprofil in NSX-T für HTTPS-Anforderungen hinzufügen.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Profile**.
- 2 Wählen Sie **Anwendung** als Profiltyp aus.
- 3 Klicken Sie auf **Anwendungsprofil hinzufügen** und wählen Sie **Fast TCP-Profil**.
- 4 Geben Sie einen Namen für das Profil ein.

Ergebnisse

Das abgeschlossene Anwendungsprofil für die HTTPS-Anforderung sollte dem folgenden Bildschirm gleichen:

The screenshot shows the 'PROFILES' tab in the vRealize Automation interface. Under 'Select Profile Type', 'APPLICATION' is selected. Below this is a table with one profile entry:

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

Below the table, the configuration details for the selected profile are shown:

- Description:** Enter Description
- Tags:** Tag (Required) and Scope (Optional) fields. A note states: 'Maximum 30 tags are allowed.'
- Connection Close Timeout:** 8

At the bottom, there are 'SAVE' and 'CANCEL' buttons.

Konfigurieren des Persistenzprofils für Workspace ONE Access

Führen Sie folgende Schritte aus, um ein Persistenzprofil für Workspace ONE Access zu konfigurieren.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Profile**.
- 2 Wählen Sie **Persistenz** als Profiltyp aus.
- 3 Geben Sie einen Namen für das Profil ein.
- 4 Legen Sie die **Zeitüberschreitung für den Persistenzeintrag** auf 36.000 Sekunden fest.

Konfigurieren der aktiven NSX-T-Integritätsüberwachung

Führen Sie die folgenden Schritte aus, um eine aktive Integritätsüberwachung für NSX-T zu konfigurieren.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Überwachungen**.
- 2 Klicken Sie auf **Aktive Überwachung hinzufügen** und wählen Sie **HTTP** aus.
- 3 Geben Sie einen Namen für die Integritätsüberwachung ein.

4 Konfigurieren Sie die Integritätsüberwachung wie in dieser Tabelle beschrieben:

Tabelle 5-1. Integritätsüberwachung konfigurieren

Name	Überwachungspunkt	Intervall	Zeitüberschreitung	Fehleranzahl	Typ	Methode	URL	Antwortcode	Antworttext
vRealize Automation	8008	3	10	3	HTTP	GET	/health	200	Keine
vRealize Orchestrator	8008	3	10	3	HTTP	GET	/health	200	Keine
VMware Identity Manager	443	3	10	3	HTTPS	GET	/ SAAS/API/1.0/REST/system/health/heartbeat	200	OK

Ergebnisse

Die abgeschlossene Konfiguration sollte den folgenden Bildschirmen gleichen:

The screenshot displays the 'MONITORS' configuration page in vRealize Orchestrator. The top navigation bar includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. Below the navigation bar, there is a 'Select Monitor Type' dropdown set to 'ACTIVE'. A search bar contains the text 'vRealize'. A table lists the configured monitors:

Name	Protocol	Monitoring Port	Monitoring Interval	Timeout Period (sec)	Server Pools
vRealize Automation VA *	HTTP	8008	3	10	

Below the table, the configuration details for the selected monitor are shown:

- Description:** Enter Description
- Tags:** Tag (Req) Scope (Opt) (checked). Maximum 30 tags are allowed.
- Additional Properties:**
 - HTTP Request:** Configure
 - HTTP Response:** Configure

At the bottom, there 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
 <p>Request Header not found</p>	

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

Konfigurieren von NSX-T Serverpools

Sie müssen Serverpools für vRealize Automation, vRealize Orchestrator, VMware Identity Manager und einen externen vRealize Orchestrator (optional) konfigurieren.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Serverpools**.
- 2 Klicken Sie auf **Serverpool hinzufügen**.
- 3 Geben Sie einen Namen für den Pool ein.
- 4 Konfigurieren Sie den Pool wie in dieser Tabelle beschrieben:

Tabelle 5-2. Konfigurieren von Serverpools

Poolname	Algorithmus	Aktive Überwachung	Name	IP	Port
vRealize Automation	Geringste Anzahl an Verbindungen	vRealize Automation	VA1 VA2 VA3	IP	443
vRealize Orchestrator	Geringste Anzahl an Verbindungen	vRealize Orchestrator	VA1 VA2 VA3	IP	443
Hinweis Nur für externe vRealize Orchestrator-Instanzen.					
VMware Identity Manager	Geringste Anzahl an Verbindungen	VMware Identity Manager	VA1 VA2 VA3	IP	443

Ergebnisse

Die abgeschlossene Konfiguration sollte den folgenden Bildschirmen gleichen:

The screenshot displays the 'SERVER POOLS' configuration page in the vRealize Orchestrator interface. The top navigation bar includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS' (selected), 'PROFILES', 'MONITORS', and 'About'. Below the navigation bar is a table with columns: 'Name', 'Algorithm', 'Members/Group', and 'Virtual Servers'. A new pool named 'pool_vra-va-web_443' is being configured. The 'Algorithm' is set to 'Least Conn'. The 'Members/Group' field is empty. The 'Virtual Servers' field is empty. The 'Description' field is empty. The 'SNAT Translation Mode' is set to 'Automap'. The 'Active Monitor' is set to 'vra_htt'. The interface includes buttons for 'ADD SERVER POOL', 'SAVE', and 'CANCEL'.

Configure Server Pool Members

Server Pool - pool_iaas-manager_443

☒ Enter individual members☐ Select a group

ADD MEMBER

Name	IP	Port	Weight	State	Backup Member	Max Concurrent Connections
⋮ <input type="text"/>	<input type="text"/>	443	1	Enabled	<input checked="" type="radio"/> Disabled	
⋮ <input type="text"/>	<input type="text"/>	443	1	Enabled	<input checked="" type="radio"/> Disabled	

CANCEL

APPLY

Konfigurieren von virtuellen NSX-T-Servern

Virtuelle Server müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) konfiguriert werden.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Virtuelle Server**.
- 2 Klicken Sie auf **Virtuellen Server hinzufügen** und wählen Sie **Ebene** aus.

3 Konfigurieren Sie die virtuellen Server wie in der folgenden Tabelle beschrieben:

Tabelle 5-3. Konfigurieren von virtuellen Servern

Name	Typ	Anwendungsprofil	IP-Adresse	Port	Serverpool	Persistenzprofil
vRealize Automation	L4-TCP	vRealize Automation	IP	443	vRealize Automation	Keine
vRealize Orchestrator	L4-TCP	vRealize Orchestrator	IP	443	vRealize Orchestrator	Keine
VMware Identity Manager	L4-TCP	VMware Identity Manager	IP	443	VMware Identity Manager	VMware Identity Manager

Hinweis Nur für externe vRealize Orchestrator-Instanzen.

Ergebnisse

Die abgeschlossene Konfiguration sollte dem folgenden Bildschirm gleichen:

The screenshot shows the vRealize Automation console interface. The top navigation bar includes tabs for LOAD BALANCERS, VIRTUAL SERVERS (selected), SERVER POOLS, PROFILES, MONITORS, and About. Below the navigation bar is a button labeled 'ADD VIRTUAL SERVER'. The main content area displays the configuration for a virtual server named 'vs_vra-va-web_443'. The configuration includes the following fields:

- Name:** vs_vra-va-web_443 (with a red asterisk indicating a required field)
- IP Address:** 10.10.10.10 (with a red asterisk indicating a required field and a hint 'e.g. 10.10.10.10')
- Ports:** 443 (with a red asterisk indicating a required field and a warning icon)
- Type:** L4 TCP
- Load Balancer:** r34r3r4 (with a dropdown arrow)
- Server Pool:** pool_ (with a dropdown arrow)
- Description:** Enter Description (text input field)
- Persistence:** Disabled (dropdown menu)
- Additional Properties:**
 - Max Concurrent Connections:** Unlimited (text input field)
 - Max New Connection Rate:** Unlimited (text input field)
 - Default Pool Member Ports:** 443 (text input field, with a hint '(e.g. 8080, ...)')
 - Access Log:** Disabled (toggle switch)
 - Admin State:** Enabled (toggle switch)
 - Tags:** Tag (Required) and Scope (Optional) (text input fields, with a hint 'Maximum 30 tags are allowed.')

At the bottom of the configuration form are two buttons: 'SAVE' and 'CANCEL'.

Konfigurieren des Lastausgleichsdiensts

Geben Sie einen Lastausgleichsdienst für jede vRealize Automation-, VMware Identity Manager- und für eine externe (optionale) vRealize OrchestratorInstanz an.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Lastausgleichsdienste**.
- 2 Klicken Sie auf **Lastausgleichsdienst hinzufügen**.
- 3 Geben Sie einen Namen ein und wählen Sie die entsprechende **Lastausgleichsdienstgröße** aus (hängt von der vRealize Automation-Clustergröße ab).
- 4 Wählen Sie **Logischer Tier-1-Router** aus.

Hinweis In NSX-T Version 2.4 werden die Integritätsprüfungen mithilfe der IP-Adresse des Tier-1-Uplinks (oder des ersten Dienstports für eigenständige SR Tier-1) für alle Lastausgleichsdienst-Serverpools durchgeführt. Stellen Sie sicher, dass die Serverpools über diese IP-Adresse erreichbar sind.

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

The screenshot displays the 'LOAD BALANCERS' configuration interface. At the top, there's a navigation bar with tabs: LOAD BALANCERS, VIRTUAL SERVERS, SERVER POOLS, PROFILES, MONITORS, and About. Below the navigation bar is a button 'ADD LOAD BALANCER'. The main form area contains several fields: 'Name' (vra75_lb), 'Size' (Small), and 'Tier-1 Gateway' (vRA-LB-Tier-1-Router). Below these are 'Description' (Enter Description), 'Tags' (Tag (Required), Scope (Optional)), 'Error Log Level', and 'Admin State' (toggle switch). A 'VIRTUAL SERVERS' section is collapsed. At the bottom, there are 'SAVE' and 'CANCEL' buttons.

Hinzufügen von virtuellen Servern zum Lastausgleichsdienst

Nachdem Sie den Lastausgleichsdienst konfiguriert haben, können Sie ihm virtuelle Server hinzufügen.

Verfahren

- 1 Navigieren Sie zu **Netzwerk > Lastausgleich > Virtuelle Server**.

- 2 Bearbeiten Sie die konfigurierten virtuellen Server.
- 3 Weisen Sie den zuvor konfigurierten Lastausgleichsdienst als den **Lastausgleichsdienst** zu.

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

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	p
Description <input type="text" value="Enter Description"/>		Application Profile * vRA_HTTPS			
Persistence Disabled					
> Additional Properties					
<div>SAVE</div> <div>CANCEL</div>					

Konfigurieren von F5 BIG-IP LTM

6

Bevor Sie Ihr F5-Gerät konfigurieren, muss es in der Umgebung mit Zugriff auf vRealize-Komponenten über ein Netzwerk bereitgestellt werden.

Für die Konfiguration muss das F5-Gerät folgende Anforderungen erfüllen:

- Das F5-Gerät kann entweder physisch oder virtuell sein.
- Der F5 LTM-Lastausgleichsdienst (Local Traffic Module) kann in einarmigen oder in mehrarmigen Topologien bereitgestellt werden.
- Das LTM muss als „Nominal“, „Minimal“ oder „Dediziert“ konfiguriert und lizenziert sein. Sie können das LTM konfigurieren, indem Sie zu **System > Ressourcenbereitstellung** navigieren.

Wenn Sie eine Version von F5 LTM vor 11.x verwenden, müssen Sie möglicherweise Ihre Einstellungen für die Integritätsüberwachung im Zusammenhang mit der Senden-Zeichenfolge ändern. Weitere Informationen zum Einrichten der Senden-Zeichenfolge für die Integritätsüberwachung für die einzelnen Versionen von F5 LTM finden Sie unter [HTTP health checks may fail even though the node is responding correctly](#).

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren des benutzerdefinierten Persistenzprofils für Workspace ONE Access](#)
- [Konfigurieren von Überwachungen](#)
- [Konfigurieren von F5-Serverpools](#)
- [Konfigurieren von virtuellen F5-Servern](#)

Konfigurieren des benutzerdefinierten Persistenzprofils für Workspace ONE Access

Sie können das Persistenzprofil für Ihren F5-Lastausgleichsdienst konfigurieren.

Verfahren

- 1 Melden Sie sich beim F5-Gerät an und navigieren Sie zu **Lokaler Datenverkehr > Profile > Persistenz**.
- 2 Klicken Sie auf **Erstellen**.
- 3 Geben Sie einen Namen ein und wählen Sie **Quelladressaffinität** aus dem Dropdown-Menü aus.

- 4 Aktivieren Sie den benutzerdefinierten Modus.
- 5 Legen Sie die **Zeitüberschreitung** auf 36.000 Sekunden fest.
- 6 Klicken Sie auf **Fertiggestellt**.

Konfigurieren von Überwachungen

Überwachungen müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) hinzugefügt werden.

Verfahren

- 1 Melden Sie sich beim F5-Lastausgleichsdienst an und wählen Sie **Lokaler Datenverkehr > Überwachung** aus.
- 2 Klicken Sie auf **Erstellen** und konfigurieren Sie die Überwachung wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 6-1. Konfigurieren von Überwachungen

Name	Typ	Intervall	Zeitüberschreitung	Senden-Zeichenfolge.	Empfangen-Zeichenfolge.	Alias-Dienst-Port
vRealize Automation	HTTP	3	10	GET/health HTTP/1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
vRealize Orchestrator Hinweis Nur für externe vRealize Orchestrator-Instanzen.	HTTP	3	10	GET/health HTTP/1.0\r\n\r\n	HTTP/1\.(0 1) (200)	8008
VMware Identity Manager	HTTPS	3	10	GET/ SAAS/API/1.0/ REST/system/ health/ heartbeat	ok\$	443

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

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

Konfigurieren von F5-Serverpools

Serverpools müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) konfiguriert werden.

Verfahren

- 1 Melden Sie sich beim F5-Lastausgleichsdienst an und wählen Sie **Lokaler Datenverkehr > Pools** aus.

- 2 Klicken Sie auf **Erstellen** und konfigurieren Sie den Pool wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 6-2. Konfigurieren von Serverpools

Name	Integritätsüberwachungen	Lastausgleichsmethode	Knotenname	Adresse	Dienst-Port
vRealize Automation	vRealize Automation	Geringste Anzahl an Verbindungen (Mitglied)	VA1 VA2 VA3	IP-Adresse	443
vRealize Orchestrator	vRealize Orchestrator	Geringste Anzahl an Verbindungen (Mitglied)	VA1 VA2 VA3	IP-Adresse	443
Hinweis Nur für externe vRealize Orchestrator-Instanzen.					
VMware Identity Manager	VMware Identity Manager	Geringste Anzahl an Verbindungen (Mitglied)	VA1 VA2 VA3	IP-Adresse	443

- 3 Geben Sie jedes Poolmitglied als **Neuer Knoten** ein und fügen Sie es zur Gruppe **Neue Mitglieder** hinzu.

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

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

Load Balancing

Load Balancing Method:

Priority Group Activation:

Current Members

<input checked="" 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)

Konfigurieren von virtuellen F5-Servern

Virtuelle Server müssen für vRealize Automation, VMware Identity Manager und für einen externen vRealize Orchestrator (optional) konfiguriert werden.

Verfahren

- 1 Melden Sie sich beim F5-Lastausgleichsdienst an und wählen Sie **Lokaler Datenverkehr > Virtuelle Server** aus.
- 2 Klicken Sie auf **Erstellen** und konfigurieren Sie den virtuellen Server wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 6-3. Konfigurieren von virtuellen Servern

Name	Typ	Zieladresse	Dienst-Port	Quelladressübersetzung	Standardpool	Standard-Persistenzprofil
vRealize Automation	Leistung (Ebene 4)	IP-Adresse	443	Automatische Zuordnung	vRealize Automation	Keine
vRealize Orchestrator	Leistung (Ebene 4)	IP-Adresse	443	Automatische Zuordnung	vRealize Orchestrator	Keine
Hinweis Nur für externe vRealize Orchestrator-Instanzen.						
VMware Identity Manager	Leistung (Ebene 4)	IP-Adresse	443	Automatische Zuordnung	VMware Identity Manager	VMware Identity Manager

- 3 Wählen Sie für eine Gesamtansicht und den Status der virtuellen Server **Lokaler Datenverkehr > Virtuelle Server**.

Ergebnisse

Die Konfiguration sollte den folgenden Bildschirmen gleichen:

General Properties	
Name	vs_vra-va-00_443
Description	
Type	Performance (Layer 4) ▾
Source Address	<input checked="" type="radio"/> Host <input type="radio"/> Address List <input type="text"/>
Destination Address/Mask	<input checked="" type="radio"/> Host <input type="radio"/> Address List 192.168.10.33
Service Port	<input checked="" type="radio"/> Port <input type="radio"/> Port List 443 HTTPS ▾
Notify Status to Virtual Address	<input checked="" type="checkbox"/>
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	<div> <div>Enabled</div> <div>Available</div> <div> <div><<</div> <div>>></div> <div> <div>Up</div> <div>Down</div> </div> </div> </div> <div> /Common _sys_APM_ExchangeSupport_OA_BasicAuth _sys_APM_ExchangeSupport_OA_NtimAuth _sys_APM_ExchangeSupport_helper _sys_APM_ExchangeSupport_main </div>
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

Konfigurieren von Citrix ADC (NetScaler ADC)

7

Stellen Sie vor der Konfiguration von Citrix ADC sicher, dass das NetScaler-Gerät in der Umgebung mit Zugriff auf die vRealize-Komponenten bereitgestellt wird.

Für die Konfiguration muss Citrix ADC folgende Anforderungen erfüllen:

- Sie können entweder einen virtuellen oder einen physischen NetScaler verwenden.
- Der Citrix-Lastausgleichsdienst kann sowohl in einarmigen als auch in mehrarmigen Topologien bereitgestellt werden.
- Aktivieren Sie den Lastausgleichsdienst und die SSL-Module, indem Sie zu **NetScaler > System > Einstellungen > Konfigurieren > Grundlegende Funktionen** navigieren.

Dieses Kapitel enthält die folgenden Themen:

- [Konfigurieren von Citrix-Überwachungen](#)
- [Konfigurieren von Citrix-Dienstgruppen](#)
- [Konfigurieren von virtuellen Citrix-Servern](#)
- [Konfigurieren der Persistenzgruppe für Workspace ONE Access](#)

Konfigurieren von Citrix-Überwachungen

Sie können eine Citrix-Überwachung konfigurieren, indem Sie die folgenden Schritte ausführen.

Verfahren

- 1 Melden Sie sich beim NetScaler-Lastausgleichsdienst an und navigieren Sie zu **NetScaler > Datenverkehrsverwaltung > Lastausgleich > Überwachungen**.

- 2 Klicken Sie auf **Hinzufügen** und konfigurieren Sie die Überwachung wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 7-1. Konfigurieren von Citrix-Überwachungen

Name	Typ	Intervall	Zeitüberschreitung	Wiederholungen	Wiederholung bis zum Erfolg	HTTP-Anforderung/ Senden - Zeichenfolge	Antwortcodes	Empfangen-Zeichenfolge	Ziel Port	Sicher
vRealize Automation	HTTP	5	4	3	1	GET / health	200	Keine	8008	Nein
vRealize Orchestrator	HTTP	5	4	3	1	GET / health	200	Keine	8008	Nein
Hinweis Nur für externe vRealize Orchestrator-Instanzen										
VMware Identity Manager	HTTP-ECV	5	4	3	1	GET / SAAS/API/1.0/REST/system/health/heartbeat	200	ok	443	yes

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

← Create Monitor

Name*

Type*

HTTP

>

Basic Parameters

Interval

Second

▼

Response Time-out

Second

▼

Response Codes

+

200

×

Custom Header

HTTP Request

☐ Secure

Advanced Parameters

Destination IP

Destination Port

Down Time

Second

▼

TROFS Code

TROFS String

Dynamic Time-out

Deviation

Second

▼

Dynamic Interval

Retries

Konfigurieren von Citrix-Dienstgruppen

Sie können Dienstgruppen konfigurieren, indem Sie die folgenden Schritte ausführen.

Verfahren

- 1 Melden Sie sich beim NetScaler-Lastausgleichsdienst an und navigieren Sie zu **NetScaler > Datenverkehrsverwaltung > Lastausgleich > Dienstgruppen**.
- 2 Klicken Sie auf **Hinzufügen** und konfigurieren Sie die Dienstgruppen wie in dieser Tabelle beschrieben.

Tabelle 7-2. Dienstgruppen konfigurieren

Name	Integritätsüberwachungen	Protokoll	Dienstgruppenmitglieder	Adresse	Port
vRealize Automation	vRealize Automation	SSL-Brücke	VA1 VA2 VA3	IP-Adresse	443
vRealize Orchestrator	vRealize Orchestrator	SSL-Brücke	VA1 VA2 VA3	IP-Adresse	443
Hinweis Nur für externe vRealize Orchestrator-Instanzen.					
VMware Identity Manager	VMware Identity Manager	SSL-Brücke	VA1 VA2 VA3	IP-Adresse	443

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

← 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

Konfigurieren von virtuellen Citrix-Servern

Sie können virtuelle Server konfigurieren, indem Sie die folgenden Schritte ausführen.

Verfahren

- 1 Melden Sie sich beim NetScaler-Lastausgleichsdienst an und navigieren Sie zu **NetScaler > Datenverkehrsverwaltung > Lastausgleich > Virtuelle Server**.

- 2 Klicken Sie auf **Hinzufügen** und konfigurieren Sie den virtuellen Server wie in dieser Tabelle beschrieben. Verwenden Sie den Standardwert, wenn nichts angegeben ist.

Tabelle 7-3. Konfigurieren von virtuellen Servern

Name	Protokoll	Zieladresse	Port	Lastausgleichsmethode	Bindung der Dienstgruppe
vRealize Automation	SSL-Brücke	IP-Adresse	443	Geringste Anzahl an Verbindungen	vRealize Automation
vRealize Orchestrator	SSL-Brücke	IP-Adresse	443	Geringste Anzahl an Verbindungen	vRealize Orchestrator
Hinweis Nur für externe vRealize Orchestrator-Instanzen.					
VMware Identity Manager	SSL-Brücke	IP-Adresse	443	Geringste Anzahl an Verbindungen	VMware Identity Manager

Ergebnisse

Die Konfiguration sollte folgendem Bildschirm gleichen:

← 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

Konfigurieren der Persistenzgruppe für Workspace ONE Access

Führen Sie die folgenden Schritte aus, um eine Persistenzgruppe für VMware Identity Manager zu konfigurieren.

Verfahren

- 1 Melden Sie sich bei NetScaler an und navigieren Sie zu **NetScaler > Datenverkehrsverwaltung > Lastausgleich > Persistenzgruppen**.
- 2 Klicken Sie auf **Hinzufügen**.
- 3 Legen Sie die **Zeitüberschreitung** auf 36.000 Sekunden fest.
- 4 Fügen Sie VMware Identity Manager alle zugehörigen virtuellen Server hinzu.

Hinweis Fügen Sie keine virtuellen Server für vRealize Automation oder vRealize Orchestrator hinzu.

- 5 Klicken Sie auf **OK**.

Dieses Kapitel enthält die folgenden Themen:

- [Bereitstellungsfehler bei der Verwendung von OneConnect mit F5 BIG-IP](#)
- [F5 BIG-IP-Lizenzgrenzwerte für die Netzwerkbandbreite](#)

Bereitstellungsfehler bei der Verwendung von OneConnect mit F5 BIG-IP

Wenn Sie die Funktion OneConnect mit F5 BIG-IP für einen virtuellen Server verwenden, schlagen die Bereitstellungsaufgaben manchmal fehl.

Mit OneConnect wird gewährleistet, dass Verbindungen vom Lastausgleichsdienst zu den Backendservern im Multiplex-Betrieb laufen und wiederverwendet werden. Dies senkt die Auslastung der Server und macht sie widerstandsfähiger.

Die Verwendung von OneConnect mit einem virtuellen Server mit SSL-Passthrough wird von F5 nicht empfohlen und führt möglicherweise zu fehlgeschlagenen Bereitstellungsversuchen. Dies geschieht, weil der Lastausgleichsdienst versucht, eine neue SSL-Sitzung über eine vorhandene Sitzung zu erstellen, während die Backendserver erwarten, dass der Client die vorhandene Sitzung entweder schließt oder neu verhandelt, was zu einem Verbindungsausfall führt. Deaktivieren Sie OneConnect, um dieses Problem zu beheben.

- 1 Melden Sie sich beim F5-Lastausgleichsdienst an und navigieren Sie zu **Lokaler Datenverkehr > Virtuelle Server > Liste der virtuellen Server**.
- 2 Klicken Sie auf den Namen des virtuellen Servers, den Sie ändern möchten.
- 3 Wählen Sie im Abschnitt **Beschleunigung** die Option **Keine** für das **OneConnect-Profil** aus.
- 4 Klicken Sie auf **Fertig stellen**.

F5 BIG-IP-Lizenzgrenzwerte für die Netzwerkbandbreite

Möglicherweise kann es zu Bereitstellungsfehlern oder Problemen beim Laden von vRealize Automation-Konsolenseiten kommen, weil der Netzwerkdatenverkehr des Lastausgleichsdiensts den F5 BIG-IP-Lizenzgrenzwert überschritten hat.

Informationen zur Prüfung, ob das Problem mit der BIG-IP-Plattform auftritt, finden Sie unter [How the BIG-IP VE system enforces the licensed throughput rate](#).