

Handleiding vRealize Automation 8.4 Load Balancing

15 april 2021

vRealize Automation 8.4

U vindt de recentste technische documentatie op de website van VMware:

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

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

VMware Nederland B.V.
Key Office Papendorp
3e verdieping
Orteliuslaan 850
Utrecht
Nederland
Tel: +31 (0) 30-2849500
Fax: +31 (0) 30- 2849501
www.vmware.com/nl

Copyright © 2021 VMware, Inc. Alle rechten voorbehouden. [Informatie over copyright en handelsmerken.](#)

Inhoud

1	Load balancing in vRealize Automation en vRealize Orchestrator	5
2	Load balancing-concepten	6
	SSL-passthrough	6
	Meldingen over load balancers	7
	One-arm en multi-arm topologieën	7
3	Vereisten voor het configureren van load balancers voor vRealize Automation	9
	De eerste installatie van vRealize Automation/ vRealize Orchestrator voltooien	10
4	NSX-V configureren	11
	Algemene instellingen configureren	11
	Applicatieprofielen configureren	13
	Servicebewaking configureren	14
	Serverpools configureren	16
	Virtuele servers configureren	18
5	NSX-T configureren	20
	NSX-T-applicatieprofielen configureren	20
	Actieve statusbewaking voor NSX-T configureren	21
	NSX-T-serverpools configureren	24
	Virtuele NSX-T-servers configureren	25
	Load balancer configureren	27
	Virtuele servers toevoegen aan load balancer	27
6	F5 BIG-IP LTM configureren	29
	Monitoren configureren	29
	F5-serverpools configureren	31
	Virtuele F5-servers configureren	32
7	Citrix ADC (NetScaler ADC) configureren	35
	Citrix-monitoren configureren	35
	Citrix-servicegroepen configureren	38
	Virtuele Citrix-servers configureren	39
8	Problemen oplossen	41

Fouten tijdens de vRealize Automation-installatie wanneer u NSX-V als load balancer gebruikt voor Workspace ONE 41

Inrichtingsfouten bij het gebruik van OneConnect met F5 BIG-IP 42

F5 BIG-IP-licentie beperkt netwerkbandbreedte 42

Load balancing in vRealize Automation en vRealize Orchestrator

1

Dit document beschrijft de configuratie van load balancing van vRealize Automation en vRealize Orchestrator in een gedistribueerde en clusterimplementatie met hoge beschikbaarheid met behulp van VMware NSX, F5 Networks BIG-IP (F5) en Citrix NetScaler-technologieën.

Dit document is geen installatiehandleiding, maar een configuratiehandleiding ter aanvulling op de installatie- en configuratiedocumentatie voor vRealize Automation en vRealize Orchestrator die beschikbaar is via de [productdocumentatie voor VMware vRealize Automation](#) en de [productdocumentatie voor VMware vRealize Orchestrator](#).

Deze informatie is bedoeld voor de volgende producten en versies.

Tabel 1-1.

Product	Versie
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

Raadpleeg de [VMware Product Interoperability Matrices](#) voor meer details.

Load balancing-concepten

2

Load balancers verdelen het werk tussen servers in implementaties met hoge beschikbaarheid. De systeembeheerder maakt regelmatig back-ups van de load balancers op hetzelfde ogenblik als andere onderdelen.

Voer deze back-ups van load balancers uit volgens het bij uw organisatie geldende beleid en houd daarbij rekening met het behoud van netwerktopologie en de planning van back-ups voor VMware-producten.

Dit hoofdstuk omvat de volgende onderwerpen:

- [SSL-passthrough](#)
- [Meldingen over load balancers](#)
- [One-arm en multi-arm topologieën](#)

SSL-passthrough

SSL-passthrough wordt gebruikt voor load balancing-configuraties.

SSL-passthrough wordt om de volgende redenen gebruikt:

- Eenvoudigere implementatie
 - Als u geen vRealize Automation- of vRealize Orchestrator-certificaten hoeft te implementeren voor de load balancer, wordt de implementatie zelf eenvoudiger en het systeem minder complex.
- Geen operationele overhead
 - Wanneer de certificaten moeten worden vernieuwd, hoeft u niets te veranderen aan de configuratie van de load balancer.
- Eenvoudige communicatie
 - In het SAN-veld op de certificaten worden de individuele hostnamen van de onderdelen voor load balancing vermeld als alternatieve houders, zodat de client eenvoudig kan communiceren met de knooppunten met taakverdeling.

Meldingen over load balancers

Het wordt aanbevolen om meldingen in te schakelen wanneer een vRealize Automation- of vRealize Orchestrator-knooppunt in een serverpool uitvalt.

VMware NSX Data Center ondersteunt het inschakelen van meldingen wanneer een waarschuwing wordt gegenereerd in vRealize Operations Manager en vRealize Network Insight. Raadpleeg de documentatie voor vRealize Operations Manager en vRealize Network Insight.

Configureer in NetScaler de specifieke SNMP-traps en de SNMP-beheerder die de waarschuwingen ontvangt. Raadpleeg de documentatie van NetScaler voor meer informatie over de SNMP-configuratie.

Met F5 kunt u een van de volgende methoden gebruiken om e-mailmeldingen in te stellen:

- [Het BIG-IP-systeem configureren om lokaal gegenereerde e-mailberichten af te leveren](#)
- [Aangepaste SNMP-traps configureren](#)
- [Waarschuwingen configureren om e-mailmeldingen te verzenden](#)

One-arm en multi-arm topologieën

In one-arm en multi-arm implementaties wordt het verkeer op een verschillende manier naar de load balancer geleid.

In een one-arm implementatie bevindt de load balancer zich niet fysiek in de lijn van het verkeer, wat betekent dat zowel het inkomend als uitgaand verkeer van de load balancer via dezelfde netwerkinterface verloopt. Het verkeer wordt vanaf de client op basis van IP-omzetting (NAT) door de load balancer gestuurd met de load balancer als bronadres. De knooppunten sturen hun retourverkeer eerst naar de load balancer voordat het naar de client wordt teruggeleid. Zonder deze stroom van retourpakketten zou het retourverkeer de client direct proberen te bereiken, waardoor de verbinding mislukt.

In een multi-arm configuratie wordt het verkeer door de load balancer geleid. In dit geval is de load balancer doorgaans de standaardgateway van de eindapparaten.

De meest voorkomende implementatie is een one-arm configuratie. Multi-arm implementaties zijn gestoeld op dezelfde principes en beide topologieën werken met F5 en NetScaler.

In dit document worden de onderdelen vRealize Automation en vRealize Orchestrator geïmplementeerd in een one-arm configuratie. Multi-arm implementaties worden ook ondersteund en hun configuratie is doorgaans vergelijkbaar met die van een one-arm configuratie.

One-arm configuratie:



Vereisten voor het configureren van load balancers voor vRealize Automation

3

Voordat u load balancers configureert, moet u de volgende voorbereidingen treffen.

- **NSX-V/T:** voordat u aan de slag kunt gaan met de implementatie met hoge beschikbaarheid van vRealize Automation of vRealize Orchestrator met NSX-V/T als load balancer, moet u ervoor zorgen dat uw NSX-V/T-topologie is geconfigureerd en dat uw versie van NSX-V/T wordt ondersteund. In dit document wordt de load balancing van een NSX-V/T-configuratie behandeld en wordt ervan uitgegaan dat NSX-V/T is geconfigureerd en dat de juiste werking ervan op de doelomgeving en -netwerken is gevalideerd. Zie de [ondersteuningsmatrix](#) voor het product om te controleren of uw versie wordt ondersteund.
- **F5 BIG-IP LTM:** voordat u aan de slag kunt gaan met de implementatie met hoge beschikbaarheid van vRealize Automation of vRealize Orchestrator met een F5 LTM load balancer, moet u ervoor zorgen dat de load balancer inclusief licentie is geïnstalleerd en dat de configuratie van de DNS-server is voltooid.
- **NetScaler:** voordat u aan de slag kunt gaan met de implementatie met hoge beschikbaarheid van vRealize Automation of vRealize Orchestrator met de load balancer van NetScaler, moet u ervoor zorgen dat NetScaler is geïnstalleerd en ten minste één Standard Edition-licentie heeft.
- **Certificaten:** een door de certificaatautoriteit (CA) ondertekend certificaat met vermelding van de volledig gekwalificeerde domeinnaam van de load balancer en de hostnamen van de clusterknooppunten in de sectie SubjectAltNames. Met deze configuratie kan de load balancer het verkeer zonder SSL-fouten verwerken.
- **Identiteitsprovider:** vanaf versie vRealize Automation 8.0 is Workspace ONE Access de identiteitsprovider die extern is geïmplementeerd naar de vRealize Automation Appliances en het cluster.

Zie de documentatie vRealize Automation op docs.vmware.com voor meer informatie over de installatie en configuratie.

Indien nodig kunt u een extern vRealize Orchestrator-cluster configureren voor gebruik met het vRealize Automation-systeem. Dit is mogelijk zodra het vRealize Automation-systeem volledig is geïnstalleerd. Bij de installatie van vRealize Automation met een hoge beschikbaarheid wordt standaard al een vRealize Orchestrator-cluster ingesloten.

Dit hoofdstuk omvat de volgende onderwerpen:

■ [De eerste installatie van vRealize Automation/ vRealize Orchestrator voltooien](#)

De eerste installatie van vRealize Automation/ vRealize Orchestrator voltooien

U moet uw load balancer configureren voordat u de eerste installatie van vRealize Automation, vRealize Orchestrator voltooit.

Tijdens het installatieproces van vRealize Automation of vRealize Orchestrator zal een load balancer normaal gesproken de helft van het verkeer naar de secundaire knooppunten leiden, die nog niet zijn geconfigureerd, waardoor de installatie mislukt. Om dit soort fouten te vermijden en de eerste installatie van vRealize Automation of vRealize Orchestrator te voltooien, moet u de volgende stappen uitvoeren.

Procedure

- 1 Configureer de F5, NSX of NetScaler load balancer. Zie [Hoofdstuk 6 F5 BIG-IP LTM configureren](#), [Hoofdstuk 5 NSX-T configureren](#) en [Hoofdstuk 7 Citrix ADC \(NetScaler ADC\) configureren](#).
- 2 Schakel de statusbewaking uit of wijzig deze tijdelijk in de standaard ICMP en zorg ervoor dat het verkeer nog steeds naar uw primaire knooppunten wordt doorgestuurd.
- 3 Schakel alle secundaire knooppunten uit in de load balancer-pools.
- 4 Installeer en configureer alle systeemonderdelen zoals beschreven in de installatie- en configuratiedocumentatie van vRealize Automation/vRealize Orchestrator.
- 5 Wanneer alle onderdelen zijn geïnstalleerd, moet u alle niet-primaire knooppunten op de load balancer inschakelen.
- 6 Configureer de load balancer zodat alle bewakingen (statuscontroles) zijn ingeschakeld.
Nadat u deze procedure hebt voltooid, moet u de bewaking die u hebt gemaakt in [Monitoren configureren](#) bijwerken.
- 7 Zorg ervoor dat alle knooppunten na de installatie de verwachte status hebben en dat de statusbewaking van de load balancer is ingeschakeld. De pool, servicegroepen en virtuele server van de virtual appliance-knooppunten moeten beschikbaar zijn en worden uitgevoerd. Alle virtual appliance-knooppunten moeten beschikbaar, actief en ingeschakeld zijn.

NSX-V configureren

4

U kunt een nieuwe NSX-V Edge Services-gateway implementeren of een bestaande opnieuw gebruiken. De gateway moet echter wel een netwerkconnectiviteit in twee richtingen hebben met de vRealize-onderdelen waarvoor load balancing wordt uitgevoerd.

Opmerking Raadpleeg de documentatie voor [VMware Workspace ONE](#) load balancing om de identiteitsprovider met hoge beschikbaarheid voor vRealize Automation te configureren.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Algemene instellingen configureren](#)
- [Applicatieprofielen configureren](#)
- [Servicebewaking configureren](#)
- [Serverpools configureren](#)
- [Virtuele servers configureren](#)

Algemene instellingen configureren

Configureer de algemene instellingen met behulp van deze stappen.

Procedure

- 1** Meld u aan bij de NSX-V, klik op **Manager > Instellingen** en selecteer **Interfaces**.
- 2** Selecteer uw edge-apparaat in de lijst.
- 3** Klik op **vNIC-nr.** voor de externe interface die de virtuele IP-adressen host en klik op het pictogram **Bewerken**.

- 4 Selecteer het juiste netwerkbereik voor de NSX-V Edge en klik op het pictogram **Bewerken**.

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 Voeg de IP-adressen toe die zijn toegewezen aan de virtuele IP-adressen en klik op **Opslaan**.
- 6 Klik op **OK** om de configuratiepagina van de interface af te sluiten.
- 7 Ga naar het tabblad **Load balancer** en klik op het pictogram **Bewerken**.
- 8 Selecteer **Load balancer inschakelen** en (indien nodig) **Logboekregistratie**, en klik op **Opslaan**.

Edit Load Balancer Global Configuration

Load Balancer ☒ Enable

Acceleration ☐ Disable

Logging ☒ Enable

Log Level

CANCEL SAVE

Applicatieprofielen configureren

U moet de vereiste applicatieprofielen toevoegen voor vRealize Automation en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Klik op **Applicatieprofielen** in het linker deelvenster.
- 2 Klik op het pictogram **Toevoegen** om de vereiste applicatieprofielen voor het specifieke product te maken overeenkomstig de beschrijving in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 4-1. Applicatieprofielen

Naam	Type	Persistentie	Vervalt over
vRealize Automation	SSL-passthrough	Geen	Geen
vRealize Orchestrator	SSL-passthrough	Geen	Geen
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.			

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien:

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**

Servicebewaking configureren

U moet servicemonitors toevoegen voor vRealize Automation en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Klik op **Servicebewaking** in het linker deelvenster.

- 2 Klik op het pictogram **Toevoegen** om de vereiste servicebewaking voor het specifieke product te maken overeenkomstig de beschrijving in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 4-2. Servicebewaking

Naam	Interval	Time-out	Aantal nieuwe pogingen	Type	Methode	URL	Ontvangen	Verwacht
vRealize Automation	3	10	3	HTTP	GET	/health		200
vRealize Orchestrator	3	10	3	HTTP	GET	/health		200
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.								

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien:

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**

Serverpools configureren

U moet serverpools maken voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Klik op **Pools** in het linker deelvenster.

- 2 Klik op het pictogram **Toevoegen** om de vereiste pools voor het specifieke product te maken overeenkomstig de beschrijving in deze tabel.

Tabel 4-3. Serverpools

Poolnaam	Algoritme	Monitoren	Naam van lid	IP-adres/ vCenter- container	Poort	Monitorpoort
vRealize Automation	Minste aantal verbindingen	vRealize Automation	VA1 VA2 VA	IP-adres	443	8008
vRealize Orchestrator	Minste aantal verbindingen	vRealize Orchestrator	VA1 VA2 VA3	IP-adres	443	8008

Opmerking
Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien:

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

Virtuele servers configureren

U moet virtuele servers configureren voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Klik op **Virtuele servers** in het linker deelvenster.
- 2 Klik op het pictogram **Toevoegen** om de vereiste virtuele servers voor het specifieke product te maken overeenkomstig de beschrijving in deze tabel. Gebruik standaardwaarden als er niets is opgegeven.

Tabel 4-4. Virtuele servers

Naam	Versnelling	IP-adres	Protocol	Poort	Standaardpool	Applicatieprofiel		
vRealize Automation	Uitgeschakeld	IP-adres	HTTPS	443	vRealize Automation	vRealize Automation		
vRealize Orchestrator	Uitgeschakeld	IP-adres	HTTPS	443	vRealize Orchestrator	vRealize Orchestrator		
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.								

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien.

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

NSX-T configureren

5

Voordat u de NSX-T configureert, moet u deze eerst in de omgeving implementeren en ervoor zorgen dat de laag-1 gateway met de load balancer netwerktoegang heeft tot de vRealize-onderdelen.

Opmerking Raadpleeg de documentatie voor [VMware Workspace ONE](#) load balancing om de identiteitsprovider met hoge beschikbaarheid voor vRealize Automation te configureren.

Opmerking NSX-T versie 2.3 biedt geen ondersteuning voor de HTTPS-monitor voor de virtuele FAST TCP-serverpool. De HTTPS-monitor wordt ondersteund voor NSX-T versie 2.4 en hoger.

Dit hoofdstuk omvat de volgende onderwerpen:

- [NSX-T-applicatieprofielen configureren](#)
- [Actieve statusbewaking voor NSX-T configureren](#)
- [NSX-T-serverpools configureren](#)
- [Virtuele NSX-T-servers configureren](#)
- [Load balancer configureren](#)
- [Virtuele servers toevoegen aan load balancer](#)

NSX-T-applicatieprofielen configureren

U kunt in NSX-T een applicatieprofiel toevoegen voor HTTPS-aanvragen.

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Profielen**.
- 2 Selecteer **Applicatie** als profieltype.
- 3 Klik op **Applicatieprofiel toevoegen** en selecteer **Snel TCP-profiel**.
- 4 Voer een naam in voor het profiel.

Resultaten

Het voltooide applicatieprofiel voor de HTTPS-aanvraag moet er ongeveer als volgt uitzien:

Select Profile Type **APPLICATION** ▾

ADD APPLICATION PROFILE ▾

Name	Type	Idle Timeout (sec)	HA Flow Mirroring
vRA_HTTPS *	Fast TCP	1800	<input type="checkbox"/> Disabled

Description:

Tags: ☒
Maximum 30 tags are allowed.

SAVE **CANCEL**

Actieve statusbewaking voor NSX-T configureren

Volg deze stappen om een actieve statusbewaking te configureren voor NSX-T.

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Monitoren**.
- 2 Klik op **Actieve bewaking toevoegen** en selecteer **HTTP**.
- 3 Voer een naam in voor de statusbewaking.

4 Configureer de statusbewaking zoals beschreven in deze tabel:

Tabel 5-1. Statusbewaking configureren

Naam	Bewakingspoort	Interval	Time-out	Aantal voor uitval	Type	Method e	URL	Antwoordcode	Antwoordberichttekst
vRealize Automation	8008	3	10	3	HTTP	GET	/health	200	Geen
vRealize Orchestrator	8008	3	10	3	HTTP	GET	/health	200	Geen

Opmerking
Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien.

LOAD BALANCERS VIRTUAL SERVERS SERVER POOLS PROFILES **MONITORS** [About](#)

Select Monitor Type **ACTIVE** ▾

[ADD ACTIVE MONITOR](#) ▾ [COLLAPSE ALL](#)

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

Description **Fall Count**

Tags ☒ **Rise Count**
Maximum 30 tags are allowed.

▾ **Additional Properties**

HTTP Request [Configure](#) HTTP Response [Configure](#)

[SAVE](#) [CANCEL](#)

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

NSX-T-serverpools configureren

U moet serverpools configureren voor vRealize Automation, en optioneel voor een externe vRealize Orchestrator (optioneel).

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Serverpools**.
- 2 Klik op **Serverpool toevoegen**.
- 3 Voer een naam in voor de pool.
- 4 Configureer de pool zoals beschreven in deze tabel:

Tabel 5-2. Serverpools configureren

Poolnaam	Algoritme	Actieve monitor	Naam	IP	Poort
vRealize Automation	Minste aantal verbindingen	vRealize Automation	VA1 VA2 VA3	IP	443
vRealize Orchestrator	Minste aantal verbindingen	vRealize Orchestrator	VA1 VA2 VA3	IP	443
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.					

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien.

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	vra_htt

Description: Enter Description

SNAT Translation Mode: Automap

Active Monitor

SAVE CANCEL

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

Virtuele NSX-T-servers configureren

U moet virtuele servers configureren voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Virtuele servers**.
- 2 Klik op **Virtuele server toevoegen** en selecteer **Laag**.

3 Configureer de virtuele servers zoals beschreven in deze tabel:

Tabel 5-3. Virtuele servers configureren

Naam	Type	Applicatieprofiel	IP-adres	Poort	Serverpool	Persistentieprofiel
vRealize Automation	L4 TCP	vRealize Automation	IP	443	vRealize Automation	Geen
vRealize Orchestrator	L4 TCP	vRealize Orchestrator	IP	443	vRealize Orchestrator	Geen

Opmerking
Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.

Resultaten

De voltooide configuratie moet er ongeveer als volgt uitzien.

The screenshot displays the 'VIRTUAL SERVERS' configuration page in the vRealize Automation interface. At the top, there is a navigation bar with 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 area shows a table with one entry: 'vs_vra-va-web_443'. The table columns are Name, IP Address, Ports, Type, Load Balancer, and Server Pool. The configuration details for this server are shown below the table:

- Name:** vs_vra-va-web_443
- IP Address:** 10.10.10.10 (with a note: e.g. 10.10.10.10)
- Ports:** 443 (with a warning icon)
- Type:** L4 TCP
- Load Balancer:** r34r3r4
- Server Pool:** pool_...
- Description:** Enter Description
- Persistence:** Disabled
- Additional Properties:**
 - Max Concurrent Connections:** Unlimited
 - Max New Connection Rate:** Unlimited
 - Default Pool Member Ports:** 443 (with a note: e.g. 8080, ...)
 - Access Log:** Disabled
- Admin State:** Enabled
- Tags:** Tag (Required), Scope (Optional) (with a note: Maximum 30 tags are allowed.)

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

Load balancer configureren

Geef een load balancer op voor elke vRealize Automation-instantie, optioneel voor een externe vRealize Orchestrator-instantie.

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Load Balancers**.
- 2 Klik op **Load balancer toevoegen**.
- 3 Voer een naam in en selecteer de juiste **load balancer-grootte** (afhankelijk van de vRealize Automation-cluster grootte).
- 4 Selecteer de **logische router van laag 1**.

Opmerking In versie 2.4 van NSX-T worden de statuscontroles voor alle serverpools met load balancing uitgevoerd op basis van het IP-adres van een laag-1 uplink (of de eerste servicepoort voor laag-1 standalone SR). Zorg ervoor dat de serverpools vanaf dit IP-adres toegankelijk zijn.

Resultaten

De configuratie moet er ongeveer als volgt uitzien:

The screenshot displays the 'LOAD BALANCERS' configuration page in vRealize Automation. The top navigation bar includes 'LOAD BALANCERS', 'VIRTUAL SERVERS', 'SERVER POOLS', 'PROFILES', 'MONITORS', and 'About'. A blue button 'ADD LOAD BALANCER' is visible. Below the navigation bar, 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, there is a form for adding a new load balancer. The form includes fields for 'Name' (with a red asterisk indicating it is required), 'Size' (a dropdown menu), 'Tier-1 Gateway' (a dropdown menu), 'Description' (a text area), 'Tags' (with 'Tag (Required)' and 'Scope (Optional)' dropdowns), 'Error Log Level' (a dropdown menu), and 'Admin State' (a toggle switch). A note states 'Maximum 30 tags are allowed.' Below the form, there is a section for 'VIRTUAL SERVERS' which is currently collapsed. At the bottom of the form are 'SAVE' and 'CANCEL' buttons.

Virtuele servers toevoegen aan load balancer

Zodra u de load balancer hebt geconfigureerd, kunt u virtuele servers toevoegen.

Procedure

- 1 Navigeer naar **Netwerken > Load Balancing > Virtuele servers**.
- 2 Bewerk de geconfigureerde virtuele servers.

3 Wijs de eerder geconfigureerde load balancer toe als **Load Balancer**.

Resultaten

De configuratie moet er ongeveer als volgt uitzien:

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 Enter Ports or Port Rang	L4 TCP	vRA_LB (x) v	p
Description Enter Description		Application Profile * vRA_HTTPS			
Persistence Disabled v					
> Additional Properties					
<div>SAVE CANCEL</div>					

F5 BIG-IP LTM configureren

6

Voordat u uw F5-apparaat configureert, moet u het eerst in de omgeving implementeren en de vRealize-onderdelen toegankelijk maken via een netwerk.

Opmerking Raadpleeg de documentatie voor [Workspace ONE](#) load balancing om de identiteitsprovider met hoge beschikbaarheid voor vRealize Automation te configureren.

Voor deze configuratie moet het F5-apparaat aan de volgende vereisten voldoen:

- Het F5-apparaat kan zowel fysiek als virtueel zijn.
- De F5-load balancer voor de LTM (Local Traffic Module) kan worden geïmplementeerd in een one-arm of multi-arm topologie.
- De LTM moet een nominale, minimale of specifieke configuratie en licentie hebben. U kunt de LTM configureren door te navigeren naar **Systeem > Resource-inrichting**.

Als u een F5 LTM-versie gebruikt die ouder is dan 11.x, moet u voor de verzendreeks mogelijk andere instellingen voor de statusbewaking opgeven. Voor meer informatie over het instellen van de verzendreeks voor de statusbewaking voor de verschillende versies van F5 LTM, raadpleegt u [Mislukte HTTP-statuscontroles voor goed reagerende knooppunten](#).

Dit hoofdstuk omvat de volgende onderwerpen:

- [Monitoren configureren](#)
- [F5-serverpools configureren](#)
- [Virtuele F5-servers configureren](#)

Monitoren configureren

U moet de monitoren toevoegen voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Meld u aan bij de F5 load balancer en navigeer naar **Lokaal verkeer > Monitor**.

- 2 Klik op **Maken** en configureer de monitor zoals beschreven in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 6-1. Monitoren configureren

Naam	Type	Interval	Time-out	Verzendreeks.	Ontvangstreks.	Alias servicepunt
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
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.						

Resultaten

De configuratie moet er ongeveer als volgt uitzien.

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:
Adaptive	<input type="checkbox"/> Enabled

Cancel Repeat Finished

F5-serverpools configureren

U moet serverpools configureren voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Meld u aan bij de F5 load balancer en navigeer naar **Lokaal verkeer > Pools**.

- 2 Klik op **Maken** en configureer de pool zoals beschreven in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 6-2. Serverpools configureren

Naam	Statusbewaking	Load balancing-methode	Knooppuntnaam	Adres	Servicepoort
vRealize Automation	vRealize Automation	Minste verbindingen (lid)	VA1 VA2 VA3	IP-adres	443
vRealize Orchestrator	vRealize Orchestrator	Minste verbindingen (lid)	VA1 VA2 VA3	IP-adres	443

Opmerking
Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.

- 3 Voer elk poolid in als een **nieuw knooppunt** en voeg dit toe aan de groep **Nieuwe leden**.

Resultaten

De configuratie moet er ongeveer als volgt uitzien.

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"/>	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

Virtuele F5-servers configureren

U moet virtuele servers configureren voor vRealize Automation, en (optioneel) voor een externe vRealize Orchestrator.

Procedure

- 1 Meld u aan bij de F5 load balancer en navigeer naar **Lokaal verkeer > Virtuele servers**.
- 2 Klik op **Maken** en configureer de virtuele server zoals beschreven in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 6-3. Virtuele servers configureren

Naam	Type	Bestemming adres	Servicepoort	Omzetting van bronadres	Standaardpo ol	Standaard- persistentiepr ofiel
vRealize Automation	Prestaties (laag 4)	IP-adres	443	Automatisch toewijzen	vRealize Automation	Geen
vRealize Orchestrator	Prestaties (laag 4)	IP-adres	443	Automatisch toewijzen	vRealize Orchestrator	Geen
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.						

- 3 Voor een algemene weergave en de status van de virtuele servers selecteert u **Lokaal verkeer > Virtuele servers**.

Resultaten

De configuratie moet er ongeveer als volgt uitzien.

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

Enabled

Available

iRules

<<

>>

Up

Down

/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

Citrix ADC (NetScaler ADC) configureren

7

Voordat u Citrix ADC configureert, moet u ervoor zorgen dat het NetScaler-apparaat in de omgeving is geïmplementeerd en toegang heeft tot de vRealize-onderdelen.

Voor deze configuratie moet het Citrix ADC-apparaat aan de volgende vereisten voldoen:

- U kunt zowel een virtuele als fysieke NetScaler gebruiken.
- De Citrix-load balancer kan worden geïmplementeerd in een one-arm of multi-arm topologie.
- Ga naar **NetScaler > Systeem > Instellingen > Configureren > Basisfuncties** en schakel de load balancer- en SSL-modules in.

Dit hoofdstuk omvat de volgende onderwerpen:

- [Citrix-monitoren configureren](#)
- [Citrix-servicegroepen configureren](#)
- [Virtuele Citrix-servers configureren](#)

Citrix-monitoren configureren

Voer de volgende procedure uit als u een Citrix-monitor wilt configureren.

Procedure

- 1 Meld u aan bij de NetScaler load balancer en navigeer naar **NetScaler > Verkeersbeheer > Load Balancing > Monitoren**.

- 2 Klik op **Toevoegen** en configureer de monitor zoals beschreven in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 7-1. Citrix-monitoren configureren

Naam	Type	Interval	Time-out	Aantal nieuwe pogingen	Geslaagde pogingen	HTTP-aanvraag/Send-tekenreeks	Antwoordcodes	Receivete-kenreeks	Best. Poort	Veilige
vRealize Automation	HTTP	5	4	3	1	Get/status	200	Geen	8008	Nee
vRealize Orchestrator	HTTP	5	4	3	1	Get/status	200	Geen	8008	Nee
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.										

Resultaten

De configuratie moet er ongeveer als volgt uitzien.

← 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

Citrix-servicegroepen configureren

Voer de volgende procedure uit als u servicegroepen wilt configureren.

Procedure

- 1 Meld u aan bij de NetScaler load balancer en navigeer naar **NetScaler > Verkeersbeheer > Load Balancing > Servicegroepen**.
- 2 Klik op **Toevoegen** en configureer de servicegroepen zoals beschreven in deze tabel.

Tabel 7-2. Servicegroepen configureren

Naam	Statusbewaking	Protocol	SG-leden	Adres	Poort
vRealize Automation	vRealize Automation	SSL-brug	VA1 VA2 VA3	IP-adres	443
vRealize Orchestrator	vRealize Orchestrator	SSL-brug	VA1 VA2 VA3	IP-adres	443
Opmerking Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.					

Resultaten

De configuratie moet er ongeveer als volgt uitzien:

← 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

Virtuele Citrix-servers configureren

Voer de volgende procedure uit als u virtuele servers wilt configureren.

Procedure

- 1 Meld u aan bij de NetScaler load balancer en navigeer naar **NetScaler > Verkeersbeheer > Load Balancing > Virtuele servers**.

- 2 Klik op **Toevoegen** en configureer de virtuele server zoals beschreven in deze tabel. Gebruik de standaardwaarde als er niets is opgegeven.

Tabel 7-3. Virtuele servers configureren

Naam	Protocol	Bestemmingsadres	Poort	Load balancing-methode	Servicegroepbinding
vRealize Automation	SSL-brug	IP-adres	443	Minste aantal verbindingen	vRealize Automation
vRealize Orchestrator	SSL-brug	IP-adres	443	Minste aantal verbindingen	vRealize Orchestrator

Opmerking
Gebruik deze optie alleen voor externe vRealize Orchestrator-instanties.

Resultaten

De configuratie moet er ongeveer als volgt uitzien:

← 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

Problemen oplossen

8

Dit hoofdstuk omvat de volgende onderwerpen:

- [Fouten tijdens de vRealize Automation-installatie wanneer u NSX-V als load balancer gebruikt voor Workspace ONE](#)
- [Inrichtingsfouten bij het gebruik van OneConnect met F5 BIG-IP](#)
- [F5 BIG-IP-licentie beperkt netwerkbandbreedte](#)

Fouten tijdens de vRealize Automation-installatie wanneer u NSX-V als load balancer gebruikt voor Workspace ONE

Als u fouten ziet wanneer u vRealize Automation installeert en tegelijk Workspace ONE als load balancer gebruikt, volgt u deze probleemoplossingsstappen.

Wanneer u NSX-V gebruikt als load balancer voor VMware Workspace ONE, kunnen er specifieke netwerkbependingen zijn die resulteren in fouten en time-outs tijdens de installatie van vRealize Automation zoals:

```
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
```

U kunt deze fouten beperken door de afsluittijd van de inactieve NSX-V-verbinding tot 5 minuten uit te stellen in plaats van de standaardwaarde van 1 seconde.

Dit kan worden bereikt met een applicatieregel die het volgende bevat:

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

Inrichtingsfouten bij het gebruik van OneConnect met F5 BIG-IP

Wanneer u gebruikmaakt van de functie OneConnect in combinatie met F5 BIG-IP voor een virtuele server, kunnen de inrichtingstaken soms mislukken.

OneConnect zorgt ervoor dat verbindingen tussen de load balancer en de back-endservers worden gemultiplext en opnieuw worden gebruikt. Hiermee verlaagt u de belasting van de servers en vergroot u hun flexibiliteit.

Het gebruik van OneConnect in combinatie met virtuele servers met SSL-passthrough, wordt niet aanbevolen door F5 en kan leiden tot mislukte inrichtingspogingen. Dit gebeurt omdat de load balancer probeert een nieuwe SSL-sessie tot stand te brengen over een bestaande sessie terwijl de back-endservers verwachten dat de client de bestaande sessie sluit of opnieuw onderhandelt, wat resulteert in een verbroken verbinding. Schakel OneConnect uit om dit probleem op te lossen.

- 1 Meld u aan bij de F5 load balancer en navigeer naar **Lokaal verkeer > Virtuele servers > Overzicht virtuele servers**.
- 2 Klik op naam van de virtuele server die u wilt aanpassen.
- 3 Selecteer in de sectie **Versnelling Geen** voor het **OneConnect-profiel**.
- 4 Klik op **Voltooien**.

F5 BIG-IP-licentie beperkt netwerkbandbreedte

Mogelijk ondervindt u inrichtingsfouten of problemen bij het laden van pagina's op de vRealize Automation-console doordat het netwerkverkeer van de load balancer de limiet van de F5 BIG-IP-licentie overschrijdt.

Als u wilt controleren of het BIG-IP-platform dit probleem ondervindt, raadpleegt u [Hoe het BIG-IP VE-systeem de doorvoercapaciteit conform de licentie afdwingt](#).