

vRealize Automation 8.1 ロード バランシング ガイド

2020 年 4 月 14 日

vRealize Automation 8.1



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認いただけます。このドキュメントに関するご意見および感想は、docfeedback@vmware.com までお送りください。

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

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2020 VMware, Inc. All rights reserved. [著作権および商標情報](#)。

目次

1	vRealize Automation 8.0 ロード バランシング	5
2	ロード バランシングの概念	6
	SSL パススルー	6
	ロード バランサでの E メール通知	6
	1 アームおよびマルチアーム トポロジ	7
3	vRealize Automation のロード バランサを構成するための前提条件	8
	初期インストールの完了	9
4	NSX-V の構成	10
	グローバル設定	10
	アプリケーション プロファイルの設定	12
	サービス監視の設定	13
	サーバ プールの構成	14
	仮想サーバの構成	16
5	NSX-T の構成	18
	NSX-T アプリケーション プロファイルの設定	18
	Workspace ONE Access のパーシステンス プロファイルの構成	19
	NSX-T アクティブ健全性モニターの構成	19
	NSX-T サーバ プールの構成	22
	NSX-T 仮想サーバの構成	23
	ロード バランサの構成	25
	ロード バランサへの仮想サーバの追加	25
6	F5 Big-IP LTM の構成	27
	Workspace ONE Access のカスタム パーシステンス プロファイルの構成	27
	モニターの構成	28
	F5 サーバ プールの構成	29
	F5 仮想サーバの構成	31
7	Citrix ADC (NetScaler ADC) の構成	33
	Citrix モニターの構成	33
	Citrix サービス グループの構成	36
	Citrix 仮想サーバの構成	37
	Workspace ONE Access のパーシステンス グループの構成	39

8 トラブルシューティング 40

F5 BIG-IP と OneConnect を併用した場合のプロビジョニングの失敗 40

F5 BIG-IP ライセンスによるネットワーク帯域幅の制限 40

vRealize Automation 8.0 ロード バランシング

1

このドキュメントでは、分散および高可用性展開における vRealize Automation、vRealize Orchestrator、および Workspace ONE Access の F5 Networks BIG-IP ソフトウェア (F5)、Citrix NetScaler、および NSX ロード バランサのロード バランシング モジュールの構成について説明します。

このドキュメントはインストール ガイドではありませんが、[VMware vRealize Automation のドキュメント](#)および [VMware vRealize Orchestrator のドキュメント](#)から利用可能な vRealize Automation および vRealize Orchestrator のインストールおよび構成ドキュメントを補足するロード バランシング構成ガイドです。

この情報は、次の製品およびバージョンに対応しています。

表 1-1.

製品	バージョン
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 (詳細については、 VMware 製品の相互運用性マトリックス を参照してください)
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 (以前の VMware Identity Manager)	3.3.1

詳細については、[VMware 製品の相互運用性マトリックス](#)を参照してください。

ロード バランシングの概念

2

ロードバランサは、高可用性環境でサーバ間のワークを分散させます。システム管理者は、他のコンポーネントと同時に、定期的にロードバランサをバックアップします。

ネットワーク トポロジの維持と VMware 製品のバックアップ プランに留意しながら、ロードバランサのバックアップについてのサイト ポリシーに従ってください。

この章には、次のトピックが含まれています。

- [SSL パススルー](#)
- [ロード バランサでの E メール通知](#)
- [1 アームおよびマルチアーム トポロジ](#)

SSL パススルー

SSL パススルーは、ロード バランシングの構成で使用されます。

SSL パススルーは、次の理由で使用されます。

- 展開の容易さ
 - vRealize Automation、vRealize Orchestrator、または Workspace ONE Access 証明書をロード バランサに展開する必要がないため、展開が簡素化され、複雑さが軽減されます。
- 運用上のオーバーヘッドがない
 - 証明書の更新時に、ロード バランサの構成を変更する必要がありません。
- 通信の容易さ
 - ロード バランシングされたコンポーネントの個々のホスト名は証明書のサブジェクト代替名フィールドであるため、クライアントはロード バランシングされたノードと簡単に通信できます。

ロード バランサでの E メール通知

vRealize Automation、vRealize Orchestrator、または Workspace ONE Access ノードが停止するたびに、システム管理者に E メールを送信する E メール通知をロード バランサで設定することをお勧めします。

現在、NSX-V/T はこのようなシナリオの E メール通知をサポートしていません。

NetScaler の場合は、アラートを送信するように特定の SNMP トラップと SNMP マネージャを構成します。SNMP 構成の詳細については、NetScaler のドキュメントを参照してください。

次の方法を使用して、F5 で E メール通知を設定できます。

- [ローカルで生成されたメール メッセージを配信するための BIG-IP システムの構成](#)
- [カスタム SNMP トラップの構成](#)
- [E メール通知を送信するためのアラートの構成](#)

1 アームおよびマルチアーム トポロジ

1 アーム展開とマルチアーム展開では、ロード バランサ トラフィックのルートが異なります。

1 アーム展開では、ロード バランサは物理的にトラフィックのライン上にありません。これは、ロード バランサの入力方向トラフィックと出力方向トラフィックが同じネットワーク インターフェイスを通過することを意味します。クライアントからロード バランサを経由するトラフィックは、ロード バランサを送信元アドレスとして使用するネットワーク アドレス変換 (NAT) です。ノードはクライアントに返される前に、リターン トラフィックをロード バランサに送信します。この逆方向の пакет フローを使用しない場合、リターン トラフィックはクライアントに直接アクセスするため、接続に失敗します。

マルチアーム構成では、トラフィックはロード バランサを経由してルーティングされます。通常、エンド デバイスにはデフォルト ゲートウェイとしてロード バランサがあります。

最も一般的な展開は、1 アーム構成です。同じ原則がマルチアーム展開にも適用され、どちらも F5 および NetScaler と連携します。このドキュメントでは、vRealize Automation、vRealize Orchestrator、または Workspace ONE Access の各コンポーネントが 1 アーム構成として展開されます。マルチアーム展開もサポートされており、その構成は 1 アーム構成と同様に行う必要があります。

[1 アーム構成:]



vRealize Automation のロード バランサを構成するための前提条件

3

vRealize Automation のロード バランサを構成する前に、次の前提条件を実行します。

- NSX-V/T – NSX-V/T をロード バランサとして使用して vRealize Automation、vRealize Orchestrator、または Workspace ONE Access の高可用性 (HA) 実装を開始する前に、NSX-V/T トポロジが構成されており、使用しているバージョンの NSX-V/T がサポートされていることを確認します。このドキュメントでは、NSX-V/T 構成のロード バランシングの側面について説明します。また、NSX-V/T が、ターゲット環境とネットワークで適切に機能するように構成および検証されていることを前提としています。

お使いのバージョンがサポートされていることを確認するには、現在のリリースの vRealize Automation のサポート マトリックス（英語）を参照してください。

- F5 BIG-IP LTM – F5 LTM ロード バランサを使用して vRealize Automation、vRealize Orchestrator、または Workspace ONE Access の高可用性 (HA) 実装を開始する前に、ロード バランサがインストールされ、ライセンスが供与されていること、および DNS サーバの構成が完了していることを確認します。
- NetScaler – NetScaler ロード バランサを使用して vRealize Automation、vRealize Orchestrator または Workspace ONE Access の高可用性 (HA) 実装を開始する前に、NetScaler がインストールされ、少なくとも Standard Edition ライセンスが構成されていることを確認します。
- 証明書 – SubjectAltNames セクションにあるロード バランサの完全修飾ドメイン名とクラスター ノードのホスト名を含む認証局 (CA) 署名付き証明書を要求します。この構成により、ロード バランサは SSL エラーを発生させずにトラフィックを処理できます。
- ID プロバイダー – vRealize Automation 8.0 以降、優先 ID プロバイダーは、vRealize Automation アプライアンスの外部にある Workspace ONE Access です。

インストールと構成の詳細については、docs.vmware.com で vRealize Automation のドキュメントを参照してください。

必要に応じて、外部 vRealize Orchestrator クラスターを vRealize Automation システムと連携するように構成できます。これは、vRealize Automation システムの実行中でも実行できます。ただし、vRealize Automation の高可用性設定には、すでに vRealize Orchestrator クラスターが組み込まれています。

この章には、次のトピックが含まれています。

- [初期インストールの完了](#)

初期インストールの完了

vRealize Automation、vRealize Orchestrator、または VMware Identity Manager の初期インストールを完了する前に、ロード バランサを構成する必要があります。

手順

- 1 F5、NSX、または NetScaler ロード バランサを構成します。F5 BIG-IP の構成、NSX の構成、および Citrix NetScaler の構成を参照してください。
- 2 vRealize Automation、vRealize Orchestrator、および VMware Identity Manager の [Easy Installer](#) を使用した [vRealize Automation 8.0 のインストールと構成](#)の説明に沿って、すべてのシステム コンポーネントをインストールおよび構成します。
- 3 インストール後にロード バランサで健全性監視が有効な状態で、すべてのノードが想定された状態であることを確認します。仮想アプライアンス ノードのプール、サービス グループ、および仮想サーバが使用可能で、実行中である必要があります。すべての仮想アプライアンス ノードが使用可能で、実行中で、有効になっている必要があります。

NSX-V の構成

4

新しい NSX-V Edge Services Gateway を展開するか、既存の NSX-V Edge Services Gateway を再利用できます。ただし、ロード バランシングされる vRealize コンポーネントとのネットワーク接続が必要です。

この章には、次のトピックが含まれています。

- [グローバル設定](#)
- [アプリケーション プロファイルの設定](#)
- [サービス監視の設定](#)
- [サーバ プールの構成](#)
- [仮想サーバの構成](#)

グローバル設定

次の手順を使用して、グローバル設定を行います。

手順

- 1 NSX-V にログインし、[Manager] - [設定] の順にクリックして、[インターフェイス] を選択します。
- 2 リストから Edge デバイスを選択します。
- 3 仮想 IP アドレスをホストする外部インターフェイスの [vNIC 番号] をクリックし、[編集] アイコンをクリックします。

- 4 NSX-V Edge の適切なネットワーク範囲を選択し、[編集] アイコンをクリックします。

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 割り当てられた IP アドレスを仮想 IP アドレスに追加し、[保存] をクリックします。
- 6 [OK] をクリックして、インターフェイスの構成ページを終了します。
- 7 [ロード バランサ] タブに移動し、[編集] アイコンをクリックします。
- 8 [ロード バランサの有効化] および必要に応じて [ログ作成] を選択して、[保存] をクリックします。

Edit Load Balancer Global Configuration

Load Balancer ☒ Enable

Acceleration ☐ Disable

Logging ☒ Enable

Log Level

CANCEL SAVE

アプリケーション プロファイルの設定

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のアプリケーション プロファイルを追加する必要があります。

手順

- 1 左側のペインの [アプリケーション プロファイル] をクリックします。
- 2 [追加] アイコンをクリックして、次の表に記載されている特定の製品に必要なアプリケーション プロファイルを作成します。何も指定されていない場合は、デフォルト値を使用します。

表 4-1. アプリケーション プロファイル

名前	タイプ	パーシステンス	有効期限
vRealize Automation	SSL パススルー	なし	なし
vRealize Orchestrator	SSL パススルー	なし	なし
注： 外部の vRealize Orchestrator インスタンスにのみ使用します。			
VMware Identity Manager	SSL パススルー	送信元の IP アドレス	36000

結果

完了した構成は次の画面のようになります。

New Application Profile

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

サービス監視の設定

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のサービス モニターを追加する必要があります。

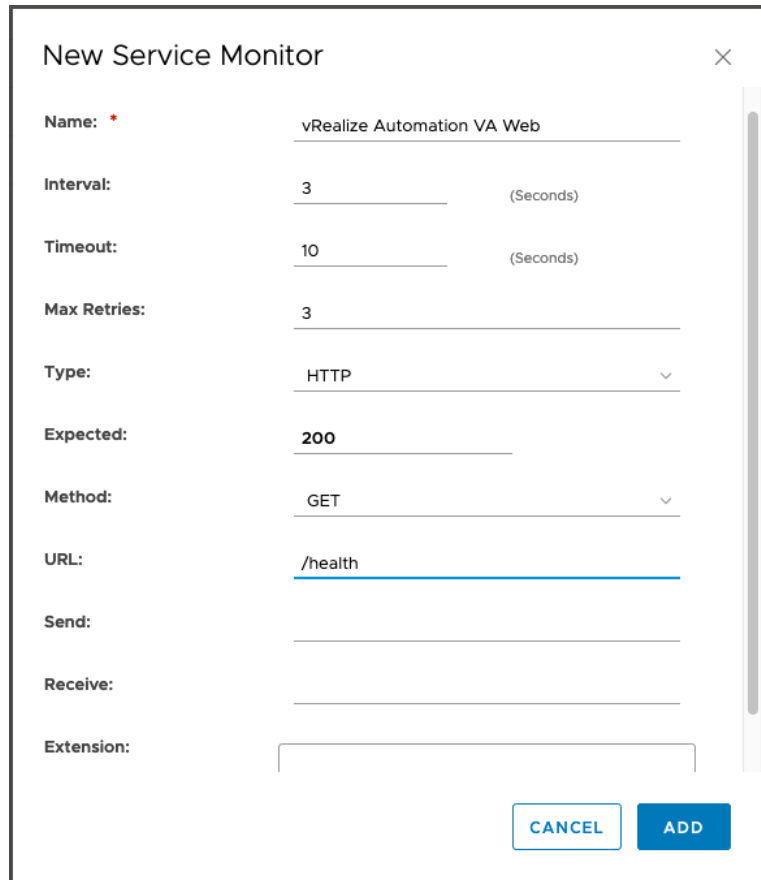
手順

- 1 左側のペインの [サービス監視] をクリックします。
- 2 [追加] アイコンをクリックして、次の表に記載されている特定の製品に必要なサービス モニターを作成します。
何も指定されていない場合は、デフォルト値を使用します。

表 4-2. サービス監視

名前	間隔	タイムアウト	再試行回数	タイプ	メソッド	URL	受信	期待値
vRealize Automation	3	10	3	HTTP	GET	/health		200
vRealize Orchestrator	3	10	3	HTTP	GET	/health		200
注： 外部の vRealize Orchestrator インスタンスにのみ使用します。								
VMware Identity Manager	3	10	3	HTTPS	GET	/ SAAS/API/ 1.0/REST/ system/ health/ heartbeat	OK	200

結果



New Service Monitor

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

完了した構成は次の画面のようになります。

サーバ プールの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のサーバプールを作成する必要があります。

手順

- 1 左側のペインの [プール] をクリックします。

2 [追加] アイコンをクリックして、次の表に記載されている特定の製品に必要なプールを作成します。

表 4-3. サーバ プール

プール名	アルゴリズム	モニター	メンバー名	IP アドレス/ vCenter Server コンテナ	ポート	監視ポート
vRealize Automation	リスト コネクション	vRealize Automation	VA1 VA2 VA	IP アドレス	443	8008
vRealize Orchestrator <small>注： 外部の vRealize Orchestrator インスタンスにのみ使用します。</small>	リスト コネクション	vRealize Orchestrator	VA1 VA2 VA3	IP アドレス	443	8008
VMware Identity Manager	リスト コネクション	VMware Identity Manager	VA1 VA2 VA3	IP アドレス	443	8008

結果

完了した構成は次の画面のようになります。

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

仮想サーバの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）の仮想サーバを構成する必要があります。

手順

- 1 左側のペインの [仮想サーバ] をクリックします。
- 2 [追加] アイコンをクリックして、次の表に記載されているさまざまな製品に必要な仮想サーバを作成します。何も指定されていない場合は、デフォルト値を使用します。

表 4-4. 仮想サーバ

名前	アクセラレーション	IP アドレス	プロトコル	ポート	デフォルト プール	アプリケーション プロファイル
vRealize Automation	無効	IP アドレス	HTTPS	443	vRealize Automation	vRealize Automation
vRealize Orchestrator	無効	IP アドレス	HTTPS	443		
注： 外部の vRealize Orchestrator インスタンスにのみ使用します。						
VMware Identity Manager	無効	IP アドレス	HTTPS	443	VMware Identity Manager	VMware Identity Manager

結果

完了した構成は次の画面のようになります。

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 の構成

5

構成する前に、NSX-T を環境に展開し、ロード バランサを使用する Tier-1 ゲートウェイがネットワーク経由で vRealize コンポーネントにアクセスできる必要があります。

注： NSX-T バージョン 2.3 は、Fast TCP 仮想サーバ プールの HTTPS モニターをサポートしていません。HTTPS モニターは、NSX-T バージョン 2.4 以降でサポートされています。

この章には、次のトピックが含まれています。

- [NSX-T アプリケーション プロファイルの設定](#)
- [Workspace ONE Access のパーシステンス プロファイルの構成](#)
- [NSX-T アクティブ健全性モニターの構成](#)
- [NSX-T サーバ プールの構成](#)
- [NSX-T 仮想サーバの構成](#)
- [ロード バランサの構成](#)
- [ロード バランサへの仮想サーバの追加](#)

NSX-T アプリケーション プロファイルの設定

HTTPS 要求のアプリケーション プロファイルを NSX-T に追加できます。

手順

- 1 [ネットワーク] - [ロード バランシング] - [プロファイル] の順に移動します。
- 2 プロファイル タイプとして [アプリケーション] を選択します。
- 3 [アプリケーション プロファイルの追加] をクリックして、[Fast TCP プロファイル] を選択します。
- 4 プロファイルの名前を入力します。

結果

HTTPS 要求の完了したアプリケーション プロファイルは、次の画面のようになります。

The screenshot shows the vRealize Automation interface with the 'PROFILES' tab selected. The 'APPLICATION' profile type is chosen. A table displays the profile 'vRA_HTTPS' with details: Name (vRA_HTTPS), Type (Fast TCP), Idle Timeout (1800), and HA Flow Mirroring (Disabled). Below the table, the configuration form for 'vRA_HTTPS' is visible, including fields for Description, Tags, and Connection Close Timeout (set to 8). The 'SAVE' button is highlighted.

Workspace ONE Access のパーシステンス プロファイルの構成

Workspace ONE Access のパーシステンス プロファイルを構成するには、次の手順を実行します。

手順

- 1 [ネットワーク] - [ロード バランシング] - [プロファイル] の順に移動します。
- 2 プロファイル タイプとして [パーシステンス] を選択します。
- 3 プロファイルの名前を入力します。
- 4 [パーシステンス エントリ タイムアウト] を 36000 秒に設定します。

NSX-T アクティブ健全性モニターの構成

NSX-T 用のアクティブ健全性モニターを構成するには、次の手順を実行します。

手順

- 1 [ネットワーク] - [ロード バランシング] - [モニター] の順に移動します。
- 2 [アクティブ モニターの追加] をクリックして、[HTTP] を選択します。
- 3 健全性モニターの名前を入力します。

4 次の表に記載されているように健全性モニターを構成します。

表 5-1. 健全性モニターの構成

名前	監視ポート	間隔	タイムアウト	失敗回数	タイプ	メソッド	URL	応答コード	応答本文
vRealize Automation	8008	3	10	3	HTTP	GET	/health	200	なし
vRealize Orchestrator	8008	3	10	3	HTTP	GET	/health	200	なし
VMware Identity Manager	443	3	10	3	HTTPS	GET	/SAAS/API/1.0/REST/system/health/heartbeat	200	OK

注： 外部の vRealize Orchestrator インスタンスにのみ使用します。

結果

完了した構成は次の画面のようになります。

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: Enter Description

Fall Count: 3

Tags: Tag (Req) Scope (Opt) ☒
 Maximum 30 tags are allowed.

Rise Count: 3

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
 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 X

1 or more response codes

HTTP Response Body

NSX-T サーバ プールの構成

vRealize Automation、vRealize Orchestrator、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のサーバ プールを構成する必要があります。

手順

- 1 [ネットワーク] - [ロード バランシング] - [サーバ プール] の順に移動します。
- 2 [サーバ プールの追加] をクリックします。
- 3 プールの名前を入力します。
- 4 次の表に記載されているようにプールを構成します。

表 5-2. サーバ プールの構成

プール名	アルゴリズム	アクティブ モニター	名前	IP アドレス	ポート
vRealize Automation	リスト コネクション	vRealize Automation	VA1 VA2 VA3	IP アドレス	443
vRealize Orchestrator <small>注: 外部の vRealize Orchestrator インスタンスにのみ使用します。</small>	リスト コネクション	vRealize Orchestrator	VA1 VA2 VA3	IP アドレス	443
VMware Identity Manager	リスト コネクション	VMware Identity Manager	VA1 VA2 VA3	IP アドレス	443

結果

完了した構成は次の画面のようになります。

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

Active Monitor: vra_htt

SNAT Translation Mode: Automap ▾

> Additional Properties

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

NSX-T 仮想サーバの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）の仮想サーバを構成する必要があります。

手順

- 1 [ネットワーク] - [ロード バランシング] - [仮想サーバ] の順に移動します。
- 2 [仮想サーバの追加] をクリックして、[レイヤー] を選択します。

3 次の表に記載されているように仮想サーバを構成します。

表 5-3. 仮想サーバの構成

名前	タイプ	アプリケーション プロファイル	IP アドレス	ポート	サーバ プール	パーシステンス プ ロファイル
vRealize Automation	L4 TCP	vRealize Automation	IP アドレス	443	vRealize Automation	なし
vRealize Orchestrator	L4 TCP	vRealize Orchestrator	IP アドレス	443	vRealize Orchestrator	なし
VMware Identity Manager	L4 TCP	VMware Identity Manager	IP アドレス	443	VMware Identity Manager	VMware Identity Manager

注： 外部の
vRealize
Orchestrator イン
スタンスにのみ使
用します。

結果

完了した構成は次の画面のようになります。

The screenshot shows the vRealize Automation console interface. The 'VIRTUAL SERVERS' tab is selected. A table lists the virtual server configuration:

Name	IP Address	Ports	Type	Load Balancer	Server
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
 - Sorry Server Pool:** Select Server Pool
 - Admin State:** Enabled
 - Tags:** Tag (Required), Scope (Optional)
- Application Profile:** vRA_HTTP
- Max New Connection Rate:** Unlimited
- Default Pool Member Ports:** 443
- Access Log:** Disabled

Buttons: SAVE, CANCEL

ロード バランサの構成

各 vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）インスタンスのロード バランサを指定します。

手順

- 1 [ネットワーク] - [ロード バランシング] - [ロード バランサ] の順に移動します。
- 2 [ロード バランサの追加] をクリックします。
- 3 名前を入力し、適切な [ロード バランサのサイズ]（vRealize Automation クラスタのサイズによって異なります）を選択します。
- 4 [Tier-1 論理ルーター] を選択します。

注： NSX-T バージョン 2.4 では、モニターの健全性チェックは、すべてのロード バランサ サーバ プールに対して、Tier-1 アップリンク（または Tier-1 スタンドアローン サポート リクエスト (SR) の最初のサービスポート）の IP アドレスを使用して実行されます。サーバ プールにこの IP アドレスからアクセスできることを確認します。

結果

構成は次の画面のようになります。

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 contains the following fields:

- Name:** vra75_lb (with a red asterisk indicating a required field)
- Size:** Small (dropdown menu)
- Tier-1 Gateway:** vRA-LB-Tier-1-Router (dropdown menu with a close icon)
- Description:** Enter Description (text input field)
- Tags:** Tag (Required) and Scope (Optional) (text input fields with a checkmark icon). Below them, it says 'Maximum 30 tags are allowed.'
- Error Log Level:** (dropdown menu)
- Admin State:** (toggle switch, currently turned on)

Below the main form, there's a section titled 'VIRTUAL SERVERS' with a 'SAVE' button and a 'CANCEL' button.

ロード バランサへの仮想サーバの追加

ロード バランサを構成したら、仮想サーバを追加できます。

手順

- 1 [ネットワーク] - [ロード バランシング] - [仮想サーバ] の順に移動します。
- 2 構成された仮想サーバを編集します。

3 以前に構成したロード バランサを [ロード バランサ] として割り当てます。

結果

構成は次の画面のようになります。

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

F5 Big-IP LTM の構成

6

F5 デバイスを構成する前に、ネットワーク経由で vRealize コンポーネントにアクセスできる環境に展開する必要があります。

構成には、F5 デバイスが次の要件を満たしている必要があります。

- F5 デバイスが物理または仮想のいずれかである。
- F5 Local Traffic Module (LTM) ロード バランサを 1 アームまたはマルチアーム トポロジのいずれかに展開できる。
- LTM は、Nominal、Minimum、または Dedicated のいずれかとして構成され、ライセンス供与されている必要がある。[システム] - [リソース プロビジョニング] の順に移動して、LTM を構成できる。

11.x よりも前の F5 LTM バージョンを使用している場合は、文字列の送信に関連する健全性監視の設定の変更が必要になる場合があります。各バージョンの F5 LTM で、健全性監視の文字列の送信を設定する方法の詳細については、[HTTP health checks may fail even though the node is responding correctly](#) を参照してください。

この章には、次のトピックが含まれています。

- [Workspace ONE Access のカスタム パーシステンス プロファイルの構成](#)
- [モニターの構成](#)
- [F5 サーバ プールの構成](#)
- [F5 仮想サーバの構成](#)

Workspace ONE Access のカスタム パーシステンス プロファイルの構成

F5 ロード バランサのパーシステンス プロファイルを構成できます。

手順

- 1 F5 デバイスにログインし、[ローカル トラフィック] - [プロファイル] - [パーシステンス] の順に移動します。
- 2 [作成] をクリックします。
- 3 名前を入力し、ドロップダウン メニューから [送信元アドレスのアフィニティ] を選択します。
- 4 カスタム モードを有効にします。
- 5 [タイムアウト] を 36,000 秒に設定します。

6 [完了] をクリックします。

モニターの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のモニターを追加する必要があります。

手順

- 1 F5 ロード バランサにログインし、[ローカル トラフィック] - [モニター] の順に移動します。
- 2 [作成] をクリックして、次の表に記載されているようにモニターを構成します。何も指定されていない場合は、デフォルト値を使用します。

表 6-1. モニターの構成

名前	タイプ	間隔	タイムアウト	文字列の送信	文字列の受信	エイリアス サービス ポート
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
注： 外部の vRealize Orchestrator インスタンスにのみ使用します。						
VMware Identity Manager	HTTPS	3	10	GET/ SAAS/API/1.0/ REST/system/ health/ heartbeat	ok\$	443

結果

構成は次の画面のようになります。

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

F5 サーバ プールの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）のサーバ プールを構成する必要があります。

手順

- 1 F5 ロード バランサにログインし、[ローカル トラフィック] - [プール] の順に移動します。

- 2 [作成] をクリックして、次の表に記載されているようにプールを構成します。何も指定されていない場合は、デフォルト値を使用します。

表 6-2. サーバ プールの構成

名前	健全性監視	ロード バランシングの方法	ノード名	アドレス	サービス ポート
vRealize Automation	vRealize Automation	リスト コネクション (メンバー)	VA1 VA2 VA3	IP アドレス	443
vRealize Orchestrator <small>注: 外部の vRealize Orchestrator インスタンスにのみ使用します。</small>	vRealize Orchestrator	リスト コネクション (メンバー)	VA1 VA2 VA3	IP アドレス	443
VMware Identity Manager	VMware Identity Manager	リスト コネクション (メンバー)	VA1 VA2 VA3	IP アドレス	443

- 3 各プール メンバーを [新規ノード] として入力し、[新規メンバー] グループに追加します。

結果

構成は次の画面のようになります。

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

Load Balancing

Load Balancing Method:

Priority Group Activation:

Current Members

<input checked="" type="checkbox"/>	<input type="button" value="Status"/>	<input type="button" value="Member"/>	<input type="button" value="Address"/>	<input type="button" value="Service Port"/>	<input type="button" value="FQDN"/>	<input type="button" value="Ephemeral"/>	<input type="button" value="Ratio"/>	<input type="button" value="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)

F5 仮想サーバの構成

vRealize Automation、VMware Identity Manager、および外部 vRealize Orchestrator（オプション）の仮想サーバを構成する必要があります。

手順

- 1 F5 ロード バランサにログインし、[ローカル トラフィック] - [仮想サーバ] の順に移動します。
- 2 [作成] をクリックして、次の表に記載されているように仮想サーバを構成します。何も指定されていない場合は、デフォルト値を使用します。

表 6-3. 仮想サーバの構成

名前	タイプ	宛先のアドレス	サービス ポート	送信元アドレス 変換	デフォルト プール	デフォルト パーシ ステンス プロファ イル
vRealize Automation	パフォーマンス (レイヤー 4)	IP アドレス	443	自動マップ	vRealize Automation	なし
vRealize Orchestrator	パフォーマンス (レイヤー 4)	IP アドレス	443	自動マップ	vRealize Orchestrator	なし
注： 外部の vRealize Orchestrator イン スタンスにのみ使 用します。						
VMware Identity Manager	パフォーマンス (レイヤー 4)	IP アドレス	443	自動マップ	VMware Identity Manager	VMware Identity Manager

- 3 全体的なビューと仮想サーバのステータスについては、[ローカル トラフィック] - [仮想サーバ] の順に選択します。

結果

構成は次の画面のようになります。

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
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>Enabled Available</div> <div><< >></div> <div>Up Down</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

Citrix ADC (NetScaler ADC) の構成

7

Citrix ADC を構成する前に、vRealize コンポーネントにアクセスできる環境に NetScaler デバイスが展開されていることを確認します。

構成には、Citrix ADC が次の要件を満たしている必要があります。

- 仮想または物理 NetScaler のいずれかを使用できる。
- Citrix ロード バランサを 1 アームまたはマルチアーム トポロジのいずれかに展開できる。
- [NetScaler] - [システム] - [設定] - [構成] - [基本的な機能] の順に移動して、ロード バランサと SSL モジュールを有効にする。

この章には、次のトピックが含まれています。

- [Citrix モニターの構成](#)
- [Citrix サービス グループの構成](#)
- [Citrix 仮想サーバの構成](#)
- [Workspace ONE Access のパーシステンス グループの構成](#)

Citrix モニターの構成

Citrix モニターを構成するには、次の手順を実行します。

手順

- 1 NetScaler ロード バランサにログインし、[NetScaler] - [トラフィック管理] - [ロード バランシング] - [モニター] の順に移動します。

- 2 [追加] をクリックして、次の表に記載されているようにモニターを構成します。何も指定されていない場合は、デフォルト値を使用します。

表 7-1. Citrix モニターの構成

名前	タイプ	間隔	タイムアウト	再試行回数	成功再試行回数	HTTP 要求/文字列の送信	応答コード	文字列の受信	宛先ポート	セキュア
vRealize Automation	HTTP	5	4	3	1	GET/health	200	なし	8008	いいえ
vRealize Orchestrator	HTTP	5	4	3	1	GET/health	200	なし	8008	いいえ
注： 外部の vRealize Orchestrator インスタンスにのみ使用します。										
VMware Identity Manager	HTTP-ECV	5	4	3	1	GET/SAAS/API/1.0/REST/system/health/heartbeat	200	OK	443	はい

結果

構成は次の画面のようになります。

← Create Monitor

Name*

vra_https_va_web

i

Type*

HTTP

>

i

Basic Parameters

Interval

5

Second

▼

Response Time-out

4

Second

▼

i

Response Codes

+

200

×

Custom Header

HTTP Request

GET /health

i

☐ Secure

Advanced Parameters

Destination IP

Destination Port

8008

i

Down Time

30

Second

▼

TROFS Code

TROFS String

Dynamic Time-out

i

Deviation

Second

▼

Dynamic Interval

Retries

3

i

Citrix サービス グループの構成

サービス グループを構成するには、次の手順を実行します。

手順

- 1 NetScaler ロード バランサにログインし、[NetScaler] - [トラフィック管理] - [ロード バランシング] - [サービス グループ] の順に移動します。
- 2 [追加] をクリックして、次の表に記載されているようにサービス グループを構成します。

表 7-2. サービス グループの構成

名前	健全性監視	プロトコル	SG メンバー	アドレス	ポート
vRealize Automation	vRealize Automation	SSL ブリッジ	VA1 VA2 VA3	IP アドレス	443
vRealize Orchestrator <small>注: 外部の vRealize Orchestrator インスタンスにのみ使用します。</small>	vRealize Orchestrator	SSL ブリッジ	VA1 VA2 VA3	IP アドレス	443
VMware Identity Manager	VMware Identity Manager	SSL ブリッジ	VA1 VA2 VA3	IP アドレス	443

結果

← 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

構成は次の画面のようになります。

Citrix 仮想サーバの構成

仮想サーバを構成するには、次の手順を実行します。

手順

- 1 NetScaler ロード バランサにログインし、[NetScaler] - [トラフィック管理] - [ロード バランシング] - [仮想サーバ] の順に移動します。

- 2 [追加] をクリックして、次の表に記載されているように仮想サーバを構成します。何も指定されていない場合は、デフォルト値を使用します。

表 7-3. 仮想サーバの構成

名前	プロトコル	宛先のアドレス	ポート	ロード バランシングの方法	サービス グループのバインド
vRealize Automation	SSL ブリッジ	IP アドレス	443	リスト コネクション	vRealize Automation
vRealize Orchestrator	SSL ブリッジ	IP アドレス	443	リスト コネクション	vRealize Orchestrator
VMware Identity Manager	SSL ブリッジ	IP アドレス	443	リスト コネクション	VMware Identity Manager

注： 外部の vRealize Orchestrator インスタンスにのみ使用します。

結果

構成は次の画面のようになります。

← 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

Workspace ONE Access のパーシステンス グループの構成

VMware Identity Manager のパーシステンス グループを構成するには、次の手順を実行します。

手順

- 1 NetScaler にログインし、[NetScaler] - [トラフィック管理] - [ロード バランシング] - [パーシステンス グループ] の順に移動します。
- 2 [追加] をクリックします。
- 3 [タイムアウト] を 36,000 秒に設定します。
- 4 関連するすべての仮想サーバを VMware Identity Manager に追加します。

注： vRealize Automation または vRealize Orchestrator 仮想サーバは追加しないでください。

- 5 [OK] をクリックします。

トラブルシューティング

8

この章には、次のトピックが含まれています。

- [F5 BIG-IP と OneConnect を併用した場合のプロビジョニングの失敗](#)
- [F5 BIG-IP ライセンスによるネットワーク帯域幅の制限](#)

F5 BIG-IP と OneConnect を併用した場合のプロビジョニングの失敗

仮想サーバに対して F5 BIG-IP と OneConnect 機能を併用すると、プロビジョニング タスクが失敗することがあります。

OneConnect は、ロード バランサからバックエンド サーバへの接続を多重化し、再利用されるようにします。これにより、サーバの負荷が軽減され、回復性が向上します。

SSL パススルーを備えた仮想サーバで OneConnect を使用することは F5 で推奨されておらず、プロビジョニングの試行が失敗する可能性があります。これは、ロード バランサがバックエンド サーバ間で既存のセッションを介して新しい SSL セッションを確立しようとする一方で、バックエンド サーバはクライアントが既存のセッションを開じるか再ネゴシエートすることを想定しているため、結果的に接続が切断されるために発生します。この問題を解決するには、OneConnect を無効にします。

- 1 F5 ロード バランサにログインし、[ローカル トラフィック] - [仮想サーバ] - [仮想サーバ リスト] の順に移動します。
- 2 変更する仮想サーバの名前をクリックします。
- 3 [アクセラレーション] セクションで、[OneConnect プロファイル] の [なし] を選択します。
- 4 [完了] をクリックします。

F5 BIG-IP ライセンスによるネットワーク帯域幅の制限

ロード バランサのネットワーク トラフィックが F5 BIG-IP ライセンスの制限を超えているため、プロビジョニングの失敗または vRealize Automation コンソール ページのロード中に問題が発生する場合があります。

BIG-IP プラットフォームでこの問題が発生しているかどうかを確認するには、「[How the BIG-IP VE system enforces the licensed throughput rate](#)」を参照してください。