



Rackspace Cloud への ASA 仮想の導入

Rackspace Cloud に ASA 仮想を導入できます。



重要 9.13(1)以降では、サポートされているすべての ASA 仮想 vCPU/メモリ構成ですべての ASA 仮想 ライセンスを使用できるようになりました。これにより、ASA 仮想を使用しているお客様は、さまざまな VM リソースフットプリントで実行できるようになります。

- [Rackspace Cloud への ASA 仮想の導入について \(1 ページ\)](#)
- [ASA 仮想 と Rackspace の前提条件 \(3 ページ\)](#)
- [Rackspace Cloud ネットワーク \(3 ページ\)](#)
- [Rackspace の第 0 日の構成 \(5 ページ\)](#)
- [Rackspace Cloud への ASA 仮想の導入 \(7 ページ\)](#)
- [CPU 使用率とレポート \(8 ページ\)](#)

Rackspace Cloud への ASA 仮想の導入について

Rackspace は、あらゆる主要なパブリックおよびプライベートクラウドテクノロジーにわたる専門知識とマネージドサービスを提供するリーディングプロバイダです。Rackspace Cloud は、ユーティリティ コンピューティング ベースで課金が行われるクラウドコンピューティング製品およびサービスのセットです。

Rackspace Cloud で ASA 仮想 for Rackspace を仮想アプライアンスとして導入できます。この章では、単一インスタンスの ASA 仮想 アプライアンスをインストールして構成する方法について説明します。

Rackspace Cloud のインスタンスタイプは、フレーバと呼ばれます。フレーバという用語は、RAM サイズ、vCPU、ネットワークスループット (RXTX ファクタ)、ディスク容量から成るサーバーの組み合わせを指します。次の表に、ASA 仮想の導入に適した Rackspace フレーバを示します。

表 1: Rackspace でサポートされるフレーバ

フレーバ	属性		総帯域幅
	vCPU	メモリ (GB)	
汎用 1-2	2	2	400 Mbps
汎用 1-4	4	4	800 Mbps
汎用 1-8	8	8	1.6 Gbps
コンピューティング 1-4	2	3.75	312.5 Mbps
コンピューティング 1-8	4	7.5	625 Mbps
コンピューティング 1-15	8	15	1.3 Gbps
メモリ 1-15	2	15	625 Mbps
メモリ 1-15	4	30	1.3 Gbps
メモリ 1-15	8	60	2.5 Gbps

Rackspace のフレーバについて

Rackspace 仮想クラウドサーバーのフレーバは、次のクラスに分類されます。

• 汎用 v1

- 汎用ワークロードから高パフォーマンスの Web サイトまで、さまざまなユースケースに役立ちます。
- vCPU はオーバーサブスクライブされ、「バースト可能」です。つまり、物理ホスト上のクラウドサーバーに割り当てられる vCPU の数は、物理 CPU スレッドの数よりも多くなります。

• コンピューティング v1

- Web サーバー、アプリケーションサーバー、およびその他の CPU 集約型のワークロード向けに最適化されています。
- vCPU は「予約済み」です。つまり、物理ホスト上のクラウドサーバーに割り当てられる vCPU の数は、そのホスト上の物理 CPU スレッドの数よりも多くなることはありません。

• メモリ v1

- メモリ集約型のワークロードに推奨されます。

- I/O v1

- 高速ディスク I/O のメリットを得やすい高パフォーマンスのアプリケーションおよびデータベースに最適です。

ASA 仮想 と Rackspace の前提条件

- [Rackspace](#) アカウントを作成します。

すべての Rackspace Public Cloud アカウントは、デフォルトで Managed Infrastructure サービスレベルに設定されます。クラウドコントロールパネル内で Managed Operations サービスレベルにアップグレードできます。クラウドコントロールパネルの上部で、アカウントのユーザー名をクリックし、[Upgrade Service Level] を選択します。

- ASA 仮想 へのライセンス付与。ASA 仮想 にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「[ASA 仮想のライセンス](#)」を参照してください。

- インターフェイスの要件：

- 管理インターフェイス
- 内部および外部インターフェイス
- (任意) 追加のサブネット (DMZ)

- 通信パス：

- 管理インターフェイス：ASDM に ASA 仮想 を接続するために使用され、トラフィックの通過には使用できません。
- 内部インターフェイス (必須)：内部ホストに ASA 仮想 を接続するために使用されます。
- 外部インターフェイス (必須)：ASA 仮想 をパブリック ネットワークに接続するために使用されます。
- DMZ インターフェイス (任意)：DMZ ネットワークに ASA 仮想 を接続するために使用されます。

- ASA および ASA 仮想 システムの互換性と要件については、[Cisco Secure Firewall ASA の互換性](#) [英語] を参照してください。

Rackspace Cloud ネットワーク

クラウド構成には、必要に応じて接続された複数の種類のネットワークを含めることができます。クラウドサーバーのネットワーキング機能は、多くの場合、他のネットワークと同じ方法

で管理できます。ASA 仮想の導入では、主に、Rackspace Cloud の次の3種類の仮想ネットワークと情報を交換します。

- **PublicNet** : クラウドサーバー、クラウドロードバランサ、ネットワークアプライアンスなどのクラウドインフラストラクチャ コンポーネントをインターネットに接続します。
 - PublicNet を使用して、ASA 仮想 をインターネットに接続します。
 - ASA 仮想 は、Management0/0 インターフェイスを介してこのネットワークに接続します。
 - PublicNet は、IPv4 と IPv6 のデュアルスタックです。PublicNet を使用してサーバーを作成すると、そのサーバーはデフォルトで IPv4 アドレスと IPv6 アドレスを受け取ります。
- **ServiceNet** : 各 Rackspace クラウドリージョン内の IPv4 専用の内部マルチテナントネットワーク。
 - ServiceNet は、構成内のサーバー間でトラフィック（East-West トラフィック）を伝送するように最適化されます。
 - クラウドファイル、クラウドロードバランサ、クラウドデータベース、クラウドバックアップなどのリージョン別サービスへの無料アクセスをサーバーに提供します。
 - ネットワーク 10.176.0.0/12 および 10.208.0.0/12 は ServiceNet 用に予約されています。ServiceNet 接続を備えるサーバーは、これらのネットワークのいずれかの IP アドレスを使用してプロビジョニングされます。
 - ASA 仮想 は、Gigabit0/0 インターフェイスを介してこのネットワークに接続します。
- **プライベート Cloud Networks** : Cloud Networks を使用すると、クラウドで分離された安全なネットワークを作成および管理できます。
 - これらのネットワークは単一のテナントであり、ネットワークトポロジ、IP アドレスリング（IPv4 または IPv6）、および接続するクラウドサーバーを完全に制御できます。
 - Cloud Networks はリージョンを対象範囲とし、特定のリージョン内の任意のクラウドサーバーに接続できます。
 - API を介して、または Rackspace Cloud コントロールパネルを使用して、Cloud Networks を作成および管理できます。ASA 仮想 は、Gigabit0/1 ~ Gigabit0/8 のインターフェイスを介してこれらのネットワークに接続します。

Rackspace の第 0 日の構成

Rackspace Cloud に VM を展開すると、Rackspace のプロビジョニング情報を持つファイルを含む CD-ROM デバイスが VM に接続されます。プロビジョニング情報には次の項目があります。

- ホスト名
- 必要なインターフェイスの IP アドレス
- スタティック IP ルート
- ユーザー名とパスワード (オプションの SSH 公開キー)
- DNS サーバー
- NTP サーバー

これらのファイルは初期展開時に読み込まれ、ASA の構成が生成されます。

ASA 仮想 ホスト名

デフォルトでは、ASA 仮想 ホスト名は、ASA 仮想の構築を開始するときにクラウドサーバーに割り当てる名前です。

```
hostname rackspace-asav
```

ASA ホスト名構成では、RFC 1034 および 1101 に準拠するホスト名のみ使用できます。

- 先頭と末尾が文字または数字である必要があります。
- 内側の文字は、文字、数字、またはハイフンである必要があります。



(注) ASA 仮想では、これらのルールに準拠するように、元のクラウドサーバー名にできるだけ近い名前にクラウドサーバー名が変更されます。クラウドサーバー名の先頭と末尾に特殊文字がある場合はそれを削除し、ルールに準拠しない内側の文字をハイフンに置き換えます。

たとえば、クラウドサーバーの名前が **ASAv-9.13.1.200** の場合、ホスト名は **ASAv-9-13-1-200** になります。

Interfaces

インターフェイスは次のように設定されます。

- Management0/0
 - PublicNet に接続されているため、「outside」という名前が付けられます。
- Rackspace は、IPv4 と IPv6 の両方のパブリックアドレスを PublicNet インターフェイスに割り当てます。

- Gigabit0/0
 - ServiceNet に接続されているため、「management」という名前が付けられます。
 - Rackspace は、Rackspace リージョンの ServiceNet サブネットから IPv4 アドレスを割り当てます。
- Gigabit0/1 ~ Gigabit0/8
 - プライベート Cloud Networks に接続されているため、「inside」、「inside02」、「inside03」などの名前が付けられます。
 - Rackspace は、Cloud Networks サブネットから IP アドレスを割り当てます。

3 つのインターフェイスを持つ ASA 仮想のインターフェイス構成は次のようになります。

```
interface GigabitEthernet0/0
  nameif management
  security-level 0
  ip address 10.176.5.71 255.255.192.0
!
interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.19.219.7 255.255.255.0
!
interface Management0/0
  nameif outside
  security-level 0
  ip address 162.209.103.109 255.255.255.0
  ipv6 address 2001:4802:7800:1:be76:4eff:fe20:1763/64
```

スタティック ルート

Rackspace は、次のスタティック IP ルートをプロビジョニングします。

- PublicNet インターフェイス (**outside**) 経由のデフォルト IPv4 ルート。
- PublicNet インターフェイス経由のデフォルト IPv6 ルート。
- ServiceNet インターフェイス (**management**) 上のインフラストラクチャ サブネット ルート。

```
route outside 0.0.0.0 0.0.0.0 104.130.24.1 1
ipv6 route outside ::/0 fe80::def
route management 10.176.0.0 255.240.0.0 10.176.0.1 1
route management 10.208.0.0 255.240.0.0 10.176.0.1 1
```

ログイン クレデンシャル

Rackspace によって作成されたパスワードを使用して、「admin」という名前のユーザーが作成されます。Rackspace 公開キーを使用してクラウドサーバーが展開されている場合、ユーザー「admin」の公開キーが作成されます。

```
username admin password <admin_password> privilege 15
username admin attributes
ssh authentication publickey <public_key>
```

day0 SSH 構成 :

- PublicNet インターフェイス (**outside**) 経由の SSH が IPv4 と IPv6 に対して有効になります。
- ServiceNet インターフェイス (**management**) 経由の SSH が IPv4 に対して有効になります。
- Rackspace の要求に応じて、より強力なキー交換グループを設定します。

```
aaa authentication ssh console LOCAL
ssh 0 0 management
ssh 0 0 outside
ssh ::0/0 outside
ssh version 2
ssh key-exchange group dh-group14-sha1
```

DNS と NTP

Rackspace は、DNS と NTP に使用される 2 つの IPv4 サービスアドレスを提供します。

```
dns domain-lookup outside
dns server-group DefaultDNS
name-server 69.20.0.164
name-server 69.20.0.196

ntp server 69.20.0.164
ntp server 69.20.0.196
```

Rackspace Cloud への ASA 仮想の導入

Rackspace Cloud で ASA 仮想を仮想アプライアンスとして導入できます。この手順では、単一インスタンスの ASA 仮想アプライアンスをインストールする方法を示します。

始める前に

ホスト名の要件、インターフェイスのプロビジョニング、ネットワーク情報など、ASA 仮想の導入を成功させるために Rackspace Cloud で有効にする構成パラメータの説明については、[Rackspace の第 0 日の構成 \(5 ページ\)](#) のトピックを参照してください。

ステップ 1 Rackspace mycloud ポータルで、**[SERVERS] > [CREATE RESOURCES] > [Cloud Server]** に移動します。

ステップ 2 [Create Server] ページの [Server Details] で次のように入力します。

- a) [サーバー名 (Server Name)] フィールドに ASA 仮想 マシンの名前を入力します。

b) [Region] ドロップダウンリストからリージョンを選択します。

ステップ3 [Image] で、[Linux/Appliances] > [ASAv] > [Version] を選択します。

(注) 通常、新しいASA仮想を導入する場合は、サポートされている最新バージョンを選択します。

ステップ4 [Flavor] で、リソースのニーズに合った [Flavor Class] を選択します。適切な VM のリストについては、[表 1: Rackspace でサポートされるフレーバ \(2 ページ\)](#) を参照してください。

重要 9.13(1) 以降は、ASA 仮想の最小メモリ要件は 2GB です。1 つ以上の vCPU を使用して ASA 仮想を導入する場合、ASA 仮想の最小メモリ要件は 4GB です。

ステップ5 (オプション) [Advanced Options] で、SSH キーを設定します。

Rackspace Cloud の SSH キーの詳細については、「[Managing access with SSH keys](#)」を参照してください。

ステップ6 ASA 仮想の該当する [推奨のインストール (Recommended Installs)] および [項目別のチャージ (Itemized Charges)] を確認し、[サーバーの作成 (Create Server)] をクリックします。

root 管理者のパスワードが表示されます。パスワードをコピーし、ダイアログを閉じます。

ステップ7 サーバーを作成すると、サーバーの詳細ページが表示されます。サーバーのステータスがアクティブになるまで待ちます。通常、これには数分かかります。

次のタスク

- ASA 仮想に接続します。
- SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、[ASDM の起動](#)を参照してください。

CPU 使用率とレポート

CPU 使用率レポートには、指定された時間内に使用された CPU の割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ~ 40% で動作し、ピーク時は約 60 ~ 70% の容量で動作します。

ASA Virtual の vCPU 使用率

ASA Virtual の vCPU 使用率には、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量が表示されます。

Rackspace で報告される vCPU 使用率には、ASA Virtual の使用率に加えて、次のものが含まれます。

- ASA Virtual アイドル時間
- ASA Virtual マシンに使用された %SYS オーバーヘッド

- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

CPU 使用率の統計情報を表示するには、**show cpu usage** コマンドを使用します。

例

```
Ciscoasa#show cpu usage
CPU 00005000 1%01 000 2%05 000 1%
```

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA Virtual レポート : 40%
- DP : 35%
- 外部プロセス : 5%
- ASA (ASA Virtual レポート) : 40%
- ASA アイドル ポーリング : 10%
- オーバーヘッド : 45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

Rackspace CPU 使用率レポート

使用可能なクラウドサーバーの CPU、RAM、およびディスク容量の構成情報の表示に加えて、ディスク、I/O、およびネットワーク情報も表示できます。この情報を使用して、ニーズに適したクラウドサーバーを決定してください。コマンドライン nova クライアントまたは [Cloud Control Panel](#) インターフェイスを使用して、使用可能なサーバーを表示できます。

コマンドラインで、次のコマンドを実行します。

```
nova flavor-list
```

使用可能なすべてのサーバー構成が表示されます。リストには、次の情報が含まれています。

- ID : サーバー構成 ID
- 名前 : RAM サイズとパフォーマンスタイプでラベル付けされた構成名
- Memory_MB : 構成の RAM の量
- ディスク : GB 単位のディスクサイズ (汎用クラウドサーバーの場合、システムディスクのサイズ)

- エフェメラル：データディスクのサイズ
- スワップ：スワップ領域のサイズ
- VCPU：構成に関連付けられた仮想 CPU の数
- RXTX_Factor：サーバーに接続された PublicNet ポート、ServiceNet ポート、および分離されたネットワーク（クラウドネットワーク）に割り当てられる帯域幅の量（Mbps 単位）
- Is_Public：未使用

ASA Virtual と Rackspace のグラフ

ASA Virtual と Rackspace の間には CPU % の数値に違いがあります。

- Rackspace グラフの数値は ASA Virtual の数値よりも常に大きくなります。
- Rackspace ではこの値は「%CPU usage」と呼ばれ、ASA Virtual ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

Rackspace では「%CPU usage」は次のように計算されます。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲストオペレーティングシステムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。