cloudstack DOCUMENTATION

Apache CloudStack 4.1.1

インストールガイド

エディッション 1

cloudstack™
open source cloud computing

CloudStack Apache [FAMILY Given]

法律上の通知

概要

CloudStack のためのインストールガイド。

第1章 コンセプト

1.1. CloudStack とは

CloudStack はオープンソースのソフトウェアプラットフォームで、コン ピューティングリソースをプールすることにより、パブリック、プライベート、 およびハイブリッドの IaaS(Infrastructure as a Service)クラウドを構築す ることができます。CloudStack で、クラウドインフラストラクチャを構成する ネットワーク、ストレージ、およびコンピューティングノードを管理します。 CloudStack を使用して、クラウドコンピューティング環境を展開、管理、お よび構成します。

本製品の主なユーザーはサービスプロバイダーと企業です。CloudStack を使用すると、次のタスクを実行できます。

- オンデマンドで弾力的なクラウドコンピューティングサービスをセッ トアップする。サービスプロバイダーはインターネットを経由して、セルフサービスの仮想マシンインスタンス、スト レージボリューム、およびネットワーク構成を販売できます。
- 従業員が使用するオンプレミスなプライベートクラウドをセットアップする。企業は物理マシンと同じ方法で仮想マシンを管理せずに、IT 部門を介さずにセルフサービスの仮想マシンをユーザーに提供することができます。

1.2. CloudStack の機能

複数のハイパーバイザーのサポート

CloudStack はさまざまなハイパーバイザーと連動します。単一のクラウド環境に、ハイパーバイザーの実装を複数含められます。現在の CloudStack リリースでは、エンタープライズクラスのハイパーバイザーである Citrix XenServer や VMware vSphere も CentOS, Ubuntu 上の KVM, Xen と同様にサポートされます。

高度にスケーラブルなインフラストラクチャ管理

CloudStack では、地理的に分散した複数のデータセンターに設置される、何万台ものサーバーを管理することが できます。集中型の管理サーバーを直線的に拡張できるので、中間のクラスターレベルの管理サーバーが不要 です。単一のコンポーネントに障害が発生しても、クラスターまたはクラウド全体が停止することはありません。ク ラウドで実行中の仮想マシンの機能に影響を与えずに、管理サーバーの定期保守を実行できます。

自動的な構成管理

CloudStack では、各ゲスト仮想マシンのネットワークとストレージの設定が自動的に構成されます。

CloudStack では、クラウド自体をサポートする仮想アプライアンスのプールが内部的に管理されます。これらのア プライアンスにより、ファイアウォール、ルーティング、DHCP、VPN アクセス、コンソールプロキシ、ストレージアク セス、およびストレージ複製などのサービスが提供されます。仮想アプライアンスを幅広く使用することによって、 クラウド環境のインストール、構成、および継続的な管理を大いに単純化します。

グラフィカルユーザーインターフェイス

CloudStack には、クラウドのプロビジョニングと管理のための管理者用の Web インターフェイスと、仮想マシンの 実行と仮想マシンテンプレートの管理のためのエンドユーザー用の Web インターフェイスが搭載されています。 ユーザーインターフェイスは、サービスプロバイダーまたは企業が希望する外観になるようにカスタマイズできま す。

標準 API のサポート

CloudStack provides an API that gives programmatic access to all the management features available in the UI. The API is maintained and documented. This API enables the creation of command line tools and new user interfaces to suit particular needs. See the Developer's Guide and API Reference, both available at Apache CloudStack Guides and Apache CloudStack API Reference respectively.

CloudStack のプラッガブルなアロケーターのアーキテクチャはホストやストレージに対する新しいタイプの割り当てを許容しています。以下のアロケーター実装ガイドも参照して下さい。http://docs.cloudstack.org/CloudStack_Documentation/Allocator_Implementation_Guide

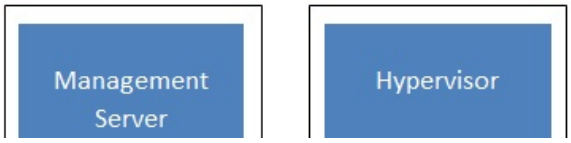
高可用性

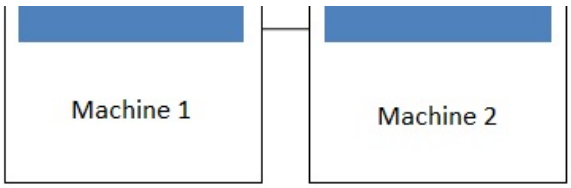
CloudStack は可用性を高めるためシステムに幾つかの機能を持っています。管理サーバーを複数ノードにインストールし、サーバー間でロードバランシングをすることが出来ます。MySQLをデータベースの障害時に手動でフェイルオーバーするためレプリケーションの設定をすることも可能でしょう。ホストに対しては CloudStack はNICのボンディングやiSCSIのマルチパスのようにストレージ通信を分割することをサポートしています。

1.3. 展開アーキテクチャの概要

CloudStack のインストールは、管理サーバーおよび管理サーバーで管理するクラウドインフラストラクチャの 2 つの部分に分けられます。CloudStack クラウドのセットアップと管理においては、ホスト、ストレージデバイス、および IP アドレスのようなリソースを管理者が管理サーバーに準備し、管理サーバーがそれらのリソースを管理します。

最小構成でインストールする場合は、CloudStack 管理サーバーを実行する 1 台のマシンとクラウドインフラストラクチャとして動作するもう 1 台のマシンをセットアップします。この場合のクラウドインフラストラクチャは非常に単純で、ハイパーバイザーソフトウェアを実行する 1 台のホストで構成されます。最小の展開では 1 台のマシン上で管理サーバーとハイパーバイザーホストの両方を担うことができます。(その場合、KVM ハイパーバイザーを利用します)





Simplified view of a basic deployment

A more full-featured installation consists of a highly-available multi-node Management Server installation and up to tens of thousands of hosts using any of several advanced networking setups. For information about deployment options, see the "Choosing a Deployment Architecture" section of the $PRODUCT; Installation Guide.

1.3.1. 管理サーバーについて

管理サーバーは、クラウドリソースを管理する CloudStack ソフトウェアです。ユーザーインターフェイスまたは API を介して 管理サーバーを操作することにより、クラウドインフラストラクチャを構成し管理できます。

管理サーバーは専用のサーバーまたは仮想マシンです。ホストに対する仮想マシンの割り当てを制御し、ストレージと IP アドレスを仮想マシンインスタンスに割り当てます。CloudStack 管理サーバーは Tomcat コンテナー内で動作し、データ保 持のために MySQL データベースを必要とします。

このマシンは「4.3: 最小システム要件」にあるシステム要件を満たしている必要があります。

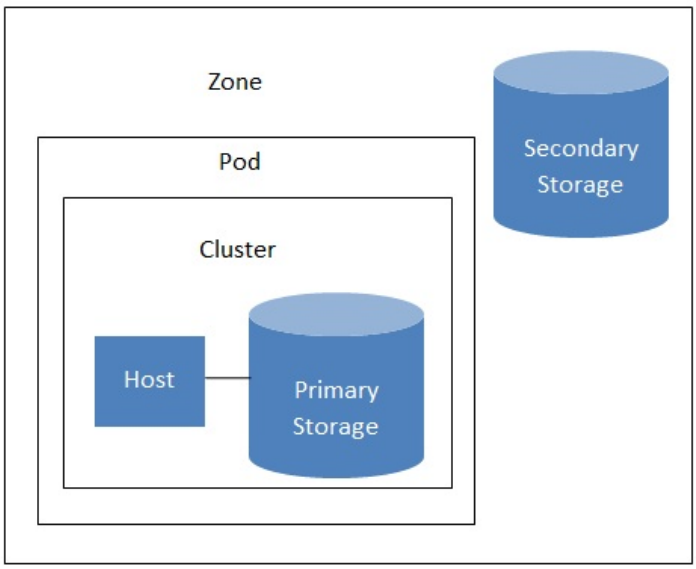
管理サーバー

- 管理者とエンドユーザーに Web ユーザーインターフェイスを提供します。
- CloudStack プラットフォームの API を提供します。
- 特定ホストに対するゲスト仮想マシンの割り当てを管理します。
- 特定アカウントに対するパブリックおよびプライベート IP アドレスの割り当てを管理します。
- ゲストに対する仮想ディスクとしてのストレージの割り当てを管理します。
- スナップショット、テンプレート、および ISO イメージを管理し、場合によっては複数のデータセンターの間でそれらを 複製します。
- クラウド構成のための単一の場を提供します。

1.3.2. クラウドインフラストラクチャの概要

名前が示すとおり、管理サーバーで 1 つ以上のゾーンを管理します。ゾーンは通常データセンターに相当し、ゲスト仮想マ シンが動作するホストコンピューターを含みます。クラウドインフラストラクチャは次のように組織されます。

- ゾーン:通常、1 つのゾーンは単一のデータセンターに相当します。ゾーンは 1 つ以上のポッドとセカンダリストレー ジから構成されます。
- ポッド:普通、ポッドはレイヤー2スイッチと1つ以上のクラスターを含む1ラック分のハードウェアです。
- クラスター:クラスターは 1 つ以上のホストとプライマリストレージから構成されます。
- ホスト:クラスター内の単一のコンピューティングノードです。実際のクラウドサービスは、ゲスト仮想マシンの形式でホストから提供されます。
- プライマリストレージはクラスターと関連付けられ、そのクラスター内のホスト上で動作するすべての仮想マシンのディスクボリュームを格納します。
- セカンダリストレージはゾーンと関連付けられ、テンプレート、ISO イメージ、およびディスクボリュームのスナップショットを格納します。



Nested organization of a zone

詳細情報

より詳細な情報はドキュメントの「クラウドインフラストラクチャコンセプト」を参照してください。

1.3.3. ネットワーク

CloudStack では基本と拡張の 2 種類のネットワーク設定を提供します。

- 基本ネットワーク。 基本ネットワーク設定では、AWSスタイルのネットワークの単一共有ネットワークを提供します。セキュリティグループ(発信元 IP アドレスのフィルター) のようなレイヤー3 レベルの方法でゲストを分離できます。
- 拡張ネットワーク。拡張ネットワー ク設定は、より洗練されたネットワーク技術をサポートします。このネットワークモデルを選択すると、より柔軟にゲストの ネットワークを定義できます。

詳しくは、「ネットワークセットアップ」を参照してください。

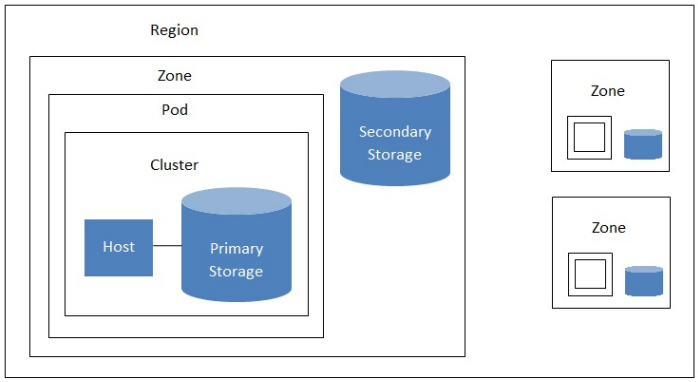
第2章 クラウドインフラストラクチャのプロビジョニング

2.1. About Regions

To increase reliability of the cloud, you can optionally group resources into multiple geographic regions. A region is the largest available organizational unit within a CloudStack deployment. A region is made up of several availability zones, where each zone is roughly equivalent to a datacenter. Each region is controlled by its own cluster of Management Servers, running in one of the zones. The zones in a region are typically located in close geographical proximity. Regions are a useful technique for providing fault tolerance and disaster recovery.

By grouping zones into regions, the cloud can achieve higher availability and scalability. User accounts can span regions, so that users can deploy VMs in multiple, widely-dispersed regions. Even if one of the regions becomes unavailable, the services are still available to the end-user through VMs deployed in another region. And by grouping communities of zones under their own nearby Management Servers, the latency of communications within the cloud is reduced compared to managing widely-dispersed zones from a single central Management Server.

Usage records can also be consolidated and tracked at the region level, creating reports or invoices for each geographic region.



A region with multiple zones

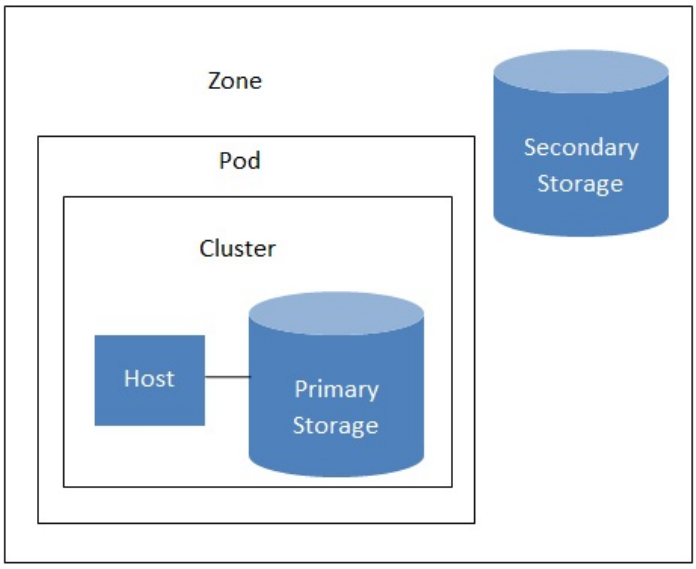
Regions are visible to the end user. When a user starts a guest VM, the user must select a region for their guest. Users might also be required to copy their private templates to additional regions to enable creation of guest VMs using their templates in those regions.

2.2. ゾーンについて

A zone is the second largest organizational unit within a CloudStack deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple zones in a datacenter. The benefit of organizing infrastructure into zones is to provide physical isolation and redundancy. For example, each zone can have its own power supply and network uplink, and the zones can be widely separated geographically (though this is not required).

ゾーンは次のものから構成されます。

- 1つ以上のポッド。各ポッドはホストを含む1つ以上のクラスターと、1つ以上のプライマリストレージサーバーから構成されます。
- セカンダリストレージ。ゾーン内のすべてのポッドで共有されます。



Nested organization of a zone

ゾーンはユーザーが確認することができ、ユーザーがゲストVMを起動させた際ゾーンを選択する必要があります。また、ユーザーは追加ゾーンでプライベートのテンプレートを利用する場合追加ゾーンに対してテンプレートのコピーを実施する必要があります。

ゾーンはパブリック、プライベートを選択でき、パブリックゾーンは全てのユーザーに対して公開されます。これはどのユーザーもゾーンに対してゲストVMを作成することを意味します。プライベートゾーンは特定のドメインに対し予約され、対象ドメインもしくはそのサブドメインのユーザーのみがゾーンに対してゲストVMを作成できます。

同一ゾーンのホストはファイアウォールを介さず直接互いにアクセス可能であり、異種ゾーン間のホストは静的に設定されたVPNトンネルを介して通信します。

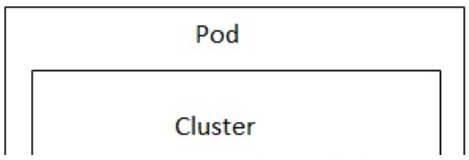
各ゾーンに対して管理者は以下について設計する必要があります。

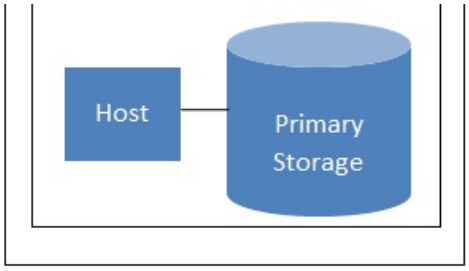
- いくつのポッドをゾーンに配置するか。
- いくつのクラスターを各ポッドに配置するか。
- いくつのホストを各クラスターに配置するか。
- いくつのプライマリストレージサーバーを各クラスターに配置し、総容量をどうするか。
- いくつのセカンダリストレージサーバーをゾーンに配置するか。

新しいゾーンを追加した際は、まずゾーンに対し物理ネットワークや第一のポッド、クラスター、ホスト、プライマリストレージ、セカンダリストレージを設定します。

2.3. ポッドについて

A pod often represents a single rack. Hosts in the same pod are in the same subnet. A pod is the second-largest organizational unit within a CloudStack deployment. Pods are contained within zones. Each zone can contain one or more pods. A pod consists of one or more clusters of hosts and one or more primary storage servers. Pods are not visible to the end user.





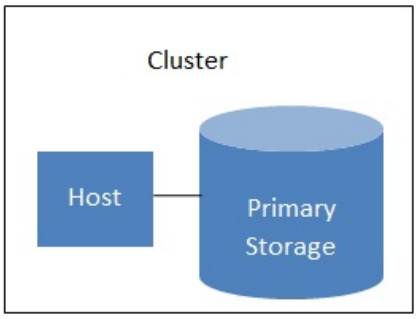
A simple pod

2.4. クラスタについて

クラスターはホストをグループ化する方法です。これは XenServer のサーバープール、KVM サーバーのセットもしくは vCenter で事前用意された VMware cluster に相当します。クラスター内の全てのホストはすべて同一のハードウェアから構成され、同じハイパーバイザーを実行し、同じサブネット上にあり、同じ共有プライマリストレージにアクセスします。仮想マシンインスタンスはクラスター内のあるホストから他のホストにユーザーへのサービスを中断せずにライブマイグレーションすることができます。

クラスタはCloudStackの3番目に大きい管理単位です。クラスタはポッドに格納され、ポッドはゾーンに格納されます。クラスタ内のホスト台数は、基盤のハイパーバイザーにより制限されますが、ほとんどの場合CloudStackはより少ない台数を推奨しますので、ベストプラクティスを確認してください。

クラスタは1つ以上のホストと1つ以上のプライマリストレージから成り立ちます。



A simple cluster

CloudStackは1つのクラウドに複数のクラスタを含めることを認めています。

ローカルストレージを利用している場合クラスター毎にホストが1つしかない場合でもクラスターを組織化する必要があります。

VMware を使用する場合、すべての VMware クラスタは vCenter Server に管理されます。管理者は vCenter を CloudStack に登録する必要があります。1つのゾーンには複数の vCenter Server が存在する可能性があります。それぞれの vCenter Server の配下には、複数の VMware クラスタが存在する可能性があります。

2.5. ホストについて

ホストは単一のコンピューターです。ホストは、ゲスト仮想マシンを実行するコンピューティングリソースを提供します。各ホストにはゲスト仮想マシンを管理するためのハイパーバイザーソフトウェアをインストールしま す。たとえば、KVM が有効な Linux サーバー、Citrix XenServer が動作するサーバー、および ESXi サーバーがホストです。

ホストは CloudStack 環境内の最小の組織単位です。ホストはクラスターに含まれ、クラスターはポッドに含まれ、ポッドは ゾーンに含まれます。

CloudStack 環境内のホストには次の機能があります。

- 仮想マシンをホストするために必要な CPU、メモリ、ストレージ、およびネットワークリソースを提供します。
- 高帯域幅の TCP/IP ネットワークに相互接続して、インターネットに接続します。
- 地理的に異なる複数データセンターに横断的に配置されています。
- 1 つのクラスター内のホストはすべて同種である必要がありますが、CPU 速度や RAM サイズなど、能力が異なる可能性があります。

ゲストVMの能力を向上させるためにいつでもホストを追加できます。

CloudStack は自動的にホストのCPU、メモリのリソースを検出します。

ホストはユーザーに対し不可視であり、ユーザーはどのホストに対しゲストVMが割り当てられているかわかりません。

CloudStack 内のホストを機能させるには、次の作業が必要です。

- ホストにハイパーバイザーソフトウェアをインストールする。
- ホストに IP アドレスを割り当てる。
- ホストが CloudStack 管理サーバーに接続していることを確認する

- ホストがCloudStack管理サーバーに接続していることを確認する。

2.6. プライマリストレージについて

プライマリストレージはクラスターと関連付けられ、そのクラスター内のホスト上で動作するすべての仮想マシンのディスクボリュームを格納します。複数のプライマリストレージをクラスターに追加することができ、少なくとも1つのプライマリストレージが必要です。通常はパフォーマンス向上のため、ホストの近くに配置します。

CloudStack は利用するハイパーバイザーでサポートされている全ての標準規格に沿ったiSCSI、NFSに対応するよう設計されています。それは次にしめすデバイスを含みます。

- Dell EqualLogic™ for iSCSI
- Network Appliances filers for NFS and iSCSI
- Scale Computing for NFS

もし、ローカルディスクのみを使ってインストールを進める場合、次のセカンダリストレージにスキップすることができます。

2.7. セカンダリストレージについて

セカンダリストレージはゾーンと関連付けられ、次の項目を格納します。

- テンプレート – 仮想マシンの起動に使用できるオペレーティングシステムイメージで、アプリケーションのインストールなど追加の構成を含めることができます。
- ISO イメージ – データまたはオペレーティングシステムの起動可能なメディアを含むディスクイメージです。
- ディスクボリュームのスナップショット – 仮想マシンデータの保存コピーです。データの復元または新しいテンプ\nレートの作成に使用できます。

セカンダリストレージ内の項目は、ゾーン内のすべてのホストで使用できます。CloudStack は特定のプライマリストレージデバイスに対するゲストVMの仮想ディスクを管理します。

セカンダリストレージ内の項目をクラウドを介して全てのホストで利用可能にするには OpenStack オブジェクトストレージ(Swift, swift.openstack.org) をセカンダリストレージに追加することができます。Swiftを使う場合、Swiftストレージを CloudStack 全体で構成します。通常通りセカンダリストレージを各ゾーンで設定すると、各ゾーンのセカンダリストレージは全てのテンプレートや他のセカンダリストレージのデータをSwiftに中継します。Swiftストレージはクラウド全体に渡るリソースとして動作し、作成されたテンプレートやその他のデータがクラウド上のあらゆるゾーンから利用可能になります。Swiftストレージは階層的な構造ではなく、ストレージオブジェクト毎に単一のSwiftコンテナーが用意されます。クラウド上の全てのセカンダリストレージは必要に応じSwiftからコンテナーを取得します。その際、あるゾーンから他のゾーンに対してテンプレートやスナップショットをコピーする必要はなく、単一のNFSのように扱うことができ、全てのデータはあらゆる場所から利用可能になります。

2.8. 物理ネットワークについて

ゾーン追加時に物理ネットワークを設定します。拡張ゾーンにおいて1つもしくは複数の物理ネットワークを各ゾーン関連付けることができます。これはホストのハイパーバイザーにおけるNICに相当し、各物理ネットワークは1つもしくは複数のネットワークのトラフィックタイプを転送します。各ネットワークに対するトラフィックタイプの選択はゾーン作成時に基本ネットワーク、拡張ネットワークのどちらを選択したかに強く依存します。

物理ネットワークはゾーンにおけるネットワークハードウェアやケーブルの配線に相当し、複数の物理ネットワークを持たせることができます。管理者は次のようなことができます。

- ゾーン内の物理ネットワークの追加/削除/更新
- 物理ネットワークのVLAN設定
- ハイパーバイザーからネットワークを認識するための名前の設定
- 物理ネットワーク上で利用可能なサービスプロバイダーの設定(ファイアウォール、ロードバランサー等)
- 物理ネットワークに渡すIPアドレスの設定
- 物理ネットワークで流れるトラフィックタイプの指定

2.8.1. 基本ゾーンのネットワークトラフィックの種類

基本ネットワーク設定を使用する場合は、ゾーンで使用できる物理ネットワークは 1 つだけです。その物理ネットワークでは、次の 3 種類のトラ フィックが伝送されます。

- ゲスト : エンドユーザーが仮想マシンを実行すると、ゲストトラフィックが生成されます。ゲスト仮想マシンは、ゲストネットワークと呼ばれるネットワークを介して互いに通信します。基本ゾーンの各ポッドはブロードキャストドメイン なので、ゲストネットワークに対してそれぞれ異なる IP アドレス範囲を持ちます。管理者は、各ポッドの IP アドレス 範囲を構成する必要があります。
- Management. When CloudStack's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudStack to perform various tasks in the cloud), and any other component that communicates directly with the CloudStack Management Server. You must configure the IP range for the system VMs to use.

  注記

  管理トラフィックとゲストトラフィックに別々の NIC を使用することを強くお勧めします。

- パブリック : パブリックトラフィックはクラウド上の仮想マシンがインターネットにアクセスする際に生成されます。これには外部からアクセス可能な IP が割り当てられなければいけません。「新規 IP アドレスの取得」に記述されているようにエンドユーザーはこれらの IP を CloudStack ユーザーインターフェースから取得しゲストネットワークとパブリックネットワーク間の NAT を実現できます。
- Storage. While labeled "storage" this is specifically about secondary storage, and doesn't affect traffic for primary storage. This includes traffic such as VM templates and snapshots, which is sent between the secondary storage VM

storage. This includes traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudStack uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.

基本ネットワークの場合は、物理ネットワークの構成はごく簡単です。多くの場合、'構成する必要があるのはゲスト仮想マシンが生成するトラフィックを伝送するための 1 つのゲストネットワークだけです。もしNetScaler ロードバランサーを用い、エラスティック IP や エラスティックロードバランサー(EIP, ELB) 機能を利用する場合はパブリックトラフィックを転送するためのネットワークを設定しなければなりません。CloudStack ではユーザーインターフェースから新しいゾーンを追加する際に必要なネットワーク設定に注意を払う必要があります。

2.8.2. 基本ゾーンのゲスト IP アドレス

基本ネットワーク設定を使用する場合は、CloudStack はポッドの CIDR の IP アドレスをそのポッドのゲストに割り当てます。 管理者は、そのためにポッドの直接 IP アドレスの範囲を追加する必要があります。これらの IP アドレスはホストと同じ VLAN に含まれます。

2.8.3. 拡張ゾーンのネットワークトラフィックの種類

拡張ネットワーク設定を使用する場合は、ゾーンで複数の物理ネットワークを使用できます。各物理ネットワークで 1 つまたは複数の種類のトラフィックを伝送できます。各ネットワークで伝送するネットワークトラフィックの種類を、CloudStack に 識別させる必要があります。拡張ゾーンのトラフィックには次の種類があります。

- ゲスト : エンドユーザーが仮想マシンを実行すると、ゲストトラフィックが生成されます。ゲスト仮想マシンは、ゲストネットワークと呼ばれるネットワークを介して互いに通信します。このネットワークは、分離することも共有すること もできます。分離されたゲストネットワークの場合は、管理者は各 CloudStack アカウントのネットワークを分離するための VLAN 範囲を予約する必要があります(多数の VLAN が必要になる可能性があります)。共有されたゲ ストネットワークでは、すべてのゲスト仮想マシンが 1 つのネットワークを共有します。この場合は、セキュリティグループなどのレイヤー3 のネットワーク分離技術を使用して分離を提供できます。
- 管理 : CloudStack の内部リソースが互いに通信すると、管理トラフィックが生成されます。これには、ホスト、システム仮想マシン(クラウド内のさまざまなタスクを実行するために CloudStack によって使用される仮想マシン)、および CloudStack 管理サーバーと直接通信するほかのコンポーネントの間の通信が含まれます。使用するシステム仮想マシンの IP 範囲を構成する必要があります。
- パブリック : パブリックトラフィックは、クラウド内の仮想マシンがインターネットにアクセスすると生成されます。このために、パブリックにアクセスできる IP アドレスを割り当てる必要があります。エンドユーザーは、「新規 IP アドレスの取得」にあるように CloudStack ユーザーインターフェイスを使用してそれらの IP アドレスを取得して、ゲストネットワークとパブリックネットワークの間に NAT を実装できます。
- Storage. While labeled "storage" this is specifically about secondary storage, and doesn't affect traffic for primary storage. This includes traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudStack uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of a storage NIC that always operates on a high bandwidth network allows fast template and snapshot copying. You must configure the IP range to use for the storage network.

これらのトラフィックは、それぞれ異なる物理ネットワークで伝送することも、一定の制限の下に同じ物理ネットワークで伝送することもできます。ユーザーインターフェイスでゾーンの追加ウィザードを使用して新しいゾーンを作成すると、有効な選択肢のみが提示されます。

2.8.4. 拡張ゾーンのゲスト IP アドレス

拡張ネットワーク設定を使用する場合は、ゲストが使用するための追加のネットワークを作成できます。それらのネットワークは、ゾーン全体を対象にしてすべてのアカウントが使用できるようにすることも、単一のアカウントを対象にすること もできます。後者の場合、それらのネットワークに接続するゲストを作成できるのはそのアカウントだけになります。ネットワークは、VLAN ID、IP アドレス範囲、およびゲートウェイによって定義されます。管理者は、こうしたネットワークを必要に応じて何千もプロビジョニングできます。

2.8.5. 拡張ゾーンのパブリック IP アドレス

拡張ネットワーク設定を使用する場合は、ゲストが使用するための追加のネットワークを作成できます。それらのネットワークは、ゾーン全体を対象にしてすべてのアカウントが使用できるようにすることも、単一のアカウントを対象にすること もできます。後者の場合、それらのネットワークに接続するゲストを作成できるのはそのアカウントだけになります。ネットワークは、VLAN ID、IP アドレス範囲、およびゲートウェイによって定義されます。管理者は、こうしたネットワークを必要に応じて何千もプロビジョニングできます。

2.8.6. システムにより予約済みの IP アドレス

各ゾーンで、管理ネットワーク用に予約済みの IP アドレスの範囲を構成する必要があります。このネットワークは、CloudStack 管理サーバーとさまざまなシステム仮想マシン(セカンダリストレージ仮想マシン、コンソールプロキシ仮想マシン、DHCP など)の間の通信に使用されます。

予約済みの IP アドレスは、クラウド全体で一意である必要があります。たとえば、2 つのゾーンのホストに同じプライベート IP アドレスを使用することはできません。

ポッド内のホストにはプライベート IP アドレスが割り当てられます。これは通常、RFC1918 アドレスです。コンソールプロキシとセカンダリストレージのシステム仮想マシンにも、それらが作成されたポッドの CIDR のプライベート IP アドレスが割り当てられます。

コンピューティングサーバーと管理サーバーはシステム予約 IP 範囲外の IP アドレスを利用します。例として、システム予約 IP 範囲が 192.168.154.2 から始まり 192.168.154.7 で終わる場合、CloudStack は .2 から .7 をシステム仮想マシンに利用できます。 これはポッドの CIDR とは別になり .8 から .254 を管理サーバーやハイパーバイザーホストに利用できます。

全てのゾーンで：

各ポッドのシステムにプライベート IP アドレスを割り当てて、CloudStack で準備します。

KVM と XenServer で推奨されるポッドあたりのプライベート IP アドレスの数は、ホストごとに 1 つです。ポッドの拡張が

KVM と XenServer で推奨されるホストあたりのプライベート IP アドレスの数は、次のとおりです。ホストの拡張が予想される場合は、拡張に対応できるだけの数のプライベート IP アドレスをあらかじめ追加しておきます。

拡張ネットワーク設定を使用するゾーンで：

ゾーンに対し拡張ネットワーク設定を使用する場合は、顧客の合計数に必要な CloudStack システム仮想マシンの数を加えた数のプライベート IP アドレスを準備することをお勧めします。通常は、システム仮想マシン用に約 10 個の IP アドレスが追加で必要になります。システム仮想マシンについて詳しくは、「システム仮想マシンの操作」を参照してください。

拡張ネットワーク設定を使用する場合は、各ポッドで使用できるプライベート IP アドレスの数は、そのポッドのノードで実行するハイパーバイザーによって異なります。Citrix XenServer と KVM ではリンクローカルアドレスが使用されるため、理論上は、アドレスブロック内で 65,000 を超える数のプライベート IP アドレスを使用できます。次第にポッドが拡張されても、ホ ストやゲスト仮想ルーターの IP アドレスが足りなくなることはまずありません。一方、VMWare ESXi では、管理者が指定するサブネット方式が使用されるため、一般的なポッドあたりの IP アドレスの数は 255 個のみです。これらのアドレスは、物理マシン、ゲスト仮想ルーター、およびそのほかのエンティティに割り当てられるため、ノードで ESXi が実行されているポッ ドを拡張するときには、プライベート IP アドレスが足りなくなる可能性があります。

拡張ネットワーク設定を使用する ESXi ポッドでプライベート IP 領域を拡張するための適切な余裕を確保するには、次のどちらか、または両方の方法を使用します。

- サブネットに対してより大きい CIDR ブロックを指定する。サフィックスが/20 のサブネットマスクでは、4,000 個を超える IP アドレスを提供できます。
- 複数のポッドを、それぞれ独自のサブネットを指定して作成する。たとえば、10 個のポッドを作成し、各ポッドに 255 個の IP を持たせる場合、2,550 個の IP アドレスを提供できます。

第3章 Building from Source

The official CloudStack release is always in source code form. You will likely be able to find "convenience binaries," the source is the canonical release. In this section, we'll cover acquiring the source release and building that so that you can deploy it using Maven or create Debian packages or RPMs.

Note that building and deploying directly from source is typically not the most efficient way to deploy an IaaS. However, we will cover that method as well as building RPMs or Debian packages for deploying CloudStack.

The instructions here are likely version-specific. That is, the method for building from source for the 4.0.x series is different from the 4.1.x series.

If you are working with a unreleased version of CloudStack, see the INSTALL.md file in the top-level directory of the release.

3.1. Getting the release

You can download the latest CloudStack release from the Apache CloudStack project download page.

Prior releases are available via archive.apache.org as well. See the downloads page for more information on archived releases.

You'll notice several links under the 'Latest release' section. A link to a file ending in **`tar.bz2`**, as well as a PGP/GPG signature, MD5, and SHA512 file.

- The **`tar.bz2`** file contains the Bzip2-compressed tarball with the source code.
- The **`.asc`** file is a detached cryptographic signature that can be used to help verify the authenticity of the release.
- The **`.md5`** file is an MD5 hash of the release to aid in verify the validity of the release download.
- The **`.sha`** file is a SHA512 hash of the release to aid in verify the validity of the release download.

3.2. Verifying the downloaded release

There are a number of mechanisms to check the authenticity and validity of a downloaded release.

3.2.1. Getting the KEYS

To enable you to verify the GPG signature, you will need to download the KEYS file.

You next need to import those keys, which you can do by running:

```
# gpg --import KEYS
```

3.2.2. GPG

The CloudStack project provides a detached GPG signature of the release. To check the signature, run the following command:

```
$ gpg --verify apache-cloudstack-4.0.0-incubating-src.tar.bz2.asc
```

If the signature is valid you will see a line of output that contains 'Good signature'.

3.2.3. MD5

In addition to the cryptographic signature, CloudStack has an MD5 checksum that you can use to verify the download matches the release. You can verify this hash by executing the following command:

```
$ gpg --print-md MD5 apache-cloudstack-4.0.0-incubating-src.tar.bz2 | diff - apache-
cloudstack-4.0.0-incubating-src.tar.bz2.md5
```

If this successfully completes you should see no output. If there is any output from them, then there is a difference between the hash you generated locally and the hash that has been pulled from the server.

3.2.4. SHA512

In addition to the MD5 hash, the CloudStack project provides a SHA512 cryptographic hash to aid in assurance of the validity of the downloaded release. You can verify this hash by executing the following command:

```
$ gpg --print-md SHA512 apache-cloudstack-4.0.0-incubating-src.tar.bz2 | diff - apache-
cloudstack-4.0.0-incubating-src.tar.bz2.sha
```

If this command successfully completes you should see no output. If there is any output from them, then there is a difference between the hash you generated locally and the hash that has been pulled from the server.

3.3. Prerequisites for building Apache CloudStack

There are a number of prerequisites needed to build CloudStack. This document assumes compilation on a Linux system that uses RPMs or DEBs for package management.

You will need, at a minimum, the following to compile CloudStack:

1. Maven (version 3)
2. Java (OpenJDK 1.6 or Java 7/OpenJDK 1.7)
3. Apache Web Services Common Utilities (ws-commons-util)
4. MySQL
5. MySQLdb (provides Python database API)
6. Tomcat 6 (not 6.0.35)
7. genisoimage
8. rpmbuild or dpkg-dev

3.4. Extracting source

Extracting the CloudStack release is relatively simple and can be done with a single command as follows:

```
$ tar -jxvf apache-cloudstack-4.1.1.src.tar.bz2
```

You can now move into the directory:

```
$ cd ./apache-cloudstack-4.1.1-src
```

3.5. Building DEB packages

In addition to the bootstrap dependencies, you'll also need to install several other dependencies. Note that we recommend using Maven 3, which is not currently available in 12.04.1 LTS. So, you'll also need to add a PPA repository that includes Maven 3. After running the command **`add-apt-repository`**, you will be prompted to continue and a GPG key will be added.

```
        $ sudo apt-get update
        $ sudo apt-get install python-software-properties
        $ sudo add-apt-repository ppa:natecarlson/maven3
        $ sudo apt-get update
        $ sudo apt-get install ant debhelper openjdk-6-jdk tomcat6 libws-commons-util-java
genisoimage python-mysqldb libcommons-codec-java libcommons-httpclient-java liblog4j1.2-
java maven3
```

Now that we have resolved the dependencies we can move on to building CloudStack and packaging them into DEBs.

```
        mvn clean install -P developer,systemvm
        $ dpkg-buildpackage -uc -us
```

This command will build seven Debian packages. You should have the following:

- cloudstack-agent_4.1.1_all.deb
- cloudstack-awsapi_4.1.1_all.deb
- cloudstack-cli_4.1.1_all.deb
- cloudstack-common_4.1.1_all.deb
- cloudstack-docs_4.1.1_all.deb
- cloudstack-management_4.1.1_all.deb
- cloudstack-usage_4.1.1_all.deb

3.5.1. Setting up an APT repo

After you've created the packages, you'll want to copy them to a system where you can serve the packages over HTTP. You'll create a directory for the packages and then use **dpkg-scanpackages** to create **Packages.gz**, which holds information about the archive structure. Finally, you'll add the repository to your system(s) so you can install the packages using APT.

The first step is to make sure that you have the **dpkg-dev** package installed. This should have been installed when you pulled in the **debhelper** application previously, but if you're generating **Packages.gz** on a different system, be sure that it's installed there as well.

```
$ sudo apt-get install dpkg-dev
```

The next step is to copy the DEBs to the directory where they can be served over HTTP. We'll use **/var/www/cloudstack/repo** in the examples, but change the directory to whatever works for you.

```
            sudo mkdir -p /var/www/cloudstack/repo/binary
            sudo cp *.deb /var/www/cloudstack/repo/binary
            sudo cd /var/www/cloudstack/repo/binary
            sudo dpkg-scanpackages . /dev/null | tee Packages | gzip -9 > Packages.gz
```

Note: Override Files

You can safely ignore the warning about a missing override file.

Now you should have all of the DEB packages and **Packages.gz** in the **binary** directory and available over HTTP. (You may want to use **wget** or **curl** to test this before moving on to the next step.)

3.5.2. Configuring your machines to use the APT repository

Now that we have created the repository, you need to configure your machine to make use of the APT repository. You can do this by adding a repository file under **/etc/apt/sources.list.d**. Use your preferred editor to create **/etc/apt/sources.list.d/cloudstack.list** with this line:

```
deb http://server.url/cloudstack/repo binary ./
```

Now that you have the repository info in place, you'll want to run another update so that APT knows where to find the CloudStack packages.

```
$ sudo apt-get update
```

You can now move on to the instructions under Install on Ubuntu.

3.6. Building RPMs from Source

As mentioned previously in 「Prerequisites for building Apache CloudStack」, you will need to install several prerequisites before you can build packages for CloudStack. Here we'll assume you're working with a 64-bit build of CentOS or Red Hat Enterprise Linux.

```
# yum groupinstall "Development Tools"
```

```
# yum install java-1.6.0-openjdk-devel.x86_64 genisoimage mysql mysql-server ws-commons-
util MySQL-python tomcat6 createrepo
```

Next, you'll need to install build-time dependencies for CloudStack with Maven. We're using Maven 3, so you'll want to grab a Maven 3 tarball and uncompress it in your home directory (or whatever location you prefer):

```
$ tar zxvf apache-maven-3.0.4-bin.tar.gz
```

```
$ export PATH=/usr/local/apache-maven-3.0.4//bin:$PATH
```

Maven also needs to know where Java is, and expects the JAVA_HOME environment variable to be set:

```
$ export JAVA_HOME=/usr/lib/jvm/jre-1.6.0-openjdk.x86_64/
```

Verify that Maven is installed correctly:

Verify that Maven is installed correctly.

```
$ mvn --version
```

You probably want to ensure that your environment variables will survive a logout/reboot. Be sure to update **~/.bashrc** with the PATH and JAVA_HOME variables.

Building RPMs for $PRODUCT; is fairly simple. Assuming you already have the source downloaded and have uncompressed the tarball into a local directory, you're going to be able to generate packages in just a few minutes.

Packaging has Changed

If you've created packages for $PRODUCT; previously, you should be aware that the process has changed considerably since the project has moved to using Apache Maven. Please be sure to follow the steps in this section closely.

3.6.1. Generating RPMS

Now that we have the prerequisites and source, you will cd to the **packaging/centos63/** directory.

```
$ cd packaging/centos63
```

Generating RPMs is done using the **package.sh** script:

```
$ ./package.sh
```

That will run for a bit and then place the finished packages in **dist/rpmbuild/RPMS/x86_64/**.

You should see six RPMs in that directory:

- **cloudstack-agent-4.1.1.el6.x86_64.rpm**
- **cloudstack-awsapi-4.1.1.el6.x86_64.rpm**
- **cloudstack-cli-4.1.1.el6.x86_64.rpm**
- **cloudstack-common-4.1.1.el6.x86_64.rpm**
- **cloudstack-management-4.1.1.el6.x86_64.rpm**
- **cloudstack-usage-4.1.1.el6.x86_64.rpm**

Filename Variations

The file names may vary slightly. For instance, if you were to build the RPMs on a Fedora 18 system, you'd see "fc18" instead of "el6" in the filename. (Fedora 18 isn't a supported platform at this time, just providing an example.)

3.6.1.1. Creating a yum repo

While RPMs is a useful packaging format - it's most easily consumed from Yum repositories over a network. The next step is to create a Yum Repo with the finished packages:

```
$ mkdir -p ~/tmp/repo
```

```
$ cp dist/rpmbuild/RPMS/x86_64/*rpm ~/tmp/repo/
```

```
$ createrepo ~/tmp/repo
```

The files and directories within **~/tmp/repo** can now be uploaded to a web server and serve as a yum repository.

3.6.1.2. Configuring your systems to use your new yum repository

Now that your yum repository is populated with RPMs and metadata we need to configure the machines that need to install $PRODUCT;. Create a file named **/etc/yum.repos.d/cloudstack.repo** with this information:

```
[apache-cloudstack]
name=Apache CloudStack
baseurl=http://webserver.tld/path/to/repo
enabled=1
gpgcheck=0
```

Completing this step will allow you to easily install $PRODUCT; on a number of machines across the network.

3.7. Building Non-OSS

If you need support for the VMware, NetApp, F5, NetScaler, SRX, or any other non-Open Source Software (nonoss) plugins, you'll need to download a few components on your own and follow a slightly different procedure to build from source.

Why Non-OSS?

Some of the plugins supported by CloudStack cannot be distributed with CloudStack for licensing reasons. In some cases, some of the required libraries/JARs are under a proprietary license. In other cases, the required libraries may be under a license that's not compatible with Apache's licensing guidelines for third-party products.

1. To build the Non-OSS plugins, you'll need to have the requisite JARs installed under the **deps** directory.

   Because these modules require dependencies that can't be distributed with CloudStack you'll need to download them yourself. Links to the most recent dependencies are listed on the *How to build on master branch* page on the wiki.
2. You may also need to download vhd-util, which was removed due to licensing issues. You'll copy vhd-util to the **`scripts/vm/hypervisor/xenserver/`** directory.
3. Once you have all the dependencies copied over, you'll be able to build CloudStack with the **nonoss** option:

   ```
   $ mvn clean
   $ mvn install -Dnonoss
   ```
4. Once you've built CloudStack with the **nonoss** profile, you can package it using the 「Building RPMs from Source」 or 「Building DEB packages」 instructions.

第4章 インストール

4.1. 対象の読者

クラウドの設計フェーズや、精巧な展開計画を経験した人、あるいはトライアルの規模を拡大する準備ができている人。以下の手順では、VLANを使った拡張ネットワーク、高可用性、ロードバランサーやファイアウォールなどの外部機器との連携、Citrix XenServer、KVM、VMware vSphereなどマルチハイパーバイザーのサポートなど、CloudStackのさらに高度な機能を利用できます。

4.2. インストール手順の概要

簡単な試用インストール以上のことを行うには、構成のさまざまな選択肢についてガイダンスが必要になります。次の項目を参照することを強くお勧めします。

- 展開アーキテクチャの選択
- ハイパーバイザーの選択 : サポートされる機能
- ネットワークのセットアップ
- ストレージのセットアップ
- ベストプラクティス

1. 必要なハードウェアの準備ができたかどうかの確認。「最小システム要件」 を参照してください。
2. 管理サーバーのインストール(単一ノードか複数ノードかを選択します)。「管理サーバーのインストール」 を参照してください。
3. ユーザーインターフェイスへのログイン。5章 ユーザーインターフェイス を参照してください。
4. ゾーンの追加。最初のポッド、クラスター、およびホストの設定。「ゾーンの追加」 を参照してください。
5. ポッドの追加(オプション)。「ポッドの追加」 を参照してください。
6. クラスターの追加(オプション)。「クラスタの追加」 を参照してください。
7. ホストの追加(オプション)。「ホストの追加」 を参照してください。
8. プライマリストレージの追加(オプション)。「プライマリストレージの追加」 を参照してください。
9. セカンダリストレージの追加(オプション)。「セカンダリストレージの追加」 を参照してください。
10. クラウドの使用。「初期化とテスト」 を参照してください。

4.3. 最小システム要件

4.3.1. 管理サーバー, データベースとストレージシステムの要件

管理サーバーとMySQLデータベースを動作させるため以下の要件を満たすサーバー。同一サーバー上でローカルディスクやNFSを利用してプライマリストレージ、セカンダリストレージを提供することも可能です。管理サーバーは仮想マシン上で動作させることもできます。

- オペレーティングシステム:
  推奨: CentOS/RHEL 6.3以上、もしくは Ubuntu 12.04(.1)
- 64-bit x86 CPU(多くのコアを用意することでパフォーマンスの向上が見込まれます)
- 4GBのメモリ
- 250GB以上のストレージ(多くの実績から500GB以上を推奨)。
- 最少1つ以上のNIC
- 静的に割り当てられたIPアドレス
- hostnameコマンドで完全修飾ホスト名が返される

4.3.2. ホスト/ハイパーバイザーの要件

ゲストVMを構成するクラウドサービスを動作させるホスト。各ホストは一つの物理筐体であり、次の要件を満たす必要があります。

- ハードウェア仮想マシン(Intel-VTまたはAMD-Vが有効であること)をサポートする必要があります。
- 64-bit x86 CPU(多くのコアを用意することでパフォーマンスの向上が見込まれます)
- 完全仮想化のサポートが必要。
- 4GBのメモリ
- 36 GBのローカルディスク
- 最少1つ以上のNIC
- 

注記

もし、ホストに対し DHCP を利用する場合、DHCP サーバーがこれらホストに配布する IP とCloudStack によって作成された仮想ルーターの DHCP が競合しないことを確認してください。

- 最新のホットフィックスが適用されたハイパーバイザー。
- CloudStack が展開された際、ハイパーバイザーホストに既に動作しているVMが存在していない。
- クラスター内にあるホストは全て同スペックでなければいけません。CPU の種類や数、機能フラグが同じでなければいけません。

ホストはハイパーバイザーに依存した追加要件を満たす必要があります。インストールの章の上部にある要件リストからあなたの選択したハイパーバイザーを確認してください。

警告

加えてハイパーバイザーの要件とガイドに記述されているインストール手順を満たす必要があります。ハイパーバイザーホストは CloudStack と連携する出来るよう適切に準備しなければなります。例として XenServerの要件を以下のCitrix XenServer インストールに記述します。

- 「KVM ホストのシステム要件」
- 「XenServerホストのシステム要件」
- 「vSphere ホストのシステム要件」

4.4. Configure package repository

CloudStack is only distributed from source from the official mirrors. However, members of the CloudStack community may build convenience binaries so that users can install Apache CloudStack without needing to build from source.

If you didn't follow the steps to build your own packages from source in the sections for 「Building RPMs from Source」 or 「Building DEB packages」 you may find pre-built DEB and RPM packages for your convenience linked from the downloads page.

注記

These repositories contain both the Management Server and KVM Hypervisor packages.

4.4.1. DEB package repository

You can add a DEB package repository to your apt sources with the following commands. Please note that only packages for Ubuntu 12.04 LTS (precise) are being built at this time.

Use your preferred editor and open (or create) **/etc/apt/sources.list.d/cloudstack.list**. Add the community provided repository to the file:

```
deb http://cloudstack.apt-get.eu/ubuntu precise 4.1
```

We now have to add the public key to the trusted keys.

```
$ wget -O - http://cloudstack.apt-get.eu/release.asc|apt-key add -
```

Now update your local apt cache.

```
$ apt-get update
```

Your DEB package repository should now be configured and ready for use.

4.4.2. RPM package repository

There is a RPM package repository for CloudStack so you can easily install on RHEL based platforms.

If you're using an RPM-based system, you'll want to add the Yum repository so that you can install CloudStack with Yum.

Yum repository information is found under **/etc/yum.repos.d**. You'll see several **.repo** files in this directory, each one denoting a specific repository.

To add the CloudStack repository, create **/etc/yum.repos.d/cloudstack.repo** and insert the following information.

```
[cloudstack]
name=cloudstack
baseurl=http://cloudstack.apt-get.eu/rhel/4.1/
enabled=1
gpgcheck=0
```

Now you should be able to install CloudStack using Yum.

4.5. 管理サーバーのインストール

4.5.1. 管理サーバーのインストール

ここでは管理サーバーのインストール手順について説明します。インストールには2種類の手順があり、あなたのクラウド環境にいくつの管理サーバーを用意するかによって異なります。

- 単一ホストでの管理サーバーと MySQL。
- 物理的に分けられた複数ホストへの管理サーバーと MySQL。

どちらの場合でもこれらのマシンは「システム要件」に記載されているシステム要件を満たしている必要 があります。

警告

セキュリティのため、パブリックインターネット から管理サーバー上のポート 8096 または 8250 にアクセスできないようにする必要があります。

管理サーバーインストールの手順:

1. オペレーティングシステムの準備
2. (XenServer のみ) vhd-util をダウンロードしてインストールしてください。
3. 最初の管理サーバーのインストール
4. MySQLのインストールと設定
5. NFS共有の準備
6. 追加の管理サーバーの準備と起動(オプション)
7. システム仮想マシンテンプレートの準備

4.5.2. オペレーティングシステムの準備

管理サーバーをホストするために、次の手順に従ってオペレーティングシステムを準備する必要があります。これらの手順は各管理サーバーノードで実行する必要があります。

1. オペレーティングシステムにルートユーザーとしてログオンします。
2. 完全修飾ホスト名を確認します。

   ```
   hostname --fqdn
   ```

   This should return a fully qualified hostname such as "management1.lab.example.org". If it does not, edit /etc/hosts so that it does.
3. 管理サーバーからインターネットに接続できることを確認します。

   ```
   ping www.cloudstack.org
   ```
4. 時刻を同期するために NTP を有効にします。

   注記

クラウドのサーバーのクロックを同期するた めに NTP が必要です。

a. NTPのインストール

```
yum install ntp
```

```
apt-get install openntpd
```

5. これらの手順を管理サーバーがインストールされた全てのホストで実行します。

4.5.3. 初期ホストへの管理サーバーのインストール

最初のインストールでは管理サーバーのインストールを単一か複数ホストに対して行うかに関わらず単一ホストに対してのソフトウェアインストールを行います。

注記

もし高可用性のため管理サーバーを複数ノードにインストール場合ホストの追加は実施せずこの後のステップを完了してから行なってください。

CloudStack 管理サーバーは RPM か DEB パッケージを利用してインストールできます。これらのパッケージは管理サーバーを動かすために必要な全てを含んでいます。

4.5.3.1. CentOS/RHEL でのインストール

まず、必要なパッケージをインストールします。

```
yum install cloudstack-management
```

4.5.3.2. Ubuntu でのインストール

```
apt-get install cloudstack-mangagement
```

4.5.3.3. vhd-util をダウンロードします。

次の手順はハイパーバイザーホストとして XenServer をインストールした場合のみ必要となります。

管理サーバーをセットアップする前に、vhd-util から vhd-util をダウンロードしてください。

If the Management Server is RHEL or CentOS, copy vhd-util to /usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver.

If the Management Server is Ubuntu, copy vhd-util to /usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver.

4.5.4. Install the database server

The CloudStack management server uses a MySQL database server to store its data. When you are installing the management server on a single node, you can install the MySQL server locally. For an installation that has multiple management server nodes, we assume the MySQL database also runs on a separate node.

CloudStack has been tested with MySQL 5.1 and 5.5. These versions are included in RHEL/CentOS and Ubuntu.

4.5.4.1. 管理サーバーノード上でのデータベースインストール

この章では管理サーバーと同一のノードにどのように MySQL をインストールするかを説明しています。これは単一の管理サーバーノードの展開を想定しています。もし、複数ノードへの管理サーバーの展開を実施している場合、一般的には MySQL 用に別ノードを用意します。詳細は「Install the Database on a Separate Node」を参照して下さい。

1. Install MySQL from the package repository of your distribution:

```
yum install mysql-server
```

```
apt-get install mysql-server
```

2. Open the MySQL configuration file. The configuration file is **/etc/my.cnf** or **/etc/mysql/my.cnf**, depending on your OS.
3. Insert the following lines in the [mysqld] section.

   You can put these lines below the datadir line. The max_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes one Management Server.

注記

On Ubuntu, you can also create a file **/etc/mysql/conf.d/cloudstack.cnf** and add these directives there. Don't forget to add [mysqld] on the first line of the file.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

4. 新しい構成情報を反映させるため MySQL を起動、もしくは再起動します。
   RHEL/CentOS の場合 MySQL はインストール後自動で起動されません。手動で起動させて下さい。

```
service mysqld start
```

   Unbuntu の場合 MySQL を再起動します。

```
service mysqld restart
```

5. (CentOS と RHEL のみ。Ubuntu では必要ありません。)

警告

RHEL と CentOS の場合、デフォルトで MySQL にルートパスワードが設定されません。セキュリティ上の予防のためルートパスワードを設定することを強く推奨します。

   インストールを安全に実施するため次のコマンドを実行します。全ての質問には "Y" を答えることができます。

```
mysql_secure_installation
```

6. CloudStack can be blocked by security mechanisms, such as SELinux. Disable SELinux to ensure + that the Agent has all the required permissions.
   Configure SELinux (RHEL and CentOS):
   a. Check whether SELinux is installed on your machine. If not, you can skip this section.
      In RHEL or CentOS, SELinux is installed and enabled by default. You can verify this with:

```
$ rpm -qa | grep selinux
```

   b. Set the SELINUX variable in **`/etc/selinux/config`** to "permissive". This ensures that the permissive setting will be maintained after a system reboot.
      RHELもしくはCentOSの場合:

```
vi /etc/selinux/config
```

      Change the following line

```
SELINUX=enforcing
```

      to this:

```
SELINUX=permissive
```

   c. Set SELinux to permissive starting immediately, without requiring a system reboot.

```
$ setenforce permissive
```

7. データベースをセットアップします。以下のコマンドは "cloud" ユーザーをデータベースに作成します。
   - dbpassword では "cloud" ユーザーに対してのパスワードを設定します。推奨はされませんがパスワード無しも選択可能です。
   - 展開する際は、データベースを展開するユーザー名とパスワードを指定して下さい。以下のコマンドでは root ユーザーがデータベースを展開し、"cloud" ユーザーを作成しています。
   - (オプション) encryption_type にはデータベースのパスワードの暗号化方式として file か web を指定できます。詳細は 「About Password and Key Encryption」 を参照してください。
   - (オプション) management_server_key には CloudStack プロパティファイル上で機密パラメーターを暗号化する際のデフォルト鍵を変更できます。デフォルトでは "password" になりますが、より安全な値に変更することを強く推奨します。詳細は「About Password and Key Encryption」を参照してください。
   - (オプション) database_key には CloudStack データベース上で機密パラメーターを暗号化する際のデフォルト鍵を変更できます。デフォルトでは "password" になりますが、より安全な値に変更することを強く推奨します。詳細は「About Password and Key Encryption」 を参照してください。
   - (Optional) For management_server_ip, you may explicitly specify cluster management server node IP. If not specified, the local IP address will be used.

```
cloudstack-setup-databases cloud:<dbpassword>@localhost \
--deploy-as=root:<password> \
-e <encryption_type> \
-m <management_server_key> \
-k <database_key> \
-i <management_server_ip>
```

   このスクリプトが完了すると「Successfully initialized the database.」のようなメッセージが表示されま す。
8. 管理サーバーと同一のマシンで KVM ハイパーバイザーを動作させている場合は /etc/sudoers を変更し以下の行を追加してください。

```
デフォルト: cloud !requiretty
```

9. これでデータベースがセットアップされました。管理サーバーのオペレーティングシステムの構成は完了です。このコマンドにより iptables と sudoers がセットアップされ、管理サーバーが起動します。

```
 #  cloudstack-setup-management
```

   "CloudStack 管理サーバーのセットアップが完了しました。" といったメッセージを確認できます。

4.5.4.2. Install the Database on a Separate Node

This section describes how to install MySQL on a standalone machine, separate from the Management Server. This

technique is intended for a deployment that includes several Management Server nodes. If you have a single-node Management Server deployment, you will typically use the same node for MySQL. See 「管理サーバーノード上でのデータベースインストール」.

注記

The management server doesn't require a specific distribution for the MySQL node. You can use a distribution or Operating System of your choice. Using the same distribution as the management server is recommended, but not required. See 「管理サーバー, データベースとストレージシステムの要件」.

1. ディストリビューションのパッケージリポジトリから MySQL をインストールします。

```
yum install mysql-server
```

```
apt-get install mysql-server
```

2. Edit the MySQL configuration (/etc/my.cnf or /etc/mysql/my.cnf, depending on your OS) and insert the following lines in the [mysqld] section. You can put these lines below the datadir line. The max_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes two Management Servers.

注記

On Ubuntu, you can also create /etc/mysql/conf.d/cloudstack.cnf file and add these directives there. Don't forget to add [mysqld] on the first line of the file.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=700
log-bin=mysql-bin
binlog-format = 'ROW'
bind-address = 0.0.0.0
```

3. 新しい構成情報を反映させるため MySQL を起動、もしくは再起動します。
RHEL/CentOS の場合 MySQL はインストール後自動で起動されません。手動で起動させて下さい。

```
service mysqld start
```

Unbuntu の場合 MySQL を再起動します。

```
service mysqld restart
```

4. (CentOS と RHEL のみ。Ubuntu では必要ありません。)

警告

RHEL と CentOS の場合、デフォルトで MySQL にルートパスワードが設定されません。セキュリティ上の予防のためルートパスワードを設定することを強く推奨します。

Run the following command to secure your installation. You can answer "Y" to all questions except "Disallow root login remotely?". Remote root login is required to set up the databases.

```
mysql_secure_installation
```

5. If a firewall is present on the system, open TCP port 3306 so external MySQL connections can be established.
On Ubuntu, UFW is the default firewall. Open the port with this command:

```
ufw allow mysql
```

On RHEL/CentOS:

   a. Edit the /etc/sysconfig/iptables file and add the following line at the beginning of the INPUT chain.

```
-A INPUT -p tcp --dport 3306 -j ACCEPT
```

   b. Now reload the iptables rules.

```
service iptables restart
```

6. Return to the root shell on your first Management Server.
7. Set up the database. The following command creates the cloud user on the database.
   - In dbpassword, specify the password to be assigned to the cloud user. You can choose to provide no password.
   - In deploy-as, specify the username and password of the user deploying the database. In the following command, it is assumed the root user is deploying the database and creating the cloud user.
   - (オプション) encryption_type にはデータベースのパスワードの暗号化方式として file か web を指定できます。詳細は 「About Password and Key Encryption」 を参照してください。
   - (Optional) For management_server_key, substitute the default key that is used to encrypt confidential parameters in the CloudStack properties file. Default: password. It is highly recommended that you replace this with a more secure value. See About Password and Key Encryption.
   - (オプション) database_key には CloudStack データベース上で機密パラメーターを暗号化する際のデフォルト鍵を変更できます。デフォルトでは "password" になりますが、より安全な値に変更することを強く推奨しま

す。詳細は「About Password and Key Encryption」 を参照してください。

- (Optional) For management_server_ip, you may explicitly specify cluster management server node IP. If not specified, the local IP address will be used.

```
cloudstack-setup-databases cloud:<dbpassword>@<ip address mysql server> \
--deploy-as=root:<password> \
-e <encryption_type> \
-m <management_server_key> \
-k <database_key> \
-i <management_server_ip>
```

このスクリプトが完了すると「Successfully initialized the database.」のようなメッセージが表示されま す。

4.5.5. About Password and Key Encryption

CloudStack stores several sensitive passwords and secret keys that are used to provide security. These values are always automatically encrypted:

- Database secret key
- Database password
- SSH keys
- Compute node root password
- VPN password
- User API secret key
- VNC password

CloudStack uses the Java Simplified Encryption (JASYPT) library. The data values are encrypted and decrypted using a database secret key, which is stored in one of CloudStack's internal properties files along with the database password. The other encrypted values listed above, such as SSH keys, are in the CloudStack internal database.

Of course, the database secret key itself can not be stored in the open – it must be encrypted. How then does CloudStack read it? A second secret key must be provided from an external source during Management Server startup. This key can be provided in one of two ways: loaded from a file or provided by the CloudStack administrator. The CloudStack database has a new configuration setting that lets it know which of these methods will be used. If the encryption type is set to "file," the key must be in a file in a known location. If the encryption type is set to "web," the administrator runs the utility com.cloud.utils.crypt.EncryptionSecretKeySender, which relays the key to the Management Server over a known port.

The encryption type, database secret key, and Management Server secret key are set during CloudStack installation. They are all parameters to the CloudStack database setup script (cloudstack-setup-databases). The default values are file, password, and password. It is, of course, highly recommended that you change these to more secure keys.

4.5.6. NFS共有の準備

CloudStack には、プライマリストレージとセカンダリストレージを保持するための場所が必要です(「クラウドインフラストラクチャの概要」を参照)。双方には NFS 共有を用いることができ、これらのストレージは両方とも NFS 共有にできます。ここでは、ストレージを CloudStack に追加する前に NFS 共有をセットアップする方法について説明します。

代替ストレージ

NFS だけがプライマリストレージ、セカンダリストレージのオプションではありません。たとえば、Ceph RBD や GlusterFS、iSCSI なども利用できます。どのストレージシステムを利用するかはどのハイパーバイザーを選択したかやプライマリストレージ、セカンダリストレージのどちらに言及しているかに依存します。

プライマリストレージとセカンダリストレージの要件は以下の通り:

- 「プライマリストレージについて」
- 「セカンダリストレージについて」

商用環境でのインストールでは一般的にNFSサーバーを別に用意します。参照 「Using a Separate NFS Server」

また、管理サーバーと同じノードにセットアップすることもできます。これはより一般的なトライアルインストールとなりますが大規模環境の展開も技術的には可能です。参照 「Using the Management Server as the NFS Server」

4.5.6.1. Using a Separate NFS Server

This section tells how to set up NFS shares for secondary and (optionally) primary storage on an NFS server running on a separate node from the Management Server.

The exact commands for the following steps may vary depending on your operating system version.

警告

(KVM only) Ensure that no volume is already mounted at your NFS mount point.

1. On the storage server, create an NFS share for secondary storage and, if you are using NFS for primary storage as well, create a second NFS share. For example:

```
# mkdir -p /export/primary
# mkdir -p /export/secondary
```

2. To configure the new directories as NFS exports, edit /etc/exports. Export the NFS share(s) with rw,async,no_root_squash. For example:

```
# vi /etc/exports
```

Insert the following line.

```
/export  *(rw,async,no_root_squash)
```

3. Export the /export directory.

```
# exportfs -a
```

4. On the management server, create a mount point for secondary storage. For example:

```
# mkdir -p /mnt/secondary
```

5. Mount the secondary storage on your Management Server. Replace the example NFS server name and NFS share paths below with your own.

```
# mount -t nfs nfsservername:/nfs/share/secondary /mnt/secondary
```

4.5.6.2. Using the Management Server as the NFS Server

This section tells how to set up NFS shares for primary and secondary storage on the same node with the Management Server. This is more typical of a trial installation, but is technically possible in a larger deployment. It is assumed that you will have less than 16TB of storage on the host.

The exact commands for the following steps may vary depending on your operating system version.

1. On RHEL/CentOS systems, you'll need to install the nfs-utils package:

```
$ sudo yum install nfs-utils
```

2. On the Management Server host, create two directories that you will use for primary and secondary storage. For example:

```
# mkdir -p /export/primary
# mkdir -p /export/secondary
```

3. To configure the new directories as NFS exports, edit /etc/exports. Export the NFS share(s) with rw,async,no_root_squash. For example:

```
# vi /etc/exports
```

Insert the following line.

```
/export  *(rw,async,no_root_squash)
```

4. Export the /export directory.

```
# exportfs -a
```

5. Edit the /etc/sysconfig/nfs file.

```
# vi /etc/sysconfig/nfs
```

Uncomment the following lines:

```
LOCKD_TCPPORT=32803
LOCKD_UDPPORT=32769
MOUNTD_PORT=892
RQUOTAD_PORT=875
STATD_PORT=662
STATD_OUTGOING_PORT=2020
```

6. Edit the /etc/sysconfig/iptables file.

```
# vi /etc/sysconfig/iptables
```

Add the following lines at the beginning of the INPUT chain where <NETWORK> is the network that you'll be using:

```
-A INPUT -s <NETWORK> -m state --state NEW -p udp --dport 111 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 111 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 2049 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 32803 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p udp --dport 32769 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 892 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p udp --dport 892 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 875 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p udp --dport 875 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p tcp --dport 662 -j ACCEPT
-A INPUT -s <NETWORK> -m state --state NEW -p udp --dport 662 -j ACCEPT
```

7. Run the following commands:

```
# service iptables restart
# service iptables save
```

8. If NFS v4 communication is used between client and server, add your domain to /etc/idmapd.conf on both the hypervisor host and Management Server.

```
# vi /etc/idmapd.conf
```

Remove the character # from the beginning of the Domain line in idmapd.conf and replace the value in the file with your own domain. In the example below, the domain is company.com

your own domain. In the example below, the domain is company.com.

```
Domain = company.com
```

9. Reboot the Management Server host.
   Two NFS shares called /export/primary and /export/secondary are now set up.
10. It is recommended that you test to be sure the previous steps have been successful.
    a. Log in to the hypervisor host.
    b. Be sure NFS and rpcbind are running. The commands might be different depending on your OS. For example:

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
# reboot
```

    c. Log back in to the hypervisor host and try to mount the /export directories. For example (substitute your own management server name):

```
# mkdir /primarymount
# mount -t nfs <management-server-name>:/export/primary /primarymount
# umount /primarymount
# mkdir /secondarymount
# mount -t nfs <management-server-name>:/export/secondary /secondarymount
# umount /secondarymount
```

4.5.7. 追加の管理サーバーの準備と起動

2 台目以降の管理サーバーについて、管理サーバーのソフトウェアをインストールしてデータベースに接続し、管理サーバーのオペレーティングシステムをセットアップします。

1. 「オペレーティングシステムの準備」 と 「Building RPMs from Source」 もしくは 「Building DEB packages」 の手順を必要に応じて実施します。
2. ハイパーバイザーホストとして XenServer をインストールしている場合は次の手順が必要となります。
   vhd-util から vhd-utl をダウンロードします。
   Copy vhd-util to /usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver.
3. 必要なサービスが起動中であり起動時に開始するよう設定されていることを確認します。

```
# service rpcbind start
# service nfs start
# chkconfig nfs on
# chkconfig rpcbind on
```

4. データベースクライアントを構成します。このケースでは --deploy-as オプションが付与されていないことに注意してください。(このコマンドの引数に関する詳細は 「Install the Database on a Separate Node」 を参照してください)。

```
# cloudstack-setup-databases cloud:dbpassword@dbhost -e encryption_type -m
management_server_key -k database_key -i management_server_ip
```

5. オペレーティングシステムを構成し、管理サーバーを起動します。

```
# cloudstack-setup-management
```

   このノード上の管理サーバーが起動します。
6. これらの手順をそれぞれの追加する管理サーバー上で実行します。
7. Be sure to configure a load balancer for the Management Servers. See 「Management Server Load Balancing」.

4.5.8. システム仮想マシンテンプレートの準備

CloudStack システム仮想マシンに使用するテンプレートをセカンダリス トレージに配置する必要があります。

注記

コマンドをコピーして実行するときは、単一の行として貼り付けたことを確認してください。 一部のドキュメントビューアーでは、コピーしたテキストに不要な改行が含まれる可能性があります。

1. 管理サーバーで次の cloud-install-sys-tmplt コマンドを実 行して、システム仮想マシンテンプレートを取得して展開します。 このゾーンでエンドユーザーが実行することが予想される各ハイパーバイザーの種類に対応するコマンドを実行します。
   セカンダリストレージのマウントポイントが/mnt/secondary でない場合は、実際のマウントポイント名に置き換えます。
   もし CloudStack データベースの暗号化タイプを "web" に設定した場合、次のパラメーターを追加する必要があります。" -s <management-server-secret-key>. 詳細は 「About Password and Key Encryption」 を参照してください。
   この処理を実行するにはローカルファイルシステムに約 5 GB の空き領域が必要で、実行するたびに最長で 30 分かかります。
   - XenServer:

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -
m /mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.vhd.bz2 -h xenserver -s <optional-management-server-secret-key> -F
```

- vSphere:

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -
m /mnt/secondary -u http://download.cloud.com/templates/burbank/burbank-systemvm-
08012012.ova -h vmware -s <optional-management-server-secret-key>  -F
```

- KVM:

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -
m /mnt/secondary -u http://download.cloud.com/templates/acton/acton-systemvm-
02062012.qcow2.bz2 -h kvm -s <optional-management-server-secret-key> -F
```

Ubuntu の場合は代わりに以下のパスを利用してください。

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt
```

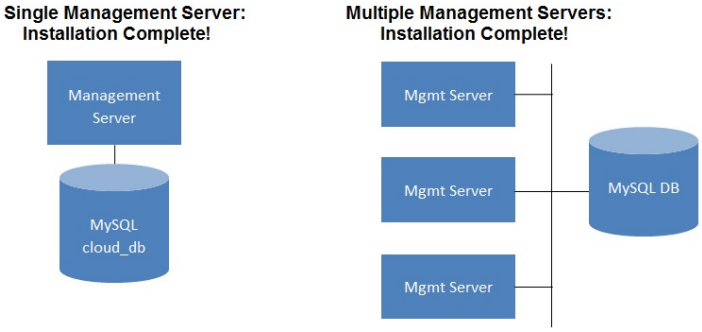
2. もし別途 NFS サーバーを利用している場合は以下の手順を実施してください。もし管理サーバー上で NFS サーバーを利用する場合は以下の手順は不要です。
   スクリプトの完了後セカンダリストレージをアンマウントし作成したディレクトリを削除します。

```
# umount /mnt/secondary
# rmdir /mnt/secondary
```

3. これらの手順を各セカンダリストレージサーバーに対して行います。

4.5.9. インストールが完了したら次の手順に進みます。

これで、CloudStack 管理サーバーとシステムデータの保持に使用するデータベースがインストールされました。



次の作業

- クラウドインフラストラクチャを追加しなくても、ユーザーインターフェイスを実行してその内容を把握し、管理段階での CloudStack の操作方法の感触をつかむことができます。「ユーザーインターフェイスへのログオン」を参照してください。
- 準備ができたら、CloudStack でインフラストラクチャを管理するしくみを確認するために、クラウドインフラストラクチャを追加し、このインフラストラクチャでいくつかの仮想マシンを実行します。「クラウドインフラストラクチャのプロビジョニング」を参照してください。

第5章 ユーザーインターフェイス

5.1. UIへのログイン

CloudStack はWebベースのUIを管理者とエンドユーザーの両方に提供しています。ログインに使用したユーザーの権限に応じて適切なUIが表示されます。UIはIE7、IE8、IE9、Firefox 3.5以降、Firefox 4、Safari 4 そしてSafari 5に対応しています。URLは(あなたの環境の管理サーバーのIPアドレスに置き換えてください)

```
http://<management-server-ip-address>:8080/client
```

未設定の管理サーバーにアクセスすると、ガイドツアーのスプラッシュスクリーンが表示されます。以降のアクセス時には、ダッシュボードにアクセスするために下記の情報を入力するログイン画面が表示されます。

ユーザー名

あなたのアカウントのユーザーID。デフォルトのユーザー名はadminです。

パスワード

ユーザーIDに関連付けられたパスワード。デフォルトユーザーのパスワードはpasswordです。

ドメイン

もしもあなたがrootドメインのユーザーならば、フィールドは空白のままにします。

もしもあなたがサブドメインのユーザーならば、rootドメインを除いた、そのドメインへのフルパスを入力します。

例えばrootドメインの下にComp1/hrといった複数階層があると仮定します。Comp1ドメインのユーザーはドメインフィールドにComp1と入力し、Comp1/salesドメインのユーザーはComp1/salesと入力します。

より詳細なUIへのログインのガイドラインに関しては「ルート管理者としてのログイン」を参照してください。

5.1.1. エンドユーザーインターフェイス

CloudStack ユーザーインターフェイスはユーザーのクラウドインフラストラクチャにおいて閲覧や仮想マシン、テンプレートと ISO、データボリュームとスナップショット、ゲストネットワーク、IP アドレスなどのクラウドリソースの利用を手助けします。もしユーザーが1つ以上の CloudStack プロジェクトのメンバーもしくは管理者である場合、ユーザーインターフェイスはプロジェクト向けのビューを提供します。

5.1.2. Root 管理者 UI の概要

CloudStack UI は CloudStack 管理者のプロビジョニングや確認、クラウドインフラストラクチャやドメイン、ユーザーアカウント、プロジェクト、構成設定の管理を手助けします。初回の管理サーバーのインストール時、クラウドインフラストラクチャのプロビジョニングのため、次のガイドツアーを利用できます。ログイン後、ユーザー毎のダッシュボードが表示され、様々なリンクや、様々な管理者機能へのナビゲーションバーが左側に表示されます。Root 管理者はエンドユーザーに提供されている UI のように全てのタスクを UI から利用することができます。

5.1.3. ルート管理者としてのログイン

管理サーバーをインストールして起動後、CloudStack のユーザーインターフェイスを起動させることができます。このユーザーインターフェイスはプロビジョニングやビュー、クラウドインフラストラクチャの管理を手助けします。

1. お好みのウェブブラウザーを開き URL を入力します。代わりに管理サーバーの IP アドレスを入力することもできます。

   ```
   http://<management-server-ip-address>:8080/client
   ```

   新しくインストールされた管理サーバーにログインするとガイドツアーのスプラッシュ画面が表示されます。後にアクセスした場合は直接ダッシュボード画面が表示されます。
2. 初回スプラッシュ画面が表示され、次の項目が選択できます。
   - **Continue with basic setup :** CloudStack を試したく、すぐ使い始められるようガイド付きの設定を行いたいたい合はこちらを選択します。次のような機能を持つクラウド環境のセットアップをお手伝いします。1台のマシン上で CloudStack ソフトウェアと NFS によって提供されるストレージが動作する。1台のマシン上で XenServer や KVM ハイパーバイザー配下に仮想マシンが動作する。そしてパブリックネットワークを共有する。

     ツアーガイドで表示される情報は全て必要な情報になります。しかしより詳細を知りたい場合は次の「トライアルインストールガイド」を参照することもできます。
   - **I have used CloudStack before** 既に高度な展開を設計、計画したことがある、もしくは基本セットアップでセットアップしたトライアルクラウドをよりスケールアップさせたい場合はこちらを選びます。管理者インターフェイスからはより高度な VLAN ネットワーク、高可用性、負荷分散装置やファイアウォールなどの追加のネットワーク要素、Citrix XenServer, KVM, VMware vSphere を含む様々なハイパーバイザーのサポートといった機能を利用することができます。

     ルート管理者のダッシュボードが表示されます。
3. 新しいルート管理者のパスワードを設定するべきです。もし基本セットアップを選択した場合、新しいパスワードの入力画面が表示されます。もし経験済みユーザーを選択した場合は 「ルートパスワードの変更」 の手順を参照してください。

警告

ルート管理者としてログインした場合、物理インフラストラクチャを含むCloudStack の展開を管理します。ルート管理者は一般的な機能を変更するための設定変更や、ユーザーアカウントの作成と削除、その他多くの権限を持つ行動を振る舞うことができます。そのためデフォルトのパスワードは新しく一意なパスワードに変更してください。

5.1.4. ルートパスワードの変更

CloudStack のインストール中は、ルート管理者としてログオンしています。このアカウントを使用して、物理インフラストラクチャを含めて CloudStack 環境を管理します。ルート管理者は、構成設定を変更して基本機能を変更したり、ユーザーアカウントを作成または削除したり、権限を持つ人物のみが実行する必要のある多くの措置を取ることができます。初回の CloudStack インストールの際はデフォルトのパスワードである password を新しい固有の値に変更してください。

1. お好みのウェブブラウザーを開き URL を入力します。代わりに管理サーバーの IP アドレスを入力することもできます。

```
http://<management-server-ip-address>:8080/client
```

2. 現在のルートユーザーの ID とパスワードで CloudStack ユーザーインターフェイスにログオンします。デフォルトは admin および password です。
3. [Accounts]をクリックします。
4. 管理者のアカウント名をクリックします。
5. [View Users]をクリックします。
6. 管理者のユーザー名をクリックします。
7. [Change Password]アイコンをクリックします。 
8. 新しいパスワードを入力して[OK]をクリックします。

5.2. Using SSH Keys for Authentication

In addition to the username and password authentication, CloudStack supports using SSH keys to log in to the cloud infrastructure for additional security. You can use the createSSHKeyPair API to generate the SSH keys.

Because each cloud user has their own SSH key, one cloud user cannot log in to another cloud user's instances unless they share their SSH key files. Using a single SSH key pair, you can manage multiple instances.

5.2.1. Creating an Instance Template that Supports SSH Keys

Create a instance template that supports SSH Keys.

1. Create a new instance by using the template provided by cloudstack.
   For more information on creating a new instance, see
2. Download the cloudstack script from The SSH Key Gen Scriptto the instance you have created.

```
wget
http://downloads.sourceforge.net/project/cloudstack/SSH%20Key%20Gen%20Script/cloud-
set-guest-sshkey.in?
r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fcloudstack%2Ffiles%2FSSH%2520Key%2520Gen%
2520Script%2F&ts=1331225219&use_mirror=iweb
```

3. Copy the file to /etc/init.d.

```
cp cloud-set-guest-sshkey.in /etc/init.d/
```

4. Give the necessary permissions on the script:

```
chmod +x /etc/init.d/cloud-set-guest-sshkey.in
```

5. Run the script while starting up the operating system:

```
chkconfig --add cloud-set-guest-sshkey.in
```

6. Stop the instance.

5.2.2. Creating the SSH Keypair

You must make a call to the createSSHKeyPair api method. You can either use the CloudStack Python API library or the curl commands to make the call to the cloudstack api.

For example, make a call from the cloudstack server to create a SSH keypair called "keypair-doc" for the admin account in the root domain:

注記

Ensure that you adjust these values to meet your needs. If you are making the API call from a different server, your URL/PORT will be different, and you will need to use the API keys.

1. Run the following curl command:

```
curl --globoff "http://localhost:8096/?command=createSSHKeyPair&name=keypair-
doc&account=admin&domainid=5163440e-c44b-42b5-9109-ad75cae8e8a2"
```

   The output is something similar to what is given below:

```
<?xml version="1.0" encoding="ISO-8859-1"?><createsshkeypairresponse cloud-stack-
version="3.0.0.20120228045507"><keypair><name>keypair-doc</name>
<fingerprint>f6:77:39:d5:5e:77:02:22:6a:d8:7f:ce:ab:cd:b3:56</fingerprint>
<privatekey>-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCSydmnQ67jP6lNoXdX3noZjQdrMAWNQZ7y5SrEu4wDxplvhYci
dXYBeZVwakDVsU2MLGl/K+wefwefwefwefwefJyKJaogMKn7BperPD6n1wIDAQAB
AoGAdXaJ7uyZKeRDoy6wA0UmF0kSPbMZCR+UTIHNkS/E0/4U+6lhMokmFSHtu
mfDZ1kGGDYhMsdytjDBztljawfawfeawefawfawfawQQDCjEsoRdgkduTy
QpbSGDIa11Jsc+XNDx2fgRinDsxXI/zJYXTKRhSl/LIPHBw/brW8vzxhOlSOrwm7
VvemkkgpAkEAwSeEw394LYZiEVv395ar9MLRVTVLwpo54jC4tsOxQCBlloocK
lYaocpk0yBqqOUSBawfIiDCuLXSdvBo1Xz5ICTM19vgvEp/+kMuECQBzm
nVo8b2Gvyagqt/KEQo8wzH2THghZ1qQ1QRhIeJG2aissEacF6bGB2oZ7Igim5L14
4KR7OeETOyCLC2k+02UCQQCrniSnWKtDVoVqeK/zbB32JhW3Wullv5p5zUEcd
KfEEuzcCUIxtJYTahJ1pvlFkQ8anpuxjSEDp8x/18bq3
-----END RSA PRIVATE KEY-----
</privatekey></keypair></createsshkeypairresponse>
```

2. Copy the key data into a file. The file looks like this:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXQIBAAKBgQCSydmnQ67jP6lNoXdX3noZjQdrMAWNQZ7y5SrEu4wDxplvhYci
dXYBeZVwakDVsU2MLGl/K+wefwefwefwefwefJyKJaogMKn7BperPD6n1wIDAQAB
AoGAdXaJ7uyZKeRDoy6wA0UmF0kSPbMZCR+UTIHNkS/E0/4U+6lhMokmFSHtu
mfDZ1kGGDYhMsdytjDBztljawfawfeawefawfawfawQQDCjEsoRdgkduTy
QpbSGDIa11Jsc+XNDx2fgRinDsxXI/zJYXTKRhSl/LIPHBw/brW8vzxhOlSOrwm7
VvemkkgpAkEAwSeEw394LYZiEVv395ar9MLRVTVLwpo54jC4tsOxQCBlloocK
lYaocpk0yBqqOUSBawfIiDCuLXSdvBo1Xz5ICTM19vgvEp/+kMuECQBzm
nVo8b2Gvyagqt/KEQo8wzH2THghZ1qQ1QRhIeJG2aissEacF6bGB2oZ7Igim5L14
4KR7OeEToyCLC2k+02UCQQCrniSnWKtDVoVqeK/zbB32JhW3Wullv5p5zUEcd
KfEEuzcCUIxtJYTahJ1pvlFkQ8anpuxjSEDp8x/18bq3
-----END RSA PRIVATE KEY-----
```

3. Save the file.

5.2.3. Creating an Instance

After you save the SSH keypair file, you must create an instance by using the template that you created at 「Creating an Instance Template that Supports SSH Keys」. Ensure that you use the same SSH key name that you created at 「Creating the SSH Keypair」.

注記

You cannot create the instance by using the GUI at this time and associate the instance with the newly created SSH keypair.

A sample curl command to create a new instance is:

```
curl --globoff http://localhost:<port number>/?
command=deployVirtualMachine\&zoneId=1\&serviceOfferingId=18727021-7556-4110-9322-
d625b52e0813\&templateId=e899c18a-ce13-4bbf-98a9-625c5026e0b5\&securitygroupids=ff03f02f-
9e3b-48f8-834d-91b822da40c5\&account=admin\&domainid=1\&keypair=keypair-doc
```

Substitute the template, service offering and security group IDs (if you are using the security group feature) that are in your cloud environment.

5.2.4. Logging In Using the SSH Keypair

To test your SSH key generation is successful, check whether you can log in to the cloud setup.

For exaple, from a Linux OS, run:

```
ssh -i ~/.ssh/keypair-doc <ip address>
```

The -i parameter tells the ssh client to use a ssh key found at ~/.ssh/keypair-doc.

5.2.5. Resetting SSH Keys

With the API command resetSSHKeyForVirtualMachine, a user can set or reset the SSH keypair assigned to a virtual machine. A lost or compromised SSH keypair can be changed, and the user can access the VM by using the new keypair. Just create or register a new keypair, then call resetSSHKeyForVirtualMachine.

第6章 Steps to Provisioning Your Cloud Infrastructure

This section tells how to add regions, zones, pods, clusters, hosts, storage, and networks to your cloud. If you are unfamiliar with these entities, please begin by looking through *2章 クラウドインフラストラクチャのプロビジョニング*.

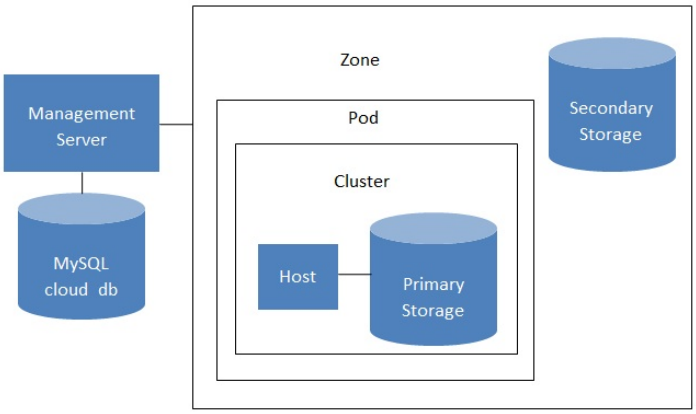
6.1. プロビジョニングの概要

管理サーバーのインストールや稼働後、新しいコンピューティングリソースを管理のために追加することができます。CloudStack クラウドインストラクチャがどのように組織化されるかに関しては 「クラウドインフラストラクチャの概要」 を参照してください。

クラウドインフラストラクチャを展開する、必要な時にスケールアップするには以下の手順に従ってください。

1. Define regions (optional). See 「Adding Regions (optional)」.
2. Add a zone to the region. See 「ゾーンの追加」.
3. Add more pods to the zone (optional). See 「ポッドの追加」.
4. Add more clusters to the pod (optional). See 「クラスタの追加」.
5. Add more hosts to the cluster (optional). See 「ホストの追加」.
6. Add primary storage to the cluster. See 「プライマリストレージの追加」.
7. Add secondary storage to the zone. See 「セカンダリストレージの追加」.
8. 新規クラウドの作成、テストに関しては 「初期化とテスト」 を参照してください。

これらの手順が完了したら、以下の一般的な構成を参考に展開することができます。



Conceptual view of a basic deployment

6.2. Adding Regions (optional)

Grouping your cloud resources into geographic regions is an optional step when provisioning the cloud. For an overview of regions, see 「About Regions」.

6.2.1. The First Region: The Default Region

If you do not take action to define regions, then all the zones in your cloud will be automatically grouped into a single default region. This region is assigned the region ID of 1.

You can change the name or URL of the default region by using the API command updateRegion. For example:

```
http://<IP_of_Management_Server>:8080/client/api?
command=updateRegion&id=1&name=Northern&endpoint=http://<region_1_IP_address_here>:8080/cli
ent&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP0O1h
U%3D
```

6.2.2. Adding a Region

Use these steps to add a second region in addition to the default region.

1. Each region has its own CloudStack instance. Therefore, the first step of creating a new region is to install the

1. Each region has its own CloudStack installation. Therefore, the first step of creating a new region is to install the Management Server software, on one or more nodes, in the geographic area where you want to set up the new region. Use the steps in the Installation guide. When you come to the step where you set up the database, use the additional command-line flag **`-r <region_id>`** to set a region ID for the new region. The default region is automatically assigned a region ID of 1, so your first additional region might be region 2.

```
cloudstack-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password> -
e <encryption_type> -m <management_server_key> -k <database_key> -r <region_id>
```

2. By the end of the installation procedure, the Management Server should have been started. Be sure that the Management Server installation was successful and complete.
3. Add region 2 to region 1. Use the API command addRegion. (For information about how to make an API call, see the Developer's Guide.)

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=addRegion&id=2&name=Western&endpoint=http://<region_2_IP_address_here>:8080/c
lient&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D
```

4. Now perform the same command in reverse, adding region 1 to region 2.

```
http://<IP_of_region_2_Management_Server>:8080/client/api?
command=addRegion&id=1&name=Northern&endpoint=http://<region_1_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D
```

5. Copy the account, user, and domain tables from the region 1 database to the region 2 database.

   In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

   a. First, run this command to copy the contents of the database:

   ```
   # mysqldump -u root -p<mysql_password> -h <region1_db_host> cloud account user
   domain > region1.sql
   ```

   b. Then run this command to put the data onto the region 2 database:

   ```
   # mysql -u root -p<mysql_password> -h <region2_db_host> cloud < region1.sql
   ```

6. Remove project accounts. Run these commands on the region 2 database:

```
mysql> delete from account where type = 5;
```

7. Set the default zone as null:

```
mysql> update account set default_zone_id = null;
```

8. Restart the Management Servers in region 2.

6.2.3. Adding Third and Subsequent Regions

To add the third region, and subsequent additional regions, the steps are similar to those for adding the second region. However, you must repeat certain steps additional times for each additional region:

1. Install CloudStack in each additional region. Set the region ID for each region during the database setup step.

```
cloudstack-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password> -
e <encryption_type> -m <management_server_key> -k <database_key> -r <region_id>
```

2. Once the Management Server is running, add your new region to all existing regions by repeatedly calling the API command addRegion. For example, if you were adding region 3:

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=addRegion&id=3&name=Eastern&endpoint=http://<region_3_IP_address_here>:8080/c
lient&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D

http://<IP_of_region_2_Management_Server>:8080/client/api?
command=addRegion&id=3&name=Eastern&endpoint=http://<region_3_IP_address_here>:8080/c
lient&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D
```

3. Repeat the procedure in reverse to add all existing regions to the new region. For example, for the third region, add the other two existing regions:

```
http://<IP_of_region_3_Management_Server>:8080/client/api?
command=addRegion&id=1&name=Northern&endpoint=http://<region_1_IP_address_here>:8080/
client&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D

http://<IP_of_region_3_Management_Server>:8080/client/api?
command=addRegion&id=2&name=Western&endpoint=http://<region_2_IP_address_here>:8080/c
lient&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8R
AP0O1hU%3D
```

4. Copy the account, user, and domain tables from any existing region's database to the new region's database.

   In the following commands, it is assumed that you have set the root password on the database, which is a CloudStack recommended best practice. Substitute your own MySQL root password.

a. First, run this command to copy the contents of the database:

```
# mysqldump -u root -p<mysql_password> -h <region1_db_host> cloud account user
domain > region1.sql
```

b. Then run this command to put the data onto the new region's database. For example, for region 3:

```
# mysql -u root -p<mysql_password> -h <region3_db_host> cloud < region1.sql
```

5. Remove project accounts. Run these commands on the region 2 database:

```
mysql> delete from account where type = 5;
```

6. Set the default zone as null:

```
mysql> update account set default_zone_id = null;
```

7. Restart the Management Servers in the new region.

6.2.4. Deleting a Region

To delete a region, use the API command removeRegion. Repeat the call to remove the region from all other regions. For example, to remove the 3rd region in a three-region cloud:

```
http://<IP_of_region_1_Management_Server>:8080/client/api?
command=removeRegion&id=3&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP0O1h
U%3D

http://<IP_of_region_2_Management_Server>:8080/client/api?
command=removeRegion&id=3&apiKey=miVr6X7u6bN_sdahOBpjNejPgEsT35eXq-
jB8CG20YI3yaxXcgpyuaIRmFI_EJTVwZ0nUkkJbPmY3y2bciKwFQ&signature=Lxx1DM40AjcXU%2FcaiK8RAP0O1h
U%3D
```

6.3. ゾーンの追加

次の手順は、CloudStack ユーザーインターフェイスにログオン済みであることを前提としています(「UIへのログイン」を参照)。

1. (オプション)クラウド全体のセカンダリストレージとして Swift を使用する場合は、ゾーンを追加する前に Swift を追加する必要があります。
   a. CloudStackユーザーインターフェイスに管理者としてログオンします。
   b. 初めてユーザーインターフェイスを使用する場合は、ガイドツアーのスプラッシュページが開きます。\n[Experienced user]を選択します。ダッシュボードが開きます。
   c. 左側のナビゲーションバーで[Global Settings]をクリックします。
   d. 検索ボックスに「swift.enable」と入力して検索ボタンをクリックします。
   e. [Edit]アイコンをクリックして swift.enable を true に設定します。 
   f. 管理サーバーを再起動します。

   ```
   # service cloudstack-management restart
   ```

   g. CloudStack ユーザーインターフェイスが表示されている Web ブラウザータブを更新して再度ログオンします。
2. 左側のナビゲーションバーで[Infrastructure]をクリックします。
3. [Zones]で[View More]をクリックします。
4. (オプション)Swift ストレージを使用する場合は、[Edit Swift]をクリックします。次の情報を指定します。
   - **URL :** Swift URL です。
   - **Account :** Swift アカウントです。
   - **Username :** Swift アカウントのユーザー名です。
   - **Key :** Swift キーです。
5. [Add Zone]をクリックします。ゾーンの作成ウィザードが開きます。
6. 次のどちらかのネットワークの種類を選択します。
   - **Basic :** AWS スタイルのネットワークシステムに対応します。単一のネットワークを提供します。このネットワークにより、各仮想マシンインスタンスに直接 IP アドレスが割り当てられます。セキュリティグループ(発信元 IP アド レスのフィルター)のようなレイヤー3 レベルの方法でゲストを分離できます。
   - **Advanced :** より高度なネットワークトポロジに対応します。このネットワークモデルでは、最も柔軟に、ゲストネットワークを定義し、ファイアウォール、VPN、負荷分散装置のサポートなどのカスタムネットワークオファリングを 提供できます。

   ネットワークの種類について詳しくは、「物理ネットワークについて」を参照してください。
7. 以降の手順は、[Basic]または[Advanced]のどちらを選択したかによって異なります。該当する手順を続行してください。
   - 「基本ゾーンの構成」
   - 「拡張ゾーンの構成」

6.3.1. 基本ゾーンの構成

1. ゾーンの追加ウィザードで［Basic］を選択して［Next］をクリックすると、次の項目の入力を求められます。入力後、［Next］をクリックします。
   - **Name:** ゾーンの名前です。
   - **DNS1 および DNS2:** ゾーン内のゲスト仮想マシンで使用する DNS サーバーです。これらの DNS サーバーには

- **DNS1およびDNS2:** ゾーン内のゲスト仮想マシンで使用するDNSサーバーです。これらのDNSサーバーには、後で追加するパブリックネットワーク経由でアクセスします。ゾーンのパブリックIPアドレスから、ここで指定するDNSサーバーに通信できる必要があります。
- **Internal DNS1およびInternal DNS2：** これらのDNSサーバーは、ゾーン内のシステム仮想マシン(仮想ルーター、コンソールプロキシ、およびセカンダリストレージ仮想マシンなど、CloudStackにより使用される仮想マシン)によって使用されます。これらのDNSサーバーは、システム仮想マシンの管理トラフィックネットワークインターフェイスを介してアクセスされます。ポッドのプライベートIPアドレスから、ここで指定する内部DNSサーバーに通信できる必要があります。
- **Hypervisor：** (Version 3.0.1より)ゾーンの最初のクラスターのハイパーバイザーを選択します。ゾーンの追加後に、異なるハイパーバイザーを使用するクラスターを追加できます。
- **Network Offering：** ここでの選択により、ゲスト仮想マシンのネットワークで使用できるネットワークサービスが決まります。

Network Offering	説明
DefaultSharedNetworkOfferingWithSGService	ゲストトラフィックの分離のためにセキュリティグループを有効にする場合は、これを選択します(「セキュリティグループによる仮想マシンに対するトラフィックの制御」を参照)。
DefaultSharedNetworkOffering	セキュリティグループが必要ない場合は、これを選択します。
DefaultSharedNetscalerEIPandELBNetworkOffering	ゾーンネットワークの一部としてCitrix NetScalerアプライアンスを設置済みで、エラスティックIPおよびエラスティック負荷分散の機能を使用する場合は、これを選択します。エラスティックIPおよびエラスティック負荷分散の機能を使用すると、セキュリティグループが有効な基本ゾーンで1対1の静的NATおよび負荷分散を提供できます。

- **Network Domain：** (オプション)ゲスト仮想マシンネットワークに特別なドメイン名を割り当てる場合は、DNSサフィックスを指定します。
- **Public：** すべてのユーザーがパブリックゾーンを利用できます。パブリックではないゾーンは、特定のドメインに割り当てられます。そのドメイン内のユーザーだけが、このゾーンにゲスト仮想マシンを作成することを許可されます。

2. 物理ネットワークにより伝送されるトラフィックの種類を選択します。

   トラフィックの種類は、管理、パブリック、ゲスト、およびストレージトラフィックです。種類について詳しくは、アイコンにマウスポインターを合わせてツールチップを表示するか、「基本ゾーンのネットワークトラフィックの種類」を参照してください。この画面は、いくつかのトラフィックの種類が既に割り当てられた状態で開きます。さらに追加するには、トラフィックの種類をネットワークにドラッグアンドドロップしてください。また、必要に応じてネットワーク名を変更することもできます。

3. (3.0.1 より)物理ネットワーク上の各トラフィックの種類にネットワークトラフィックラベルを割り当てます。このラベルは、ハイパーバイザーホストに定義済みのラベルと一致する必要があります。各ラベルを割り当てるには、トラフィッ クの種類のアイコンの下の[Edit]をクリックします。ラベルを入力するダイアログボックスが開くので入力します。 [OK]をクリックします。

   これらのトラフィックラベルは、最初のクラスターに選択したハイパーバイザーのためにのみ定義します。ほかのすべてのハイパーバイザーについては、ゾーンを作成してからラベルを構成できます。

4. ［Next］をクリックします。

5. (NetScalerのみ)NetScaler用のネットワークオファリングを選択する場合は、追加の表示画面があります。NetScalerのセットアップに必要な項目を入力したら、［Next］をクリックします。
   - **IP address：** NetScalerデバイスのNSIP(NetScaler IP)アドレスです。
   - **UsernameおよびPassword：** デバイスにアクセスするための認証資格情報です。CloudStackは、この資格情報を使用してデバイスにアクセスします。
   - **Type：** 追加するNetScalerデバイスの種類です。［NetScaler VPX］、［NetScaler MPX］、または［NetScaler SDX］です。種類を比較するには、『CloudStack管理ガイド』を参照してください。
   - **Public interface：** パブリックネットワークの一部として構成されるNetScalerのインターフェイスです。
   - **Private interface：** プライベートネットワークの一部として構成されるNetScalerのインターフェイスです。
   - **Number of retries：** 操作が失敗したとみなす前にデバイスに対してコマンドを試行する回数です。デフォルトは2です。
   - **Capacity：** このNetScalerデバイスを共有するゲストネットワーク/アカウントの数です。
   - **Dedicated：** 専用のデバイスは単一のアカウント専用になります。［Dedicated］チェックボックスをオンにすると、［Capacity］ボックスの値は無視され、暗黙的に1であるとみなされます。

6. (NetScalerのみ)パブリックトラフィックのIPアドレスの範囲を構成します。この範囲内のIPアドレスは、EIPおよびELBが有効なNetScalerのネットワークオファリングを選択することによって有効にする、静的NAT機能に使用されます。次の詳細情報を入力し、［Add］をクリックします。必要に応じてこの手順を繰り返し、さらにIPアドレスの範囲を追加できます。完了したら［Next］をクリックします。
   - **Gateway：** これらのIPアドレスに使用するゲートウェイです。
   - **Netmask：** このIPアドレスの範囲に関連付けるネットマスクです。
   - **VLAN：** パブリックトラフィックに使用するVLANです。
   - **Start IPおよびEnd IP：** インターネットからアクセスできるとみなされるIPアドレスの範囲で、ゲスト仮想マシンへのアクセスのために割り当てます。

7. 新しいゾーンでは、CloudStackにより最初のポッドが自動的に追加されます。後でさらにポッドを追加できます。ポッドの概要については、「ポッドについて」を参照してください。

   最初のポッドを構成するには、次の項目を入力して［Next］をクリックします。
   - **Pod Name：** ポッドの名前です。
   - **Reserved system gateway：** このポッド内のホストのゲートウェイです。
   - **Reserved system netmask：** ポッドのサブネットを定義するネットワークプレフィックスです。CIDR表記を使用します。
   - **Start Reserved System IPおよびEnd Reserved System IP：** セカンダリストレージ仮想マシン、コンソールプロキシ仮想マシン、およびDHCPなどのさまざまなシステム仮想マシンを管理するために、CloudStackで使用する管理ネットワーク内のIPアドレスの範囲です。詳しくは、「システムにより予約済みのIPアドレスを

用する管理ネットワーク内のIPアドレスの範囲です。詳しくは、「システムにより予約済みのIPアドレス」を参照してください。

8. ゲストトラフィック用のネットワークを構成します。次の情報を指定してから、［Next］をクリックします。
   - **Guest gateway：** ゲストが使用するゲートウェイです。
   - **Guest netmask：** ゲストの使用するサブネット上で使用されるネットマスクです。
   - **Guest start IPおよびGuest end IP：** CloudStackがゲストに割り当てられるIPアドレスの範囲を定義する、最初と最後のIPアドレスを入力します。

     複数のNICを使用することを強くお勧めします。複数のNICを使用する場合は、別のサブネットに存在するIPアドレスを入力できます。

     NICを1つ使用する場合は、これらのIPアドレスは、ポッドのCIDRと同じCIDRに存在する必要があります。
9. 新しいポッドでは、CloudStackにより最初のクラスターが自動的に追加されます。後でさらにクラスターを追加できます。クラスターの概要については、「クラスターについて」を参照してください。

   最初のクラスターを構成するには、次の項目を入力して［Next］をクリックします。
   - **Hypervisor：** (Version 3.0.0のみ。3.0.1では読み取り専用)このクラスター内のすべてのホストで実行される、ハイパーバイザーソフトウェアの種類を選択します。VMwareを選択すると追加のフィールドが表示され、vSphereクラスターに関する情報を指定できます。vSphereサーバーの場合は、vCenterでホストのクラスターを作成した後、クラスター全体をCloudStackに追加することをお勧めします。「クラスターの追加：vSphere」を参照してください。
   - **Cluster name：** クラスターの名前を入力します。任意の、CloudStackで使用されていないテキストを指定します。
10. 新しいクラスターでは、CloudStackにより最初のホストが自動的に追加されます。後でさらにホストを追加できます。ホストの概要については、「ホストについて」を参照してください。

    注記

    CloudStackを展開するときに、ハイパーバイザーに実行中の仮想マシンがあってはいけません。

    ホストを構成する前に、ハイパーバイザーソフトウェアをホストにインストールする必要があります。CloudStackがサポートするハイパーバイザーソフトウェアのバージョン、およびホストをCloudStackと連動させるために必要な追加構成を確認しておく必要があります。このインストールについて詳しくは、次のセクションを参照してください。
    - Citrix XenServerのインストールと構成
    - VMware vSphereのインストールと構成
    - KVMのインストールと構成

    最初のホストを構成するには、次の項目を入力して［Next］をクリックします。
    - **Host Name：** ホストのDNS名またはIPアドレスです。
    - **Username：** 通常はrootです。
    - **Password：** 上のユーザー名に対するパスワードです(XenServerまたはKVM側で指定したもの)。
    - **Host Tags：** (オプション)ホストを分類して保守を簡単にするために使用するラベルです。例としてクラウドのHAタグを設定できます(ha.tag をグローバル 設定パラメーターに設定します)。もしこのホスト上で仮想マシンを「高可用性」機能を有効化したうえで利用したい場合、管理者ガイドの「HAホスト上での仮想マシンでのHAの有効化」を参照してください。
11. 新しいクラスターでは、CloudStack により最初のプライマリストレージサーバーが自動的に追加されます。後でさらにサーバーを追加できます。プライマリストレージの概要については、「プライマリストレージについて」を参照してください。

    最初のプライマリストレージサーバーを構成するには、次の項目を入力して［Next］をクリックします。
    - **Name：** ストレージデバイスの名前です。
    - **Protocol：** XenServer の場合は、[NFS]、[iSCSI]、または[PreSetup]を選択します。KVM の場合は、[NFS]、[SharedMountPoint]、[CLVM]または[RBD]を選択します。vSphere の場合は、[VMFS](iSCSI またはファイバーチャネル)または [NFS]を選択します。画面のそのほかのフィールドは、ここで選択したものにより異なります。

6.3.2. 拡張ゾーンの構成

1. ゾーンの追加ウィザードで[Advanced]を選択して[Next]をクリックすると、次の詳細の入力を求められます。入力後、[Next]をクリックします。
   - **Name：** ゾーンの名前です。
   - **DNS1およびDNS2：** ゾーン内のゲスト仮想マシンで使用するDNSサーバーです。これらのDNSサーバーには、後で追加するパブリックネットワーク経由でアクセスします。ゾーンのパブリックIPアドレスから、ここで指定するDNSサーバーに通信できる必要があります。
   - **Internal DNS1 および Internal DNS2：** これらの DNS サーバーは、ゾーン内のシステム仮想マシン(仮想ルーター、 コンソールプロキシ、およびセカンダリストレージ仮想マシンなど、CloudStack により使用される仮想マシン)に よって使用されます。これらの DNS サーバーは、システム仮想マシンの管理トラフィックネットワークインターフェイスを介してアクセスされます。ポッドのプライベート IP アドレスから、ここで指定する内部 DNS サーバーに通信できる必要があります。
   - **Network Domain：** (オプション)ゲスト仮想マシンネットワークに特別なドメイン名を割り当てる場合は、DNS サフィックスを指定します。
   - **Guest CIDR：** このゾーンのゲスト仮想ネットワークで使用される IP アドレスを記述する CIDR です。これはたとえば、10.1.1.0/24 です。ゾーンごとに異なる CIDR を設定することをお勧めします。これにより、異なるゾーンのネットワーク間で簡単に VPN をセットアップできるようになります。
   - **Hypervisor：** (Version 3.0.1より) ゾーンの最初のクラスターのハイパーバイザーを選択します。ゾーンの追加後に、異なるハイパーバイザーを使用するクラスターを追加できます。
   - **Public：** すべてのユーザーがパブリックゾーンを利用できます。パブリックではないゾーンは、特定のドメインに割り当てられます。そのドメイン内のユーザーだけが、このゾーンにゲスト仮想マシンを作成することを許可されます。
2. 物理ネットワークにより伝送されるトラフィックの種類を選択します。

トラフィックの種類は、管理、パブリック、ゲスト、およびストレージトラフィックです。種類について詳しくは、アイコンにマウスポインターを合わせてツールチップを表示するか、「拡張ゾーンのネットワークトラフィックの種類」を参照してください。この画面が表示される時点で、1 つのネットワークが既に構成されています。複数の物理ネットワークがある場合は、ネットワークを追加する必要があります。トラフィックの種類をドラッグして非アクティブなネットワークにドロップすると、ネットワークがアクティブになります。トラフィックアイコンをネットワーク間で移動でき ます。たとえば、Network 1 に表示されているデフォルトのトラフィックの種類が実際の設定と一致しない場合は、トラフィックの種類を移動できます。また、必要に応じてネットワーク名を変更することもできます。

3. (Version 3.0.1 より)各物理ネットワーク上の各トラフィックの種類にネットワークトラフィックラベルを割り当てます。このラベルは、ハイパーバイザーホストに定義済みのラベルと一致する必要があります。各ラベルを割り当てるには、各物理ネットワーク内のトラフィックの種類のアイコンの下の[Edit] をクリックします。ラベルを入力するダイアログボック スが開くので入力します。[OK] をクリックします。

   これらのトラフィックラベルは、最初のクラスターに選択したハイパーバイザーのためにのみ定義します。ほかのすべてのハイパーバイザーについては、ゾーンを作成してからラベルを構成できます。

4. ［Next］をクリックします。
5. パブリックインターネットトラフィックの IP アドレスの範囲を構成します。次の詳細情報を入力し、[Add]をクリックしま す。必要に応じてこの手順を繰り返し、さらにパブリックインターネットの IP アドレスの範囲を追加できます。完了し たら[Next]をクリックします。
   - **Gateway :** これらのIPアドレスに使用するゲートウェイです。
   - **Netmask :** このIPアドレスの範囲に関連付けるネットマスクです。
   - **VLAN :** パブリックトラフィックに使用するVLANです。
   - **Start IP および End IP :** インターネットからアクセスできるとみなされる IP アドレスの範囲で、ゲストネットワークへのアクセスのために割り当てます。
6. 新しいゾーンでは、CloudStackにより最初のポッドが自動的に追加されます。後でさらにポッドを追加できます。ポッドの概要については、「ポッドについて」を参照してください。

   最初のポッドを構成するには、次の項目を入力して［Next］をクリックします。
   - **Pod Name :** ポッドの名前です。
   - **Reserved system gateway :** このポッド内のホストのゲートウェイです。
   - **Reserved system netmask :** ポッドのサブネットを定義するネットワークプレフィックスです。CIDR表記を使用します。
   - **Start Reserved System IP および End Reserved System IP :** セカンダリストレージ仮想マシン、コンソールプロキシ仮想マシン、および DHCP などのさまざまなシステム仮想マシンを管理するために、CloudStack で使用する管理ネットワーク内の IP アドレスの範囲です。詳しくは、「システムにより予約済みの IP アドレス」を参照してください。
7. 各物理ネットワークのゲストトラフィックを伝送する VLAN ID の範囲を指定して(「VLAN 割り当ての例」)、[Next] をクリックします。
8. 新しいポッドでは、CloudStack により最初のクラスターが自動的に追加されます。後でさらにクラスターを追加できます。クラスターの概要については、「クラスタについて」を参照してください。

   最初のクラスターを構成するには、次の項目を入力して［Next］をクリックします。
   - **Hypervisor :** (Version 3.0.0 のみ。3.0.1 では読み取り専用)このクラスター内のすべてのホストで実行される、ハイパーバイザーソフトウェアの種類を選択します。VMware を選択すると追加のフィールドが表示され、vSphere クラスターに関する情報を指定できます。vSphere サーバーの場合は、vCenter でホストのクラスターを作成した後、クラスター全体を CloudStack に追加することをお勧めします。「クラスターの追加:vSphere」参照してください。
   - **Cluster name :** クラスターの名前を入力します。任意の、CloudStackで使用されていないテキストを指定します。
9. 新しいクラスターでは、CloudStack により最初のホストが自動的に追加されます。後でさらにホストを追加できます。\nホストの概要については、「ホストについて」を参照してください。

注記

CloudStack を展開するときに、ハイパーバイザーに実行中の仮想マシンがあってはいけません。

   ホストを構成する前に、ハイパーバイザーソフトウェアをホストにインストールする必要があります。CloudStackがサポートするハイパーバイザーソフトウェアのバージョン、およびホストをCloudStackと連動させるために必要な追加構成を確認しておく必要があります。このインストールについて詳しくは、次のセクションを参照してください。
   - CloudStackのためのCitrix XenServerのインストール
   - VMware vSphereのインストールと設定
   - KVMのインストールと設定

   最初のホストを構成するには、次の項目を入力して［Next］をクリックします。
   - **Host Name :** ホストのDNS名またはIPアドレスです。
   - **Username :** 通常は root です。
   - **Password :** 上のユーザー名に対するパスワードです(XenServerまたはKVM側で指定したもの)。
   - Host Tags:(オプション)ホストを分類して保守を簡単にするために使用するラベルです。例としてクラウドのHAタグを設定できます(ha.tag をグローバル設定パラメーターに設定します)。もしこのホスト上で仮想マシンを「高可用性」機能を有効化したうえで利用したい場合、管理者ガイドの「HAホスト上での仮想マシンでのHAの有効化」を参照してください。
10. 新しいクラスターでは、CloudStack により最初のプライマリストレージサーバーが自動的に追加されます。後でさらにサーバーを追加できます。プライマリストレージの概要については、「プライマリストレージについて」を参照してください。

    最初のプライマリストレージサーバーを構成するには、次の項目を入力して［Next］をクリックします。
    - **Name :** ストレージデバイスの名前です。
    - **Protocol :** XenServer の場合は、[NFS]、[iSCSI]、または[PreSetup]を選択します。KVM の場合は、[NFS]、[SharedMountPoint]、[CLVM]または[RBD]を選択します。vSphere の場合は、[VMFS](iSCSI またはファイバーチャネル)または [NFS]を選択します。画面のそのほかのフィールドは、ここで選択したものにより異なります。

ライバル)または [NFS] を選択します。画面のそのほかのフィールドは、ここで選択したものにより異なります。

NFS	**Server :** ストレージデバイスの IP アドレスまたは DNS 名です。 **Path :** サーバーからエクスポートされたパスです。 **Tags(オプション) :** このストレージデバイス用のタグをコンマで区切って指定し ます。ディスクオファリングのタグと同等、またはそのスーパーセットである必要があります。 プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。
iSCSI	**Server :** ストレージデバイスの IP アドレスまたは DNS 名です。 **Target IQN :** ターゲットの IQN です。たとえば、「iqn.1986-03.com.sun:02:01ec9bb549-1271378984」とします。 **LUN :** LUN 番号です。たとえば、「3」とします。 **Tags(オプション) :** このストレージデバイス用のタグをコンマで区切って指定し ます。ディスクオファリングのタグと同等、またはそのスーパーセットである必要があります。 プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。
事前セットアップ	**Server :** ストレージデバイスの IP アドレスまたは DNS 名です。 **SR Name-Label :** CloudStack の外部にセットアップしたストレージリポジトリの名前ラベルを入力します。 **Tags(オプション) :** このストレージデバイス用のタグをコンマで区切って指定し ます。ディスクオファリングのタグと同等、またはそのスーパーセットである必要があります。 プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。
共有マウントポイント	**Path :** 各ホストのこのプライマリストレージがマウントされるパスです。たとえば、「/mnt/primary」とします。 **Tags(オプション) :** このストレージデバイス用のタグをコンマで区切って指定し ます。ディスクオファリングのタグと同等、またはそのスーパーセットである必要があります。 プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。
VMFS	**Server :** vCenter サーバーの IP アドレスまたは DNS 名です。 **Path :** データセンター名とデータストア名の組み合わせです。形式は、「/データセンター名/データストア名」です。たとえば、「/cloud.dc.VM/cluster1datastore」とします。 **Tags(オプション) :** このストレージデバイス用のタグをコンマで区切って指定し ます。ディスクオファリングのタグと同等、またはそのスーパーセットである必要があります。 プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。

11. 新しいゾーンでは、CloudStack により最初のセカンダリストレージサーバーが自動的に追加されます。セカンダリストレージの概要については、「セカンダリストレージについて」を参照してください。
    この画面に入力する前に、NFS 共有をセットアップして最新の CloudStack システム仮想マシンテンプレートをインストールし、セカンダリストレージを準備する必要があります。「セカンダリストレージの追加」を参照してく

ください。

- **NFS Server.** The IP address of the server or fully qualified domain name of the server.
- **Path :** サーバーからエクスポートされたパスです。

12. [Launch] をクリックします。

6.4. ポッドの追加

新しいゾーンを作成すると、CloudStack により最初のポッドが自動的に追加されます。このセクションの手順に従って、ポッドをいつでも追加できます。

1. CloudStack ユーザーインターフェイスにログインします。「UIへのログイン」 を参照してください。
2. 左側のナビゲーションバーで[Infrastructure]をクリックします。[Zones]で[View More]をクリックし、ポッドを追加するゾーンを選択します。
3. [Compute and Storage]タブをクリックします。ダイアグラムの[Pods]ノードの[View All]をクリックします。
4. [Add Pod]をクリックします。
5. ダイアログボックスに次の詳細情報を入力します。
   - **Name:** ポッドの名前です。
   - **Gateway:** このポッド内のホストのゲートウェイです。
   - **Netmask:** ポッドのサブネットを定義するネットワークプレフィックスです。CIDR 表記を使用します。
   - **Start Reserved System IPおよびEnd Reserved System IP:** セカンダリストレージ仮想マシン、コンソールプロキシ仮想マシン、およびDHCPなどのさまざまなシステム仮想マシンを管理するために、CloudStack で使用する管理ネットワーク内のIPアドレスの範囲です。詳しくは、「システムにより予約済みのIPアドレス」を参照してください。
6. [OK]をクリックします。

6.5. クラスタの追加

CloudStack に管理対象のホストを認識させる必要があります。ホストはクラスター内にあるため、ホストをクラウドに追加するには少なくとも 1 つのクラスターを追加する必要があります。

6.5.1. クラスターの追加:KVM または XenServer

次の手順は、ハイパーバイザーをホストにインストール済みで CloudStack ユーザーインターフェイスにログイン済みであることを前提としています。

1. 左側のナビゲーションバーで[Infrastructure]をクリックします。[Zones]で[View More]をクリックし、クラスターを追加するゾーンを選択します。
2. [Compute] タブをクリックします。
3. ダイアグラムの[Clusters]ノードの[View All]をクリックします。
4. [Add Cluster]をクリックします。
5. このクラスターのハイパーバイザーの種類を選択します。
6. クラスターを作成するポッドを選択します。
7. クラスターの名前を入力します。任意の、CloudStack で使用されていないテキストを指定します。
8. [OK]をクリックします。

6.5.2. クラスターの追加:vSphere

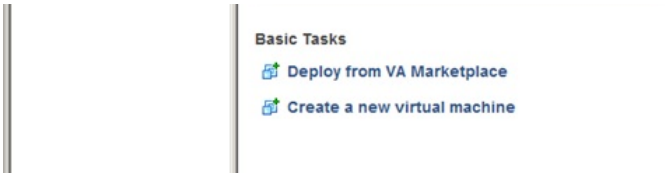
vSphere のホスト管理は、vCenter および CloudStack の管理者ユーザーインターフェイスを組み合わせて行います。CloudStack では、すべてのホストが CloudStack クラスターにあることが必要ですが、クラスターを単一のホストで構成することもできます。管理者はクラスターに 1 台のホストを使用するか、複数のホストを使用するかを決定する必要があります。 複数ホストのクラスターでは、ライブマイグレーションのような機能を使用できます。クラスターには、NFS または iSCSI のような共有ストレージも必要です。

vSphere サーバーの場合は、vCenter でホストのクラスターを作成した後、クラスター全体を CloudStack に追加することをお勧めします。次の要件に従ってください。

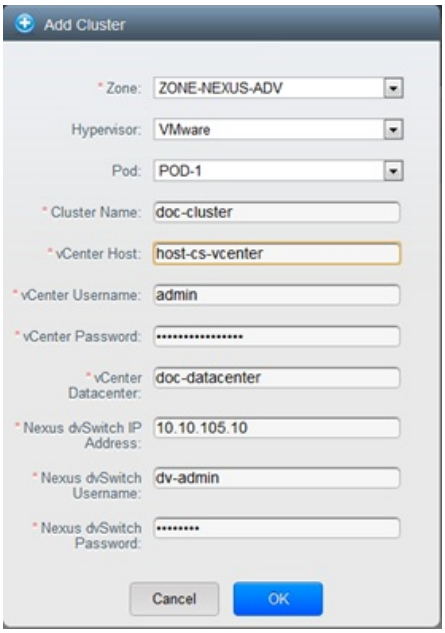
- vSphere クラスターに配置するホストは 8 台までにしてください。
- ハイパーバイザーホストに実行中の仮想マシンがないことを確認してから、CloudStack に追加してください。

vSphere クラスターを CloudStack に追加するには

1. vCenter でホストのクラスターを作成します。vCenter の指示に従って、これを実行します。クラスターを作成すると、 vCenter には次のように表示されます。



2. ユーザーインターフェイスにログインします。
3. 左側のナビゲーションバーで[Infrastructure]をクリックします。[Zones]で[View More]をクリックし、クラスターを追加するゾーンを選択します。
4. [Compute]タブをクリックし、[Pods]の[View All]をクリックします。クラスターを追加するポッドを選択します。
5. [View Clusters]をクリックします。
6. [Add Cluster]をクリックします。
7. [Hypervisor]ボックスの一覧で、[VMware]を選択します。
8. ダイアログボックスに次の情報を入力します。次のフィールドによって、vCenter 側の値を参照できるようになりま す。
   - Cluster Name: vCenter で作成したクラスターの名前を入力します。たとえば、「cloud.cluster.2.2.1」とします。
   - vCenter Host: vCenter サーバーのホスト名または IP アドレスを入力します。
   - vCenter Username: CloudStack が vCenter への接続に使用するユーザー名を入力します。このユーザーにはすべての管理特権が必要です。
   - vCenter Password: 上記のユーザー名に対するパスワードを入力します。
   - vCenter Datacenter: クラスターが存在する vCenter データセンターを入力します。たとえば、「cloud.dc.VM」とします。



   - クラスターがプロビジョニングされる間、多少の遅延が発生する場合があります。ユーザーインターフェイスにクラスターが自動的に表示されます。

6.6. ホストの追加

1. CloudStack 構成としてホストを追加する前に選択したハイパーバイザーをホストにインストールする必要があります。CloudStack ホストを様々なハイパーバイザー下で動作する仮想マシンとともに管理することができます。
   CloudStack インストールガイドではそれぞれのサポートされるハイパーバイザーを CloudStack からどのように利用するかインストール方法や設定方法を提供しています。どのバージョンのハイパーバイザーがサポートされているか「インストールガイドの」適切なセクションを参照することは CloudStack でハイパーバイザーホストを構成するための重要なステップになります。

警告

それぞれのハイパーバイザーに対して「ハイパーバイザーのインストール」で述べられる CloudStack 特有の構成手順を確認してください。

2. CloudStack に対しホストを追加します。関連する技術情報は利用するハイパーバイザーによって異なります。
   - 「ホストの追加(XenServer または KVM)」
   - 「ホストの追加 (vSphere)」

6.6.1. ホストの追加(XenServer または KVM)

XenServer および KVM のホストは、いつでもクラスターに追加できます。

6.6.1.1. XenServer および KVM ホストの要件

警告

ハイパーバイザーホストに実行中の仮想マ シンがないことを確認してから、CloudStack に追加してください。

構成要件

- 各クラスターには同一のハイパーバイザーを使用するホストのみを含める必要があります。
- XenServer の場合は、クラスターに配置するホストは 8 台までにしてください。
- KVM の場合は、クラスターに配置するホストは 16 台までにしてください。

ハードウェア要件については、CloudStack インストールガイドのハイパーバイザー毎のインストールセクションを参照してください。

6.6.1.1.1. XenServer ホストの追加要件

ネットワークボンディングを使用する場合は、管理者はホストの配線を、クラスター内のほかのホストと完全に同じにする必要があります。

クラスターに追加するすべてのホストに対して次のコマンドを実行します。これで、ホストが XenServer プールのマスターに加わります。

```
# xe pool-join master-address=[master IP] master-username=root master-password=[your
password]
```

注記

コマンドをコピーして実行するときは、単一の行として貼り付けたことを確認してください。一部のドキュメントビューアーでは、コピーしたテキストに不要な改行が含まれる可能性があります。

XenServer プールにすべてのホストを追加したら、cloud-setup-bond スクリプトを実行します。このスクリプトにより、クラスター内の新しいホストのボンドの構成とセットアップを完了します。

1. Copy the script from the Management Server in /usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh to the master host and ensure it is executable.
2. 次のスクリプトを実行します。

   ```
   # ./cloud-setup-bonding.sh
   ```

6.6.1.1.2. KVM ホストの追加要件

- 共有マウントポイントストレージを使用する場合は、管理者は新しいホストのすべてのマウントポイントを(マウントされたストレージも含めて)、クラスター内のほかのホストと完全に同じにする必要があります。
- 新しいホストのネットワーク構成(ゲスト、プライベート、およびパブリックネットワーク)が、クラスター内のほかのホ ストと同じであることを確認してください。
- OpenVswitch のブリッジを利用している場合は CloudStack にホストを追加するまえに KVM ホストの agent.properties を編集し network.bridge.type パラメーターを openvswitch に設定してください。

6.6.1.2. XenServer または KVM ホストの追加

- ホストにハイパーバイザーソフトウェアをまだインストールしていない場合はインストールします。CloudStack がサポートするハイパーバイザーソフトウェアのバージョン、およびホストを CloudStack と連動させるために必要な追加構成を確認しておく必要があります。このインストールの詳細については、CloudStack インストールガイドからハイパーバイザー毎の適切なセクションを参照してください。
- CloudStackユーザーインターフェイスに管理者としてログオンします。
- 左側のナビゲーションバーで[Infrastructure]をクリックします。[Zones]で[View More]をクリックし、ホストを追加するゾーンを選択します。
- [Compute]タブをクリックします。[Clusters]ノードの[View All]をクリックします。
- ホストを追加するクラスターを選択します。
- [View Hosts]をクリックします。
- [Add Host]をクリックします。
- 次の情報を指定します。

  Host Name: ホストの DNS 名または IP アドレスです。

  Username: 通常は root です。

  Password: XenServer または KVM 側で指定した、上のユーザー名に対するパスワードです。

  Host Tags(オプション): ホストを分類して保守を簡単にするために使用するラベルです。たとえばホストに対し仮想マシンの高可用機能を有効化した場合、クラウドの HA タグ(グローバル設定で ha.tag に設定したパラメーター)を設定することができます。詳細な情報は 「仮想マシンでの高可用性の有効化」や「ホストの高可用性」を参照してください。

  ホストがプロビジョニングされる間、多少の遅延が発生する場合があります。ユーザーインターフェイスにホストが自動的に表示されます。
- 追加のホストについて、この手順を繰り返します。

6.6.2. ホストの追加 (vSphere)

vSphereサーバーに対してはvCenterでクラスターを作成し、クラスター全体をCloudStack に対し追加することを推奨します。詳しくはクラスターの追加(vSphere)を参照してください。

6.7. プライマリストレージの追加

6.7.1. プライマリストレージのシステム要件

ハードウェア要件:

- 基になるハイパーバイザーでサポートされている標準準拠の任意の iSCSI または NFS サーバー。
- ストレージサーバーは、多数のディスクを備えたコンピューターである必要があります。ディスクは、ハードウェア RAID コントローラーで管理するのが理想的です。
- 最小限必要な容量はニーズにより異なります。

プライマリストレージをセットアップするときには次の制限に従ってください。

- プライマリストレージは、ホストをクラスターに追加しなくては追加できません。
- 共有プライマリストレージを準備しない場合は、グローバル構成パラメーターの system.vm.local.storage.required を true に設定する必要があります。設定しないと仮想マシンを起動できません。

6.7.2. プライマリストレージの追加

新しいゾーンを作成するとき、手順の一部として最初のプライマリスト レージが追加されます。プライマリストレージサーバーは、新しいクラスターを追加するときや既存のクラスターにサーバーを追加するときなど、いつでも追加できます。

警告

サーバーに何も格納されていないことを確認 してください。CloudStack にサーバーを追加すると、既存のデータはすべて破棄されます。

1. CloudStack ユーザーインターフェイスにログインします(「UIへのログイン」 を参照)。
2. 左側のナビゲーションバーで [Infrastructure] をクリックします。[Zones] で [View More] をクリックし、プライマリストレージを追加するゾーンを選択します。
3. [Compute] タブをクリックします。
4. ダイアグラムの [Primary Storage] ノードの [View All] をクリックします。
5. [Add Primary Storage] をクリックします。
6. ダイアログボックスに次の情報を入力します。必要な情報は、選択するプロトコルによって異なります。
   - **Pod:** ストレージデバイスのポッドです。
   - **Cluster:** ストレージデバイスのクラスターです。
   - **Name :** ストレージデバイスの名前です。
   - **Protocol:** XenServer の場合は、[NFS]、[iSCSI]、または[PreSetup]を選択します。KVM の場合は、[NFS]ま たは[SharedMountPoint]を選択します。vSphere の場合は、[VMFS](iSCSI またはファイバーチャネル)または [NFS] を選択します。
   - **Server(NFS、 iSCSI、 または PreSetup の場合):** ストレージデバイスの IP アドレスまたは DNS 名です。
   - **Server(VMFS の場合):** vCenter サーバーの IP アドレスまたは DNS 名です。
   - **Path(NFS の場合):** NFS の場合、これはサーバーからエクスポートされたパスです。
   - **Path(VMFS の場合):** vSphere の場合、データセンター名とデータストア名の組み合わせです。形式は、「/データセンター名/データストア名」です。たとえば、「/cloud.dc.VM/cluster1datastore」とします。
   - **Path(SharedMountPoint の場合):** KVM の場合、各ホストのこのプライマリストレージがマウントされるパスです。 たとえば、「/mnt/primary」とします。
   - **SR Name-Label(PreSetup の場合):** CloudStack の外部にセットアップしたストレージリポジトリの名前ラベルを入力します。
   - **Target IQN(iSCSI の場合):** iSCSI の場合、ターゲットの IQN です。たとえば、 「iqn.1986-03.com.sun:02:01ec9bb549-1271378984」とします。
   - **Lun 番号(iSCSI の場合):** iSCSI の場合、LUN 番号です。たとえば、「3」とします。
   - **Tags(オプション):** このストレージデバイス用のタグをコンマで区切って指定します。ディスクオファリングのタグ\nと同等、またはそのスーパーセットである必要があります。

   プライマリストレージのタグセットは、ゾーン内のクラスター間で同一である必要があります。たとえば、クラスターA でプライマリストレージのタグが T1 および T2 の場合は、同じゾーン内のほかのすべてのクラスターでもプライマリス トレージのタグを T1 および T2 にする必要があります。
7. [OK]をクリックします。

6.8. セカンダリストレージの追加

6.8.1. セカンダリストレージのシステム要件

- NFS ストレージアプライアンスまたは Linux NFS サーバー
- (オプション)OpenStack Object Storage(Swift) (http://swift.openstack.org を参照してください)
- 最小容量として 100GB
- セカンダリストレージデバイスは、そのストレージを使用するゲスト仮想マシンと同じゾーンに配置する必要があります。

- 各セカンダリストレージサーバーは、ゾーン内のすべてのホストで使用できる必要があります。

6.8.2. セカンダリストレージの追加

新しいゾーンを作成するとき、手順の一部として最初のセカンダリス トレージが追加されます。いつでもセカンダリストレージサーバーを 追加して、既存のゾーンにサーバーを追加することができます。

警告

サーバーに何も格納されていないことを確認 してください。CloudStack にサーバーを追加すると、既存のデータはすべて破棄されます。

1. クラウド全体のセカンダリストレージとして Swift を使用する場合は、ゾーンに対してローカルなセカンダリストレージサーバーを追加する前に、CloudStack に Swift ストレージを追加する必要があります。「ゾーンの追加」を参照してくだ さい。
2. ゾーンに対してローカルなセカンダリストレージの準備のため、管理サーバーのインストール中に NFS 共有を作成しマウントしておく必要があります。 「NFS共有の準備」 を参照してください。
3. 管理サーバーのインストール中にシステム仮想マシンテンプレートを準備したことを確認します。See 「システム仮想マシンテンプレートの準備」. を参照してください。
4. これでゾーン単位のストレージとしてセカンダリストレージサーバーの準備ができたので、CloudStack に追加します。 新しいゾーンの追加手順の一部として、セカンダリストレージが追加されます。 「ゾーンの追加」 を参照してください。

6.9. 初期化とテスト

すべての構成が終わると、CloudStack が初期化されます。ネットワークの速度によっては、30 分以上かかる可能性があります。初期化が正常に完了すると、管理者のダッシュボードが CloudStack ユーザーインターフェイスに表示されます。

1. システムが準備完了状態であることを確認します。左側のナビゲーションバーで[Templates]をクリックします。CentOS 5.5(64bit) no Gui(KVM)を選択します。状態が「Download Complete」であることを確認します。この状態になるまで、次の手順には進まないでください。
2. [Instances]タブで、[Filter By]ボックスの一覧で[My Instances]を選択します。
3. [Add Instance]をクリックして、ウィザードの指示に従います。
    a. 追加したばかりのゾーンを選択します。
    b. 仮想マシンで使用するテンプレートを選択します。これが新規インストールの場合は、おそらく組み込みのCentOS テンプレートのみを使用できます。
    c. サービスオファリングを選択します。使用するハードウェアで、選択したサービスオファリングを開始できることを確認してください。
    d. 必要に応じて、データディスクオファリングにもう 1 つデータディスクを追加します。これはゲストが使用できる 2 番目のボリュームですが、マウントはされません。たとえば、XenServer 上の Linux では、仮想マシンの再起動 後にゲストで/dev/xvdb が認識されます。PV が有効なオペレーティングシステムカーネルの場合は再起動が不 要です。
    e. デフォルトネットワークで、ゲストのプライマリネットワークを選択します。基本インストールでは、このオプションは 1 つしかありません。
    f. オプションで、仮想マシンに名前を付けてグループを割り当てます。仮想マシンを説明するお好みのテキストを使用します。
    g. Click Launch VM. Your VM will be created and started. It might take some time to download the template and complete the VM startup. You can watch the VMâ€™s progress in the Instances screen.
4. 仮想マシンを使用するには[View Console]をクリックします。 
   For more information about using VMs, including instructions for how to allow incoming network traffic to the VM, start, stop, and delete VMs, and move a VM from one host to another, see Working With Virtual Machines in the Administratorâ€™s Guide.

これで、CloudStack のインストールが完了しました。

展開を拡張する場合は、さらにホスト、プライマリストレージ、ゾーン、ポッド、およびクラスターを追加できます。

第7章 Global Configuration Parameters

7.1. グローバル構成パラメーターの設定

CloudStack には、クラウドのさまざまな側面を制御するために設定できるパラメーターが備わっています。CloudStack を初めてインストールするとき、そしてその後で定期的に、これらの設定を変更する必要が出てくる可能性があります。

1. ユーザーインターフェイスに管理者としてログインします。

2. 左側のナビゲーションバーで[Global Settings]をクリックします。
3. [Select view]ボックスの一覧で次のどちらかを選択します。
   - Global Settings: パラメーターが、簡単な説明と現在の値と共に一覧表示されます。
   - Hypervisor Capabilities: ハイパーバイザーのバージョンが、それぞれにサポートされるゲスト数の上限と共に一覧表示されます。
4. 検索ボックスを使用して、関心のある項目のみが表示されるように一覧内容を絞り込みます。
5. 値を変更するには[Edit]アイコンをクリックします。ハイパーバイザーの機能を表示する場合は、編集画面を開くためにまずハイパーバイザー名をクリックする必要があります。

7.2. About Global Configuration Parameters

CloudStack provides a variety of settings you can use to set limits, configure features, and enable or disable features in the cloud. Once your Management Server is running, you might need to set some of these global configuration parameters, depending on what optional features you are setting up.

To modify global configuration parameters, use the steps in "Setting Global Configuration Parameters."

The documentation for each CloudStack feature should direct you to the names of the applicable parameters. Many of them are discussed in the CloudStack Administration Guide. The following table shows a few of the more useful parameters.

Field	値
management.network.cidr	A CIDR that describes the network that the management CIDRs reside on. This variable must be set for deployments that use vSphere. It is recommended to be set for other deployments as well. Example: 192.168.3.0/24.
xen.setup.multipath	For XenServer nodes, this is a true/false variable that instructs CloudStack to enable iSCSI multipath on the XenServer Hosts when they are added. This defaults to false. Set it to true if you would like CloudStack to enable multipath. If this is true for a NFS-based deployment multipath will still be enabled on the XenServer host. However, this does not impact NFS operation and is harmless.
secstorage.allowed.internal.sites	This is used to protect your internal network from rogue attempts to download arbitrary files using the template download feature. This is a comma-separated list of CIDRs. If a requested URL matches any of these CIDRs the Secondary Storage VM will use the private network interface to fetch the URL. Other URLs will go through the public interface. We suggest you set this to 1 or 2 hardened internal machines where you keep your templates. For example, set it to 192.168.1.66/32.
use.local.storage	Determines whether CloudStack will use storage that is local to the Host for data disks, templates, and snapshots. By default CloudStack will not use this storage. You should change this to true if you want to use local storage and you understand the reliability and feature drawbacks to choosing local storage.
host	This is the IP address of the Management Server. If you are using multiple Management Servers you should enter a load balanced IP address that is reachable via the private network.
default.page.size	Maximum number of items per page that can be returned by a CloudStack API command. The limit applies at the cloud level and can vary from cloud to cloud. You can override this with a lower value on a particular API call by using the page and pagesize API command parameters. For more information, see the Developer's Guide. Default: 500.
ha.tag	The label you want to use throughout

ha.tag	This label you want to use throughout the cloud to designate certain hosts as dedicated HA hosts. These hosts will be used only for HA-enabled VMs that are restarting due to the failure of another host. For example, you could set this to ha_host. Specify the ha.tag value as a host tag when you add a new host to the cloud.

第8章 Hypervisor Installation

8.1. KVM のインストールと構成

8.1.1. KVM ホストのシステム要件

KVM は、さまざまな Linux ベースのオペレーティングシステムに含まれています。以下のディストリビューションは必須ではありませんが推奨となります。

- CentOS / RHEL: 6.3
- Ubuntu: 12.04(.1)

KVM ハイパーバイザーにおける主要な要件は libvirt と Qemu のバージョンになります。どの Linux ディストリビューションを利用するかに関わらず\n以下の要件を満たしているか確認する必要があります。

- libvirt: 0.9.4以降
- Qemu/KVM: 1.0以降

CloudStack でのデフォルトのブリッジは Linux ネイティブのブリッジ実装(ブリッジモジュール) になります。CloudStack はオプションとして OpenVswitch を動作させる仕組みを内包しており以下のような要件があります。

- libvirt: 0.9.11以上のバージョン
- openvswitch: 1.7.1以上のバージョン

加えて以下のハードウェア要件が必要となります。

- 1つのクラスター内のホストではバージョンを統一する。
- 1つのクラスター内のホストは種類が同じである必要があります。つまり、CPUの種類と数が同じで、同じ機能フラグである必要があります。
- HVM (Intel VT or AMD-V) が有効である必要があります。

- HVM (Intel-VT or AMD-V が有効である) 必要があります。
- 64-bit x86 CPU(多くのコアを用意することでパフォーマンスの向上が見込まれます)。
- 4GBのメモリ。
- 最少1つ以上のNIC。
- CloudStack が展開された際、ハイパーバイザーホストに既に動作しているVMが存在していない。

8.1.2. KVM インストールの概要s

Linux Kernel Virtual Machine(KVM) ハイパーバイザーを使用してゲスト仮想マシンを実行する場合は、クラウド内のホストに KVM をインストールします。ここでは、KVM のインストールドキュメントと重複しない、CloudStack 特有の設定について説明します。

警告

作業を続ける前に、ホストに対して最新のアップデートが適用されていることを確認してください。

警告

CloudStack の制御下にないホスト上でサービスを動作させることは推奨されません。

KVM ハイパーバイザーをインストールする手順は次のとおりです。

1. オペレーティングシステムの準備
2. libvirt のインストールと設定
3. セキュリティポリシーの設定 (AppArmor と SELinux)
4. エージェントのインストールと設定

8.1.3. オペレーティングシステムの準備

ホストのOSは CloudStack エージェントと KVM インスタンスが動作するよう準備される必要があります。

1. オペレーティングシステムにルートユーザーとしてログオンします。
2. 完全修飾ホスト名を確認します。

   ```
   $ hostname --fqdn
   ```

   これにより、「kvm1.lab.example.org」のような完全修飾ホスト名が返されます。そうでない場合は、そうなるように /etc/hosts を編集します。
3. 管理サーバーからインターネットに接続できることを確認します。

   ```
   $ ping www.cloudstack.org
   ```

4. 時刻を同期するために NTP を有効にします。

   注記

   クラウドのサーバーのクロックを同期するた めに NTP が必要です。時刻同期がされないと予期しない問題が発生する可能性があります。

   a. NTP のインストール

      ```
      $ yum install ntp
      ```

      ```
      $ apt-get install openntpd
      ```

5. これらの手順を全てのハイパーバイザーホストで実行します。

8.1.4. エージェントのインストールと設定

CloudStack ホスト上で KVM インスタンスを管理するにはエージェントを利用する必要があります。エージェントは管理サーバーと通信しホスト上の全てのインスタンスを制御します。

まず、エージェントをインストールします。

RHELもしくはCentOSの場合:

```
$ yum install cloudstack-agent
```

Ubuntuの場合:

```
$ apt-get install cloudstack-agent
```

これでホストをクラスターに追加する準備ができました。詳細に関しては後の項で説明されますのでこちら「ホストの追加」を参照してください。ホストを追加する前に上記ドキュメントを参照することを推奨します。

8.1.5. libvirt の構成とインストール

CloudStack uses libvirt for managing virtual machines. Therefore it is vital that libvirt is configured correctly. Libvirt is a dependency of cloudstack-agent and should already be installed.

1. libvirt を用いてライブマイグレーションを実施するにはセキュアでない TCP コネクションを開放する必要があります。また、libvirt がマルチキャストの DNS アドバタイズを試行しないよう無効化する必要があります。これらの設定方法は **/etc/libvirt/libvirtd.conf** にて編集してください。

   Set the following parameters:

   ```
   listen_tls = 0
   ```

   ```
   listen_tcp = 1
   ```

   ```
   tcp_port = "16509"
   ```

   ```
   auth_tcp = "none"
   ```

   ```
   mdns_adv = 0
   ```

2. libvirtd.conf では "listen_tcp" だけでなくいくつかのパラメーターを以下のように設定する必要があります。
   RHEL や CentOS を利用している場合は **/etc/sysconfig/libvirtd** を編集してください。
   次の行のコメントを外してください。

   ```
   #LIBVIRTD_ARGS="--listen"
   ```

   Ubuntu を利用している場合は **/etc/init/libvirt-bin.conf** を編集してください。
   以下の行を変更してください(ファイルの行末):

   ```
   exec /usr/sbin/libvirtd -d
   ```

   -l オプションをつける場合

   ```
   exec /usr/sbin/libvirtd -d -l
   ```

3. libvirt を再起動します。
   RHELもしくはCentOSの場合:

   ```
   $ service libvirtd restart
   ```

   Ubuntuの場合:

   ```
   $ service libvirt-bin restart
   ```

8.1.6. Configure the Security Policies

CloudStack does various things which can be blocked by security mechanisms like AppArmor and SELinux. These have to be disabled to ensure the Agent has all the required permissions.

1. Configure SELinux (RHEL and CentOS)
   a. Check to see whether SELinux is installed on your machine. If not, you can skip this section.
      In RHEL or CentOS, SELinux is installed and enabled by default. You can verify this with:

      ```
      $ rpm -qa | grep selinux
      ```

   b. Set the SELINUX variable in **/etc/selinux/config** to "permissive". This ensures that the permissive setting will be maintained after a system reboot.
      RHELもしくはCentOSの場合:

      ```
      vi /etc/selinux/config
      ```

      Change the following line

      ```
      SELINUX=enforcing
      ```

      to this

      ```
      SELINUX=permissive
      ```

   c. SELinuxをpermissiveにすると即座に適用され、システムの再起動は必要ありません。

      ```
      $ setenforce permissive
      ```

2. Configure Apparmor (Ubuntu)
   a. Check to see whether AppArmor is installed on your machine. If not, you can skip this section.
      In Ubuntu AppArmor is installed and enabled by default. You can verify this with:

      ```
      $ dpkg --list 'apparmor'
      ```

   b. Disable the AppArmor profiles for libvirt

      ```
      $ ln -s /etc/apparmor.d/usr.sbin.libvirtd /etc/apparmor.d/disable/
      ```

      ```
      $ ln -s /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper /etc/apparmor.d/disable/
      ```

      ```
      $ apparmor_parser -R /etc/apparmor.d/usr.sbin.libvirtd
      ```

      ```
      $ apparmor_parser -R /etc/apparmor.d/usr.lib.libvirt.virt-aa-helper
      ```

8.1.7. Configure the network bridges

警告

This is a very important section, please make sure you read this thoroughly.

注記

This section details how to configure bridges using the native implementation in Linux. Please refer to the next section if you intend to use OpenVswitch

In order to forward traffic to your instances you will need at least two bridges: *public* and *private*.

By default these bridges are called *cloudbr0* and *cloudbr1*, but you do have to make sure they are available on each hypervisor.

The most important factor is that you keep the configuration consistent on all your hypervisors.

8.1.7.1. Network example

There are many ways to configure your network. In the Basic networking mode you should have two (V)LAN's, one for your private network and one for the public network.

We assume that the hypervisor has one NIC (eth0) with three tagged VLAN's:

1. VLAN 100 for management of the hypervisor
2. VLAN 200 for public network of the instances (cloudbr0)
3. VLAN 300 for private network of the instances (cloudbr1)

On VLAN 100 we give the Hypervisor the IP-Address 192.168.42.11/24 with the gateway 192.168.42.1

注記

The Hypervisor and Management server don't have to be in the same subnet!

8.1.7.2. Configuring the network bridges

It depends on the distribution you are using how to configure these, below you'll find examples for RHEL/CentOS and Ubuntu.

注記

The goal is to have two bridges called 'cloudbr0' and 'cloudbr1' after this section. This should be used as a guideline only. The exact configuration will depend on your network layout.

8.1.7.2.1. Configure in RHEL or CentOS

The required packages were installed when libvirt was installed, we can proceed to configuring the network.

First we configure eth0

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Make sure it looks similar to:

```
DEVICE=eth0
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
```

We now have to configure the three VLAN interfaces:

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.100
```

```
DEVICE=eth0.100
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
IPADDR=192.168.42.11
GATEWAY=192.168.42.1
NETMASK=255.255.255.0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.200
```

```
DEVICE=eth0.200
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
BRIDGE=cloudbr0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0.300
```

```
DEVICE=eth0.300
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
VLAN=yes
BRIDGE=cloudbr1
```

Now we have the VLAN interfaces configured we can add the bridges on top of them.

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr0
```

Now we just configure it is a plain bridge without an IP-Address

```
DEVICE=cloudbr0
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
IPV6INIT=no
IPV6_AUTOCONF=no
DELAY=5
STP=yes
```

We do the same for cloudbr1

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr1
```

```
DEVICE=cloudbr1
TYPE=Bridge
ONBOOT=yes
BOOTPROTO=none
IPV6INIT=no
IPV6_AUTOCONF=no
DELAY=5
STP=yes
```

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.

警告

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

8.1.7.2.2. Configure in Ubuntu

All the required packages were installed when you installed libvirt, so we only have to configure the network.

```
vi /etc/network/interfaces
```

Modify the interfaces file to look like this:

```
auto lo
iface lo inet loopback

# The primary network interface
auto eth0.100
iface eth0.100 inet static
    address 192.168.42.11
    netmask 255.255.255.240
    gateway 192.168.42.1
    dns-nameservers 8.8.8.8 8.8.4.4
    dns-domain lab.example.org

# Public network
auto cloudbr0
iface cloudbr0 inet manual
    bridge_ports eth0.200
    bridge_fd 5
    bridge_stp off
    bridge_maxwait 1

# Private network
auto cloudbr1
iface cloudbr1 inet manual
    bridge_ports eth0.300
    bridge_fd 5
```

```
    bridge_stp off
    bridge_maxwait 1
```

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.

警告

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

8.1.8. Configure the network using OpenVswitch

警告

This is a very important section, please make sure you read this thoroughly.

In order to forward traffic to your instances you will need at least two bridges: *public* and *private*.

By default these bridges are called *cloudbr0* and *cloudbr1*, but you do have to make sure they are available on each hypervisor.

The most important factor is that you keep the configuration consistent on all your hypervisors.

8.1.8.1. Preparing

To make sure that the native bridge module will not interfere with openvswitch the bridge module should be added to the blacklist. See the modprobe documentation for your distribution on where to find the blacklist. Make sure the module is not loaded either by rebooting or executing rmmod bridge before executing next steps.

The network configurations below depend on the ifup-ovs and ifdown-ovs scripts which are part of the openvswitch installation. They should be installed in /etc/sysconfig/network-scripts/

8.1.8.2. Network example

There are many ways to configure your network. In the Basic networking mode you should have two (V)LAN's, one for your private network and one for the public network.

We assume that the hypervisor has one NIC (eth0) with three tagged VLAN's:

1. VLAN 100 for management of the hypervisor
2. VLAN 200 for public network of the instances (cloudbr0)
3. VLAN 300 for private network of the instances (cloudbr1)

On VLAN 100 we give the Hypervisor the IP-Address 192.168.42.11/24 with the gateway 192.168.42.1

注記

The Hypervisor and Management server don't have to be in the same subnet!

8.1.8.3. Configuring the network bridges

It depends on the distribution you are using how to configure these, below you'll find examples for RHEL/CentOS.

注記

The goal is to have three bridges called 'mgmt0', 'cloudbr0' and 'cloudbr1' after this section. This should be used as a guideline only. The exact configuration will depend on your network layout.

8.1.8.3.1. Configure OpenVswitch

The network interfaces using OpenVswitch are created using the ovs-vsctl command. This command will configure the interfaces and persist them to the OpenVswitch database.

First we create a main bridge connected to the eth0 interface. Next we create three fake bridges, each connected to a specific vlan tag.

```
# ovs-vsctl add-br cloudbr
# ovs-vsctl add-port cloudbr eth0
# ovs-vsctl set port cloudbr trunks=100,200,300
# ovs-vsctl add-br mgmt0 cloudbr 100
# ovs-vsctl add-br cloudbr0 cloudbr 200
# ovs-vsctl add-br cloudbr1 cloudbr 300
```

8.1.8.3.2. Configure in RHEL or CentOS

The required packages were installed when openvswitch and libvirt were installed, we can proceed to configuring the network.

First we configure eth0

```
vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Make sure it looks similar to:

```
DEVICE=eth0
HWADDR=00:04:xx:xx:xx:xx
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=Ethernet
```

We have to configure the base bridge with the trunk.

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr
```

```
DEVICE=cloudbr
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
DEVICETYPE=ovs
TYPE=OVSBridge
```

We now have to configure the three VLAN bridges:

```
vi /etc/sysconfig/network-scripts/ifcfg-mgmt0
```

```
DEVICE=mgmt0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=static
DEVICETYPE=ovs
TYPE=OVSBridge
IPADDR=192.168.42.11
GATEWAY=192.168.42.1
NETMASK=255.255.255.0
```

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr0
```

```
DEVICE=cloudbr0
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
DEVICETYPE=ovs
TYPE=OVSBridge
```

```
vi /etc/sysconfig/network-scripts/ifcfg-cloudbr1
```

```
DEVICE=cloudbr1
ONBOOT=yes
HOTPLUG=no
BOOTPROTO=none
TYPE=OVSBridge
DEVICETYPE=ovs
```

With this configuration you should be able to restart the network, although a reboot is recommended to see if everything works properly.

警告

Make sure you have an alternative way like IPMI or ILO to reach the machine in case you made a configuration error and the network stops functioning!

8.1.9. Configuring the firewall

The hypervisor needs to be able to communicate with other hypervisors and the management server needs to be able to reach the hypervisor.

In order to do so we have to open the following TCP ports (if you are using a firewall):

1. 22 (SSH)
2. 1798
3. 16509 (libvirt)
4. 5900 - 6100 (VNC consoles)
5. 49152 - 49216 (libvirt live migration)

It depends on the firewall you are using how to open these ports. Below you'll find examples how to open these ports in RHEL/CentOS and Ubuntu.

8.1.9.1. Open ports in RHEL/CentOS

RHEL and CentOS use iptables for firewalling the system, you can open extra ports by executing the following iptable commands:

```
$ iptables -I INPUT -p tcp -m tcp --dport 22 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 1798 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 16509 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 5900:6100 -j ACCEPT
```

```
$ iptables -I INPUT -p tcp -m tcp --dport 49152:49216 -j ACCEPT
```

These iptable settings are not persistent accross reboots, we have to save them first.

```
$ iptables-save > /etc/sysconfig/iptables
```

8.1.9.2. Open ports in Ubuntu

The default firewall under Ubuntu is UFW (Uncomplicated FireWall), which is a Python wrapper around iptables.

To open the required ports, execute the following commands:

```
$ ufw allow proto tcp from any to any port 22
```

```
$ ufw allow proto tcp from any to any port 1798
```

```
$ ufw allow proto tcp from any to any port 16509
```

```
$ ufw allow proto tcp from any to any port 5900:6100
```

```
$ ufw allow proto tcp from any to any port 49152:49216
```

注記

By default UFW is not enabled on Ubuntu. Executing these commands with the firewall disabled does not enable the firewall.

8.1.10. CloudStack へのホスト追加

これでホストをクラスターに追加する準備ができました。詳細に関しては後の項で説明されますのでこちら「ホストの追加」を参照してください。ホストを追加する前に上記ドキュメントを参照することを推奨します。

8.2. CloudStackのためのCitrix XenServerのインストール

If you want to use the Citrix XenServer hypervisor to run guest virtual machines, install XenServer 6.1 or XenServer 6.0.2 on the host(s) in your cloud. For an initial installation, follow the steps below. If you have previously installed XenServer and want to upgrade to another version, see 「XenServer バージョンのアップグレード」.

8.2.1. XenServerホストのシステム要件

- ホストは 次に示す互換性のいづれかを認定されている必要があります。 http://hcl.xensource.com の『Citrix Hardware Compatibility Guide』を参照してください。
  - XenServer 5.6 SP2
  - XenServer 6.0
  - XenServer 6.0.2
- 前にインストールしたホストを再使用する場合は、Citrix XenServer を再インストールする必要があります。
- ハードウェア仮想マシン(Intel-VTまたはAMD-Vが有効であること)をサポート する必要があります。
- ハイパーバイザーの製造元が提供するすべての Hotfix を適用 したことを確認します。ハイパーバイザーの製造元のサポートチャネルを通じてパッチのリリース状況を確認し、パッチがリリースされたらできるだけ早く適用します。ハイパーバイザーの必須パッチについて CloudStack が自動的に通知することはありません。ホストにハイパーバイザーの最新パッチを適用する ことは非常に重要です。最新パッチが適用されていないシステムは、おそらくハイパーバイザーの製造元からサポートを受けられません。
- クラスター内にあるホストは全て同スペックでなければいけません。CPU の種類や数、機能フラグが同じでなければいけません。
- ハードウェア仮想マシン(Intel-VTまたはAMD-VがBIOSで有効であること)をサポート する必要があります。
- 64-bit x86 CPU(多くのコアを用意することでパフォーマンスの向上が見込まれます)
- 完全仮想化のサポートが必要。
- 4GBのメモリ
- 36 GBのローカルディスク
- 最少1つ以上のNIC
- 静的IPアドレス
- CloudStack が展開された際、ハイパーバイザーホストに既に動作しているVMが存在していない。

警告

最新の Hotfix を適用しないと、データの破損や仮想マシンの喪失が生じる可能性があります。

最新の Hotfix を適用しないと、データの破損や仮想マシンの喪失が生じる可能性があります。

8.2.2. XenServerのインストール手順

1. Citrix 社の Web サイト(https://www.citrix.com/English/ss/downloads/)から あなたの CloudStack のバージョンに合った XenServer をダウンロードし、『Citrix XenServer インストールガイド』に従ってインス トールします。

Finding Older XenServer Releases

You can download the current release of XenServer through the "Free Trials" page, but if you wish to download older versions of XenServer, you will need a Citrix account and will have to browse through the download archives.

2. インストール後、次の手順に従い設定を行います。

必須	オプション
「XenServer ドメイン0のメモリ設定」	「CloudStack XenServer Support Pakcage(CSP)のインストール」
「ユーザー名とパスワード」	iSCSIやローカルディスク、NFSを利用しない場合SRをセットアップします。詳細は「XenServer 用のプライマリストレージのセットアップ」を参照してください。
「時刻同期」	「XenServer の iSCSI マルチパスのセットアップ(オプション)」
「ライセンスの取得と展開」	「XenServer の物理ネットワーク設定」

8.2.3. XenServer ドメイン0のメモリ設定

XenServer の dom0 へのメモリ割り当てを増やすために、dom0 の設定を構成します。これにより、XenServer でより多くの仮想マシンを制御できるようになります。XenServer の dom0 に 2940MB の RAM を割り当てることをお勧めします。この方法について詳しくは、http://support.citrix.com/article/CTX126531 を参照してください。 このアーティクルで言及されているのは XenServer 5.6 ですが、同じことが XenServer 6.0 にも当てはまります。

8.2.4. ユーザー名とパスワード

クラスター内のすべての XenServer に、CloudStack に構成されたものと同じユーザー名およびパスワードが必要です。

8.2.5. 時刻同期

ホストはNTPを使用する必要があります。ポッド内のすべてのホストは時刻が同期される必要があります。

1. NTPのインストール

```
# yum install ntp
```

2. 使用する NTP サーバーを参照するように、NTP 構成ファイ ルを編集します。

```
# vi /etc/ntp.conf
```

使用する NTP サーバーを参照するように、NTP 構成ファイルを編集します。例として Citrix が提供する次の NTP サーバーを使用できます。

```
server 0.xenserver.pool.ntp.org
                    server 1.xenserver.pool.ntp.org
                    server 2.xenserver.pool.ntp.org
                    server 3.xenserver.pool.ntp.org
```

3. NTPクライアントの再起動

```
# service ntpd restart
```

4. 再起動時に NTP が再び開始されることを確認します。

```
# chkconfig ntpd on
```

8.2.6. ライセンス設定

無償版の Citrix XenServer は、ライセンスなしで 30 日間使用できます。30 日の試用期間を過ぎると、無償のライセンス認証が要求されます。ここでライセンスをインストールするか、この手順を省略するかを選択できます。この手順を省略する場合は、XenServer をアクティブ化してライセンスを有効にするときに、ライセンスをインストールする必要があります。

8.2.6.1. ライセンスの取得と展開

ここでライセンスをインストールする場合は、XenCenter を使用して、ライセンスをアクティブ化して取得する必要があります。

1. XenCenter で、[ツール]>[ライセンスマネージャ]の順に選択します。
2. XenServer を選択し、[無償の XenServer のアクティブ化]を選択します。
3. ライセンスを要求します。

XenCenter または xe コマンドラインツールを使用して、ライセンスをインストールできます。

8.2.7. CloudStack XenServer Support Pakcage(CSP)のインストール

(オプション)

XenServer でセキュリティグループ、エラスティック負荷分散、およびエラスティック IP を有効にするには、CloudStack XenServer Support Package(CSP)をダウンロードしてインストールします。XenServer をインストールしたら、各 XenServer ホストで次の追加手順を実行します。

1. 次のリンクのどちらかから XenServer ホストに CSP ソフトウェアをダウンロードします。
   XenServer 6.0.2 の場合:
   http://download.cloud.com/releases/3.0.1/XS-6.0.2/xenserver-cloud-supp.tgz
   XenServer 5.6 SP2 の場合:
   http://download.cloud.com/releases/2.2.0/xenserver-cloud-supp.tgz
   XenServer 6.0 の場合:
   http://download.cloud.com/releases/3.0/xenserver-cloud-supp.tgz
2. ファイルの展開:

   ```
   # tar xf xenserver-cloud-supp.tgz
   ```
3. 以下スクリプトの実行:

   ```
   # xe-install-supplemental-pack xenserver-cloud-supp.iso
   ```
4. XenServer ホストが基本ネットワーク設定を使用するゾーンの一部である場合は、Open vSwitch(OVS)を無効にします。

   ```
   # xe-switch-network-backend  bridge
   ```
   再起動を促すメッセージが表示されたら、再起動を受け入れます。

これで、XenServer ホストを CloudStack に追加する準備ができました。

8.2.8. XenServer 用のプライマリストレージのセットアップ

CloudStack は、NFS、iSCSI、およびローカルストレージをネイティブにサポートします。これらのストレージの種類のいずれ かを使用している場合、XenServer のストレージリポジトリを作成する必要はありません。

ただし、ファイバーチャネルなどのほかの技術を介して接続されたストレージを使用する場合は、ストレージリポジトリを自分でセットアップする必要があります。これを行うには、次の手順に従います。XenServer プールにホストがある場合は、マスターノードで手順を実行します。クラスター化されていない単一の XenServer を使用する場合は、その XenServer で手順 を実行します。

1. ファイバーチャネルケーブルをクラスター内のすべてのホストとファイバーチャネルストレージホストに接続します。
2. SCSI バスを再スキャンします。次のコマンドまたは XenCenter を使用して、HBA 再スキャンを実行します。

   ```
   # scsi-rescan
   ```
3. 2 の手順を各ホスト上で繰り返します。
4. 新しいSCSIディスクを確認します。

   ```
   # ls /dev/disk/by-id/scsi-360a98000503365344e6f6177615a516b -l
   ```
   出力は次のようになりますが、具体的なファイル名は異なります(scsi-<scsiID>):

   ```
   lrwxrwxrwx 1 root root 9 Mar 16 13:47
                       /dev/disk/by-id/scsi-360a98000503365344e6f6177615a516b ->
   ../../sdc
   ```
5. 4 の手順を各ホスト上で繰り返します。
6. ストレージサーバーで次のコマンドを実行し、新しいストレージリポジトリの固有の ID を取得します。

   ```
   # uuidgen
   ```
   出力は次のようになりますが、具体的な ID は異なります。

   ```
   e6849e96-86c3-4f2c-8fcc-350cc711be3d
   ```
7. ファイバーチャネルのストレージリポジトリを作成します。名前ラベルには、生成した固有の ID を使用します。

   ```
                       # xe sr-create type=lvmohba shared=true
                       device-config:SCSIid=360a98000503365344e6f6177615a516b
                       name-label="e6849e96-86c3-4f2c-8fcc-350cc711be3d"
   ```
   このコマンドは、次の例のようにストレージリポジトリの固有の ID を戻します(実際の ID は異なります)。

   ```
   7a143820-e893-6c6a-236e-472da6ee66bf
   ```
8. ストレージリポジトリについて人間が読める説明を作成するには、次のコマンドを使用します。UUID には、前のコマ ンドで戻されたストレージリポジトリ ID を使用します。名前の説明には、好みに合わせてわかりやすいテキストを設 定します。

   ```
   # xe sr-param-set uuid=7a143820-e893-6c6a-236e-472da6ee66bf name-description="Fiber
   Channel storage repository"
   ```
   このストレージを後で CloudStack に追加するときに必要な値を控えておきます(「プライマリストレージの追加」を参照)。[プライマリストレージの追加]ダイアログボックスの[プロトコル]ボックスの一覧で、[事前セットアップ]を選択しま す。[ストレージレポジトリ名前ラベル]ボックスには、前に設定した名前ラベルを入力します(この例では、 e6849e96-86c3-4f2c-8fcc-350cc711be3d)。
9. (オプション)ファイバーチャネル SAN でマルチパス I/O を有効にする場合は、SAN の製造元が提供するドキュメン

9. (オプション)ファイバーチャネル SAN でマルチパス I/O を有効にする場合は、SAN の製造元が提供するドキュメントを参照してください。

8.2.9. XenServer の iSCSI マルチパスのセットアップ(オプション)

Citrix XenServer でストレージリポジトリをセットアップするとき、マルチパス I/O を有効にできます。マルチパス I/O を使用すると、冗長な物理コンポーネントを使用してサーバーと SAN の接続の信頼性を高めることができます。マルチパスを有効にするには、Citrix サーバーでサポートされる SAN ソリューションを使用し、Citrix ドキュメントに記載されている手順に従います。基本情報については、次のリンクを参照してください。

- http://support.citrix.com/article/CTX118791
- http://support.citrix.com/article/CTX125403

マルチパスを使用した Citrix リポジトリのセットアップについて、SAN の製造元に助言を求めることもできます。

このストレージを後で CloudStack に追加するときに必要な値を控えておきます(「プライマリストレージの追加」を参照)。[プライマリストレージの追加]ダイアログボックスの[プロトコル]ボックスの一覧で、[事前セットアップ]を選択します。[ストレージレポジトリ名前ラベル]ボックスには、ストレージリポジトリの作成に使用した名前と同じものを入力します。

問題が発生した場合は、SAN の製造元のサポート部門に問い合わせてください。問題が解決できない場合は、「サポートへの問い合わせ」を参照してください。

8.2.10. XenServer の物理ネットワーク設定

XenServer をインストールした後で、追加のネットワーク構成が必要な場合があります。この時点で、ホストの NIC の種類と 各 NIC が伝送するトラフィックについて、計画済みである必要があります。NIC は、計画に合わせて配線する必要があります。

NIC ボンディングを使用する場合は、クラスター内のすべてのホスト上の NIC を完全に同じ配線にする必要があります。例えば、eth0 がクラスター内のあるホスト上のプライベートボンドにある場合、eth0 はクラスター内のすべてのホストでプライベートボンドに存在する必要があります。

管理ネットワークインターフェイス用に割り当てる IP アドレスは、静的である必要があります。この IP アドレスはホスト自体で設定したり、静的 DHCP 経由で取得したりできます。

CloudStack では、XenServer ホストでさまざまな NIC またはボンドを使用できるように、各種のネットワークトラフィックが構成されます。XenServer のネットワーク名ラベルを使用して、このプロセスを制御し、管理サーバーに情報を提供できます。 CloudStack で名前ラベルを物理インターフェイスまたはボンドに付けて構成します。簡単な構成の場合は、名前ラベルは必要ありません。

8.2.10.1. XenServer の専用 NIC を使用したパブリックネットワークの構成(オプション)

CloudStack では、パブリックネットワークに 2 つ目の NIC(または NIC のボンドペア、「XenServer の NIC ボンディング(オプション)」を参照)を使用できます。ボンディングを使用しない場合、パブリックネットワークには任意の NIC で、 そしてクラスター内のホストの複数の NIC で接続できます。たとえば、パブリックネットワークにノード A では eth0 で、ノード B では eth1 で接続できます。ただし、XenServer のパブリックネットワーク名ラベルは、すべてのホスト間で同一でなければ なりません。次の例では、ネットワークラベルを「cloud-public」とします。管理サーバーをインストールして起動した後、選択したネットワーク名ラベル(「cloud-public」)を管理サーバーで構成する必要があります。詳しくは、「管理サーバーのインストール」を参照してください。

ボンドした 2 つの NIC を使用してパブリックネットワークを作成する場合は、「XenServer の NIC ボンディング(オプション)」を参照してください。

単一の専用 NIC を使用してパブリックネットワークアクセスを提供する場合は、この手順に従って CloudStack に追加する各新規ホストを設定してから、ホストを追加します。

1. xe network-list を実行し、パブリックネットワークを検索します。これは通常、パブリックである NIC に接続されています。ネットワークが見つかったら、その UUID を控えておきます。これを< UUID-Public>とします。
2. 次のコマンドを実行します。

```
# xe network-param-set name-label=cloud-public uuid=<UUID-Public>
```

8.2.10.2. XenServer の複数のゲストネットワークの構成(オプション)

CloudStack は、XenServer ハイパーバイザーを使用する複数のゲストネットワークの使用をサポートします。各ネットワー クには XenServer の名前ラベルを割り当てます。たとえば、「cloud-guest」と「cloud-guest2」のラベルを持つ 2 つのネットワークがあるとします。管理サーバーをインストールして起動した後に、ネットワークを追加して、CloudStack がネットワー クを認識するようにこれらのラベルを使用する必要があります。

この手順に従って各新規ホストを設定してから、CloudStack にホストを追加します。

1. xe network-list を実行し、いずれかのゲストネットワークを検索します。ネットワークが見つかった場合は、そ の UUID を控えておきます。これを<UUID-Guest>とします。
2. 次のコマンドを実行します。名前ラベルと UUID は実際の値で置き換えます。

```
# xe network-param-set name-label=<cloud-guestN> uuid=<UUID-Guest>
```

3. 追加する各ゲストネットワークに対して毎回異なる名前ラベルと UUID を使用して、この手順を繰り返します。

8.2.10.3. XenServer 用の個別のストレージネットワーク(オプション)

個別のストレージネットワークを任意にセットアップできます。この設定をまずホストで行ってから、次のボンディング手順を 実行する必要があります。使用できる 1 つまたは 2 つの NIC を使用して実行できます。前に説明したとおり、NIC が 2 つある場合はボンディングを行えます。別個のストレージネットワークのセットアップは、管理者の責任において行います。

ストレージネットワークに、ほかのネットワークとは異なる名前ラベルを指定します。

プライマリストレージデバイスの IP アドレスに ping で通信できるインターフェイスでのみ、個別のストレージネットワークは正常に動作します。たとえば、eth0 が管理ネットワークの NIC である場合は、ping -I eth0 < プライマリストレージデバイスの IP アドレス > は失敗します。すべての展開環境で、セカンダリストレージデバイスは管理ネットワークの NIC または ボンドから ping で通信できる必要があります。セカンダリストレージデバイスがストレージネットワークに配置されている場合は、ホスト上のストレージネットワークの NIC またはボンドを経由して ping で通信できる必要もあります。

個別のストレージネットワークを 2 つセットアップすることもできます。たとえば、iSCSI マルチパスを実装する場合は、ボンドしていない 2 つの NIC をマルチパス専用にします。2 つのネットワークのどちらにも、一意の名前ラベルが必要です。

ボンドしない場合は、管理者はすべてのホスト(マスターとスレーブ)上に個別のストレージネットワークをセットアップし、名前ラベルを割り当てる必要があります。

次に、172.16.0.0/24 上のストレージネットワークにアクセスするように、eth5 をセットアップする例を示します。

```
                # xe pif-list host-name-label='hostname' device=eth5
                uuid(RO): ab0d3dd4-5744-8fae-9693-a022c7a3471d
                device ( RO): eth5
                #xe pif-reconfigure-ip DNS=172.16.3.3 gateway=172.16.0.1 IP=172.16.0.55
mode=static netmask=255.255.255.0 uuid=ab0d3dd4-5744-8fae-9693-a022c7a3471d
```

8.2.10.4. XenServer の NIC ボンディング(オプション)

XenServer では、SLB(Source Level Balancing)NIC ボンディングがサポートされます。パブリック、プライベート、およびゲストのトラフィック、またはこれらを組み合わせたトラフィックを伝送するために 2 つの NIC をボンドできます。個別のストレー ジネットワークも同じようにできます。次に、サポートされる構成例をいくつか挙げます。

- プライベートに NIC を 2 つ、パブリックに NIC を 2 つ、ストレージに NIC を 2 つ
- プライベートに NIC を 2 つ、パブリックに NIC を 1 つ、ストレージは管理ネットワークの NIC を使用
- プライベートに NIC を 2 つ、パブリックに NIC を 2 つ、ストレージは管理ネットワークの NIC を使用
- プライベート、パブリック、およびストレージに NIC を 1 つ

NIC ボンディングはすべてオプションです。

XenServer では、クラスター内のすべてのノードに同じネットワーク配線と同じボンドが実装されることを想定します。マスターになるのは、展開時に最初にクラスターに追加したホストです。それ以降にクラスターに追加するホストはすべてスレーブホストです。マスターにボンドが存在するということは、後でクラスターにホストが追加されたことを想定させます。ボンドをセットアップする手順はマスターとスレーブで異なります。それぞれについて次に説明します。これには次のような重要な意味合いがあります。

- ボンドは最初にクラスターに追加したホストで設定する必要があります。次に、後述する xe コマンドを使用して、クラスターに追加した 2 番目以降のホストで同じボンドを設定する必要があります。
- クラスター内のスレーブホストは、マスターと完全に同じに配線する必要があります。たとえば、eth0 がマスター上のプライベートボンドにある場合、追加するスレーブホストの管理ネットワークに eth0 が存在する必要があります。

8.2.10.4.1. 管理ネットワークのボンディング

管理者は、CloudStack にホストを追加する前に、管理ネットワークの NIC をボンドする必要があります。

8.2.10.4.2. クラスターの最初のホストでのプライベートボンドの作成

次の手順に従って、XenServer でボンドを作成します。この手順は、クラスターの最初のホストのみで実行する必要があります。この例では、2 つの物理 NIC(eth0 および eth1)をボンドした cloud-private ネットワークを作成します。

1. ボンドする物理 NIC を検索します。

   ```
   # xe pif-list host-name-label='hostname' device=eth0
                               # xe pif-list host-name-label='hostname' device=eth1
   ```

   これらのコマンドにより、eth0 および eth1 の NIC とその UUID が表示されます。デバイス ID は実際に設定するデバイスのもので置き換えます。上のコマンドで返された UUID を slave1-UUID および slave2-UUID とします。
2. ボンド用の新しいネットワークを作成します。たとえば、新しいネットワークの名前を「cloud-private」とします。

   このラベルは重要です。CloudStack は管理者が構成した名前を使用してネットワークを検索します。管理ネット\nワークについてクラウド内のすべてのホストで同じ名前ラベルを使用する必要があります。

   ```
   # xe network-create name-label=cloud-private
                               # xe bond-create network-uuid=[uuid of cloud-private
   created above]
                               pif-uuids=[slave1-uuid],[slave2-uuid]
   ```

これで、管理ネットワークとして CloudStack で認識できるボンドペアを用意できました。

8.2.10.4.3. パブリックネットワークのボンディング

ボンディングは、個別のパブリックネットワークで実装できます。パブリックネットワークでボンディングを使用し、管理ネットワークから分離する場合は、管理者はパブリックネットワーク用のボンドを作成する必要があります。

8.2.10.4.4. クラスターの最初のホストでのパブリックボンドの作成

この手順は、クラスターの最初のホストのみで実行する必要があります。この例では、2 つの物理 NIC(eth2 および eth3)をボンドした cloud-public ネットワークを作成します。

1. ボンドする物理 NIC を検索します。

   ```
   # xe pif-list host-name-label='hostname' device=eth2
   ```

```
#xe pif-list host-name-label='hostname' device=eth2
                              # xe pif-list host-name-label='hostname' device=eth3
```

これらのコマンドにより、eth2 および eth3 の NIC とその UUID が表示されます。デバイス ID は実際に設定するデバイスのもので置き換えます。上のコマンドで返された UUID を slave1-UUID および slave2-UUID とします。

2. ボンド用の新しいネットワークを作成します。たとえば、新しいネットワークの名前を「cloud-public」とします。**このラベルは重要です。CloudStack は管理者が構成した名前を使用してネットワークを検索します。パブリックネッ\nトワークについてクラウド内のすべてのホストで同じ名前ラベルを使用する必要があります。**

```
# xe network-create name-label=cloud-public
                              # xe bond-create network-uuid=[uuid of cloud-public
created above]
                              pif-uuids=[slave1-uuid],[slave2-uuid]
```

これで、パブリックネットワークとして CloudStack で認識できるボンドペアを用意できました。

8.2.10.4.5. クラスターへのホストの追加

必要に応じてマスターにボンドを設定した場合は、スレーブホストを追加する必要があります。クラスターに追加するすべてのホストで次のコマンドを実行します。これで、ホストが単一の XenServer プールのマスターに加わります。

```
# xe pool-join master-address=[master IP] master-username=root
                    master-password=[your password]
```

8.2.10.4.6. クラスター全体でのボンドセットアップの完了

プールにすべてのホストを追加したら、cloud-setup-bond スクリプトを実行します。このスクリプトにより、クラスター内のすべてのホストのボンドの構成とセットアップを完了します。

1. Copy the script from the Management Server in /usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-setup-bonding.sh to the master host and ensure it is executable.
2. 次のスクリプトを実行します。

```
# ./cloud-setup-bonding.sh
```

これで、ボンドがセットアップされ、クラスター全体で適切に構成されました。

8.2.11. XenServer バージョンのアップグレード

ここでは、CloudStack ホスト上の XenServer ソフトウェアをアップグレードする方法について説明します。実際のアップグレードは XenServer のドキュメントで説明されていますが、アップグレードの前後に追加して実行する必要がある手順がいくつかあります。

注記

ハードウェアが新しいバージョンの XenServer との互換性を認定されていることを確認してください。

XenServer をアップグレードするには

1. データベースをアップグレードします。管理サーバーノードで次の手順を実行します。
    a. データベースをバックアップします。

    ```
    # mysqldump --user=root --databases cloud > cloud.backup.sql
                                  # mysqldump --user=root --databases cloud_usage >
    cloud_usage.backup.sql
    ```

    b. ここで、アップグレード対象のホスト上で動作している仮想マシンのOSタイプを変更する必要があるかもしれません。
        - もし、XenServer 5.6 GA から XenServer 5.6 SP2 、または仮想マシンのOSタイプをCentOS 5.5 (32-bit)、Oracle Enterprise Linux 5.5 (32-bit) もしくは Red Hat Enterprise Linux 5.5 (32-bit) 、からその他の Linux (32-bit) にアップグレードする場合一度それらを同一のOSタイプからその他のLinux (64-bit) に変換する必要があります。
        - もし、XenServer 5.6 SP2 から XenServer 6.0.2 、または仮想マシンのOSタイプをCentOS 5.6 (32-bit)、CentOS 5.7 (32-bit)、Oracle Enterprise Linux 5.6 (32-bit)、Oracle Enterprise Linux 5.7 (32-bit)、Red Hat Enterprise Linux 5.6 (32-bit) もしくは Red Hat Enterprise Linux 5.7 (32-bit) 、からその他のLinux (32-bit) にアップグレードする場合一度それらを同一のOSタイプからその他のLinux (64-bit) に変換する必要があります。
        - もし、上記の通り XenServer を 5.6 から 6.0.2 にアップグレードした場合

    c. 管理サーバーと使用状況サーバーを再起動します。これはクラスター毎に一度だけ実施します。

    ```
    # service cloudstack-management start
                                  # service cloudstack-usage start
    ```

2. CloudStack から XenServer クラスターの接続を外します。
    a. root として CloudStack UI からログインします。
    b. XenServer クラスターに移動し、[Actions]、[Unmanage]の順にクリックします。
    c. クラスターの状態が[Unmanaged]になるまで監視します。
3. クラスター上のホストにログインし、VLAN をクリーンするコマンドを実行します。

```
# . /opt/xensource/bin/cloud-clean-vlan.sh
```

4. ホストへログインしたまま、アップグレードのためのスクリプトを実行します。

```
# /opt/xensource/bin/cloud-prepare-upgrade.sh
```

トラブルシューティング : もし「CDを取り除けません」といったエラーに遭遇した場合は、仮想マシンにログインし CD を umount した後、スクリプトを続行してください。

5. クラスター上の全てのホストの XenServer ソフトウェアをアップグレードし、最初のマスターとなるホストをアップグレードしてください。
    a. 他のホストの全ての仮想マシンをライブマイグレーションするには、Administrator's Guideの「Instructions for live migration」を参照してください。
    トラブルシューティング : 仮想マシンの移動時、以下のようなエラーメッセージを見るかもしれません。

    ```
    [root@xenserver-qa-2-49-4 ~]# xe vm-migrate live=true host=xenserver-qa-2-49-5
    vm=i-2-8-VM
                                You attempted an operation on a VM which requires
    PV drivers to be installed but the drivers were not detected.
                                vm: b6cf79c8-02ee-050b-922f-49583d9f1a14 (i-2-8-VM)
    ```

    この問題を解決するため、次を実行します。

    ```
    # /opt/xensource/bin/make_migratable.sh  b6cf79c8-02ee-050b-922f-49583d9f1a14
    ```

    b. ホストを再起動します。
    c. XenServer のドキュメントを参考に XenServer を新しいバージョンにアップグレードします。
    d. アップグレードの完了後、次に示される場所に示されるファイル群を管理サーバーからコピーします。

管理サーバーの以下のファイルを	XenServer ホストにコピーします。
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/xenserver60/NFSSR.py	/opt/xensource/sm/NFSSR.py
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/setupxenserver.sh	/opt/xensource/bin/setupxenserver.sh
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/make_migratable.sh	/opt/xensource/bin/make_migratable.sh
/usr/share/cloudstack-common/scripts/vm/hypervisor/xenserver/cloud-clean-vlan.sh	/opt/xensource/bin/cloud-clean-vlan.sh

    e. 以下スクリプトの実行:

    ```
    # /opt/xensource/bin/setupxenserver.sh
    ```

    トラブルシューティング: 以下のエラーメッセージを確認した場合、安全にそれを無効化することができます。

    ```
    mv: cannot stat `/etc/cron.daily/logrotate': No such file or directory
    ```

    f. ストレージリポジトリ(物理ブロックデバイス)を XenServer ホストに接続します。

    ```
    # for pbd in `xe pbd-list currently-attached=false| grep ^uuid | awk '{print
    $NF}'`; do xe pbd-plug uuid=$pbd ; done
    ```

    注意: XenServer プールにホストを追加した際は全ての仮想マシンを別ホストに移行させ、このホストを XenServer プールから取り外す必要があります。
6. これらの手順をクラスター内の全てのホストを同じバージョンの XenServer にアップグレードするため実施します。
7. XenServer クラスター内の 1 台のホストで次のコマンドを実行し、ホストタグをクリーンアップします。

    ```
    # for host in $(xe host-list | grep ^uuid | awk '{print $NF}') ; do xe host-param-
    clear uuid=$host param-name=tags; done;
    ```

    注記

    コマンドをコピーして実行するときは、単一の行として貼り付けたことを確認してください。 一部のドキュメントビューアーでは、コピーしたテキストに不要な改行が含まれる可能性があります。

8. XenServer クラスターを CloudStack に再接続します。
    a. root として CloudStack UI からログインします。
    b. XenServer クラスターに移動し、[Actions]、[Manage]の順 にクリックします。
    c. 状態を監視し、すべてのホストが表示されるのを確認します。
9. すべてのホストが表示されたら、クラスター内の 1 台のホストで次のコマンドを実行します。

    ```
    # /opt/xensource/bin/cloud-clean-vlan.sh
    ```

8.3. VMware vSphereのインストールと構成

VMware vSphere ハイパーバイザーを使用してゲスト仮想マシンを実行する場合は、クラウド内のホストに vSphere をインストールします。

8.3.1. vSphere ホストのシステム要件

8.3.1.1. ソフトウェア要件

- Version 4.1 または 5.0 の vSphere および vCenter
- vSphere Standard をお勧めします。ただし、vSphere ライセンスの CPU 制限を考慮する必要があることに注意してく

vSphere Standard をお勧めします。ただし、vSphere ライセンスの CPU 制限を考慮する必要があることに注意してください。http://www.vmware.com/files/jp/pdf/vsphere_pricing.pdf を参照し、VMware の販売担当者と相談してください。

vCenter Server Standard をお勧めします。

- ハイパーバイザーの製造元が提供するすべての Hotfix を適用 したことを確認します。ハイパーバイザーの製造元のサポートチャネルを通じてパッチのリリース状況を確認し、パッチがリリースされたらできるだけ早く適用します。ハイパーバイザーの 必須パッチについて CloudStack が自動的に通知することはあ りません。ホストにハイパーバイザーの最新パッチを適用することは非常に重要です。最新パッチが適用されていないシステムは、おそらくハイパーバイザーの製造元からサポートを受けられません。

全ての必要な Hotfix を適用します。

最新の Hotfix を適用しないと、データの破損や仮想マシンの喪失が生じる可能性があります。

8.3.1.2. ハードウェア要件:

- ホストは vSphere との互換性を認定されている必要があります。http://www.vmware.com/resources/compatibility/search.php の『VMware Hardware Compatibility Guide』を参照してください。
- すべてのホストは64ビットマシンで、ハードウェア仮想マシン(Intel-VTまたはAMD-Vが有効であること)をサポートする必要があります。
- 1つのクラスター内のホストは種類が同じである必要があります。つまり、CPUの種類と数が同じで、同じ機能フラグである必要があります。
- 64-bit x86 CPU(多くのコアを用意することでパフォーマンスの向上が見込まれます)。
- 完全仮想化のサポートが必要。
- 4GBのメモリ。
- 36 GBのローカルディスク
- 最少1つ以上のNIC。
- 静的IPアドレス

8.3.1.3. vCenter Server の要件:

- プロセッサ: 2 つの CPU、2.0GHz 以上の Intel または AMD x86 プロセッサ。データベースを同じマシンで実行する場合は、より高性能のプロセッサが必要です。
- メモリ: 3GB の RAM。データベースを同じマシンで実行する場合は、より多くの RAM が必要です。
- ディスクストレージ: 2GB。データベースを同じマシンで実行する場合は、より多くのストレージが必要です。
- Microsoft SQL Server 2005 Express のディスク要件。バンドルされているデータベースには、インストールアーカイブを展開するための最大 2GB のディスク領域が必要です。
- ネットワークシステム: 1Gbit または 10Gbit。

詳しくは、http://pubs.vmware.com/vsp40/wwhelp/wwhimpl/js/html/wwhelp.htm#href=install/c_vc_hw.html で\n「vCenter Server and the vSphere Client Hardware Requirements」を参照してください。

8.3.1.4. そのほかの要件:

- VMware vCenter Standard Edition 4.1 または 5.0 をインストールし、vSphere ホストの管理に使用する必要があります。
- 標準ポート 443 を使用するように vCenter を構成し、CloudStack 管理サーバーと通信できるようにする必要があります。
- 以前にインストールしたホストを再使用する場合は、VMware ESXi を再インストールする必要があります。
- CloudStack には VMware vSphere 4.1 または 5.0 が必要です。VMware vSphere 4.0 はサポートされません。
- All hosts must be 64-bit and must support HVM (Intel-VT or AMD-V enabled). All hosts within a cluster must be homogeneous. That means the CPUs must be of the same type, count, and feature flags.
- CloudStack 管理ネットワークを別個の仮想ネットワークとして構成してはいけません。CloudStack 管理ネットワークは、vCenter 管理ネットワークと同じであり、その構成を継承します。「vCenter マネージメントネットワークの設定」 を参照してください。
- CloudStack には ESXi が必要です。ESX はサポートされません。
- CloudStack で使用するすべてのリソースは、CloudStack 専用にする必要があります。CloudStack では、ESXi のインスタンスまたはストレージをほかの管理コンソールと共有できません。CloudStack で使用するストレージボリュームを、CloudStack による管理対象外の別の ESXi サーバーセットと共有しないでください。
- クラスター内のすべての対象 ESXi ハイパーバイザーを、vCenter で別個のデータセンターに配置します。
- CloudStack で管理するクラスターに仮想マシンを含めないでください。CloudStack 専用のクラスターで、管理サーバー、vCenter、およびそのほかの仮想マシンを実行しないでください。CloudStack で使用する別個のクラスターを作成し、このクラスター内に仮想マシンがないことを確認してください。
- 必要なすべての VLAN は、すべての ESXi ハイパーバイザーホストにトランク接続する必要があります。これには、 管理、ストレージ、vMotion、およびゲスト VLAN のための VLAN が含まれます。ゲスト VLAN(拡張ネットワーク設定で使用します。「ネットワークのセットアップ」を参照)は、CloudStack で管理する連続した VLAN の範囲です。

8.3.2. VMware 向けチェックリストを用意します。

インストールをより円滑に進めるために以下の情報を収集します。

- 「vCenter チェックリスト」 の情報を収集します。
- 「VMware ネットワークのチェックリスト」 の情報を収集します。

8.3.2.1. vCenter チェックリスト

vCenter に関する以下の情報が必要になります。

vCenter 要件	値	注意
vCenter ユーザー		ユーザーには管理者権限が必要となります。
vCenter ユーザーパスワード		上記ユーザーに対するパスワード。
vCenter データセンター名		データセンターの名前
vCenter クラスター名		クラスターの名前

8.3.2.2. VMware ネットワークのチェックリスト

VLAN に関して以下の情報が必要になります。

VLAN 情報	値	注意
ESXi における VLAN		存在する全ての ESXi ハイパーバイザーの VLAN
ESXi の VLAN IP 範囲		ESXi VLAN 上の IP アドレスの範囲。仮想ルーター毎のアドレスがこの範囲で利用されます。
ESXi の VLAN IP のゲートウェイ		
ESXi の VLAN ネットマスク		
管理サーバーの VLAN		インストールされている CloudStack 管理サーバーの VLAN 情報
パブリック VLAN		パブリックネットワークの VLAN
パブリック VLAN のゲートウェイ		
パブリック VLAN のネットマスク		
パブリックVLAN IPアドレスの範囲		Range of Public IP Addresses available for CloudStack use. These addresses will be used for virtual router on CloudStack to route private traffic to external networks.
顧客が使うVLANの範囲		A contiguous range of non-routable VLANs. One VLAN will be assigned for each customer.

8.3.3. vSphereのインストール手順

1. If you haven't already, you'll need to download and purchase vSphere from the VMware Website (https://www.vmware.com/trymware/index.php?p=vmware-vsphere&lp=1) and install it by following the VMware vSphere Installation Guide.
2. Following installation, perform the following configuration, which are described in the next few sections:

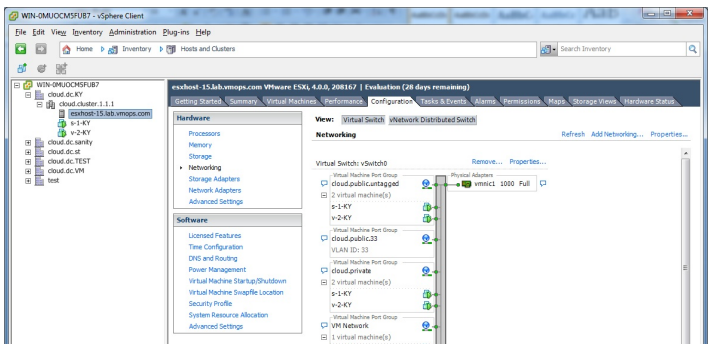
必須	オプション
ESXi ホストのSetup	ボンディングNIC
Configure host physical networking, virtual switch, vCenter Management Network, and extended port range	マルチパスストレージ
iSCSIのためのストレージを用意	
Configure clusters in vCenter and add hosts to them, or add hosts without clusters to vCenter	

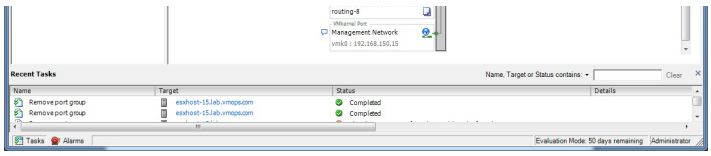
8.3.4. ESXiホストセットアップ

All ESXi hosts should enable CPU hardware virtualization support in BIOS. Please note hardware virtualization support is not enabled by default on most servers.

8.3.5. 物理ホストのネットワーク

You should have a plan for cabling the vSphere hosts. Proper network configuration is required before adding a vSphere host to CloudStack. To configure an ESXi host, you can use vClient to add it as standalone host to vCenter first. Once you see the host appearing in the vCenter inventory tree, click the host node in the inventory tree, and navigate to the Configuration tab.





In the host configuration tab, click the "Hardware/Networking" link to bring up the networking configuration page as above.

8.3.5.1. 仮想スイッチの設定

A default virtual switch vSwitch0 is created. CloudStack requires all ESXi hosts in the cloud to use the same set of virtual switch names. If you change the default virtual switch name, you will need to configure one or more CloudStack configuration variables as well.

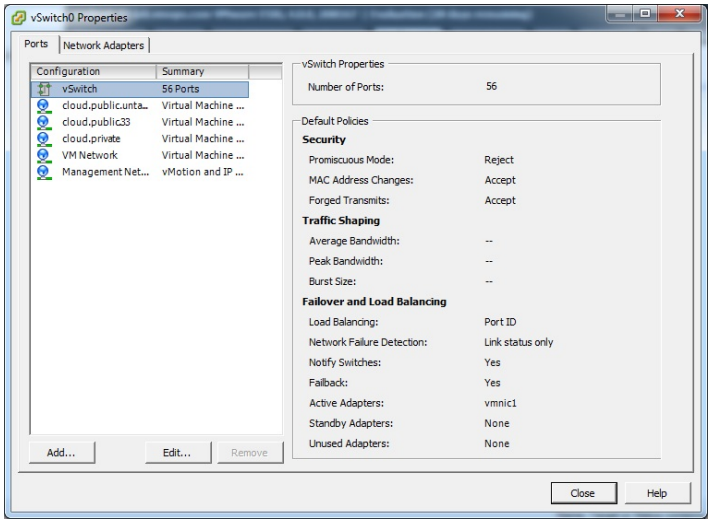
8.3.5.1.1. トラフィックの分離

CloudStack allows you to use vCenter to configure three separate networks per ESXi host. These networks are identified by the name of the vSwitch they are connected to. The allowed networks for configuration are public (for traffic to/from the public internet), guest (for guest-guest traffic), and private (for management and usually storage traffic). You can use the default virtual switch for all three, or create one or two other vSwitches for those traffic types.

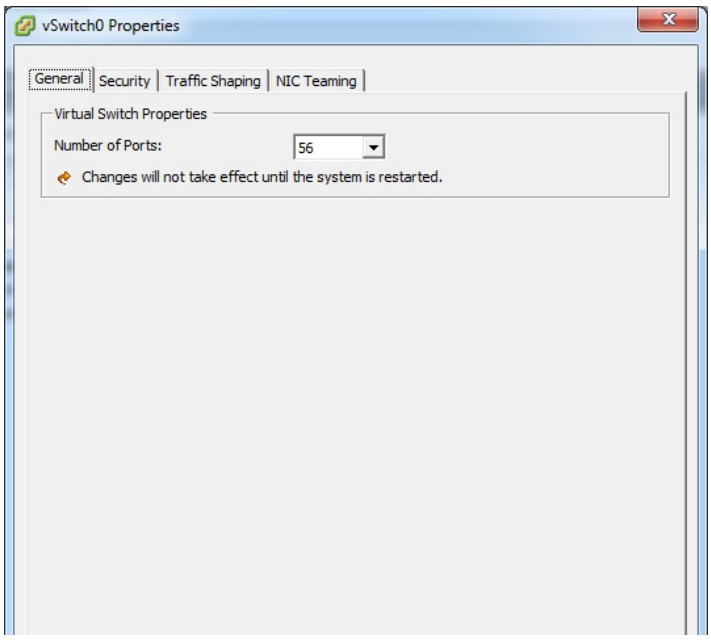
If you want to separate traffic in this way you should first create and configure vSwitches in vCenter according to the vCenter instructions. Take note of the vSwitch names you have used for each traffic type. You will configure CloudStack to use these vSwitches.

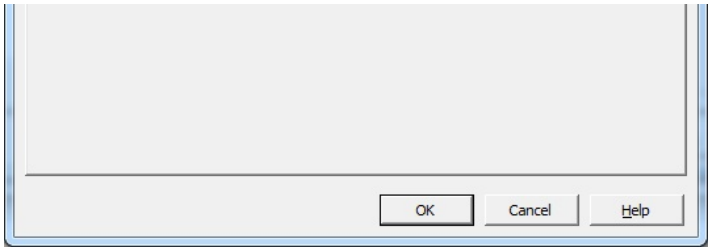
8.3.5.1.2. ポートの増加

By default a virtual switch on ESXi hosts is created with 56 ports. We recommend setting it to 4088, the maximum number of ports allowed. To do that, click the "Properties..." link for virtual switch (note this is not the Properties link for Networking).



In vSwitch properties dialog, select the vSwitch and click Edit. You should see the following dialog:

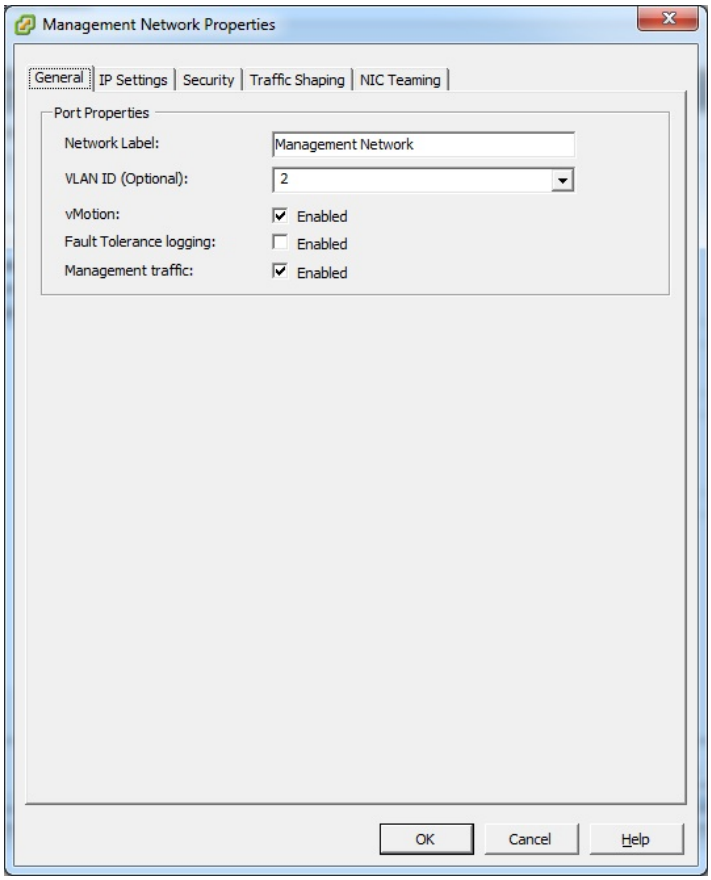




In this dialog, you can change the number of switch ports. After you've done that, ESXi hosts are required to reboot in order for the setting to take effect.

8.3.5.2. vCenter マネージメントネットワークの設定

In the vSwitch properties dialog box, you may see a vCenter management network. This same network will also be used as the CloudStack management network. CloudStack requires the vCenter management network to be configured properly. Select the management network item in the dialog, then click Edit.



下記の値が設定されたことを確認してください：

- VLAN ID set to the desired ID
- vMotion可能
- Management traffic enabled.

If the ESXi hosts have multiple VMKernel ports, and ESXi is not using the default value "Management Network" as the management network name, you must follow these guidelines to configure the management network port group so that CloudStack can find it:

- Use one label for the management network port across all ESXi hosts.
- In the CloudStack UI, go to Configuration - Global Settings and set vmware.management.portgroup to the management network label from the ESXi hosts.

8.3.5.3. Extend Port Range for CloudStack Console Proxy

(Applies only to VMware vSphere version 4.x)

You need to extend the range of firewall ports that the console proxy works with on the hosts. This is to enable the console proxy to work with VMware-based VMs. The default additional port range is 59000-60000. To extend the port range, log in to the VMware ESX service console on each host and run the following commands:

```
esxcfg-firewall -o 59000-60000,tcp,in,vncextras
esxcfg-firewall -o 59000-60000,tcp,out,vncextras
```

8.3.5.4. vSphereのNICボンディングの設定

NIC bonding on vSphere hosts may be done according to the vSphere installation guide.

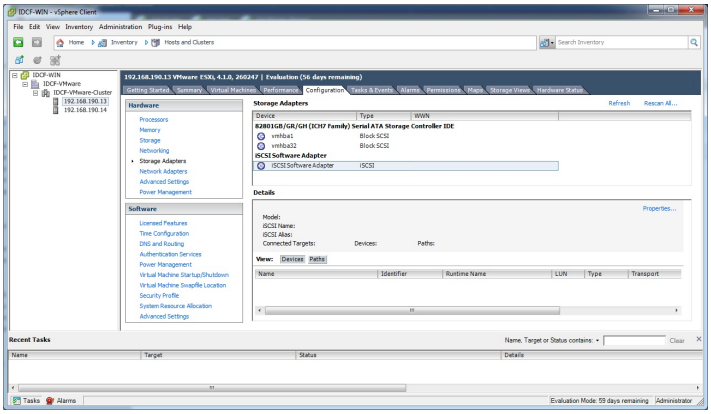
8.3.6. Storage Preparation for vSphere (iSCSI only)

Use of iSCSI requires preparatory work in vCenter. You must add an iSCSI target and create an iSCSI datastore.

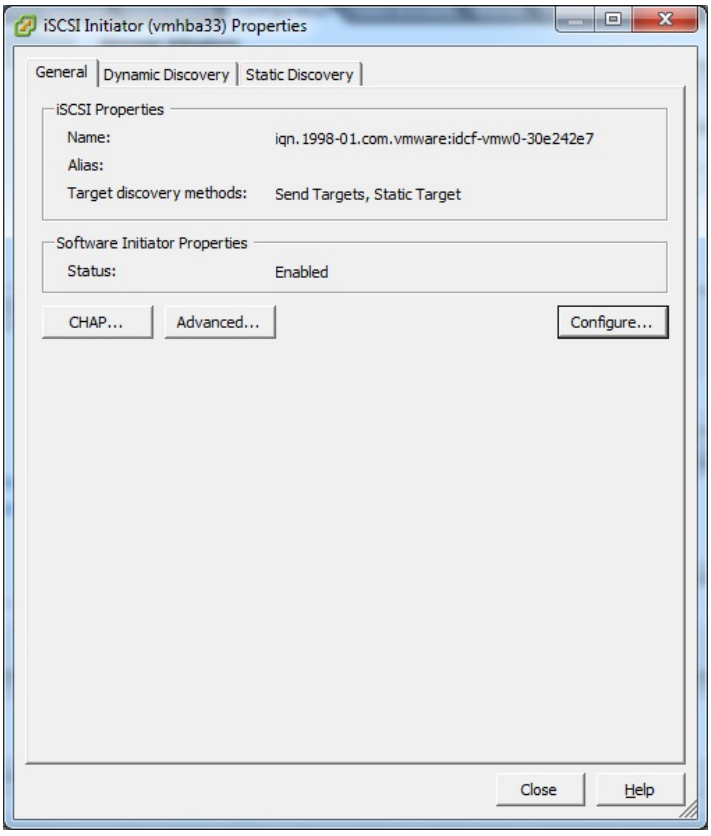
NFSを使う場合、この手順はスキップしてください。

8.3.6.1. Enable iSCSI initiator for ESXi hosts

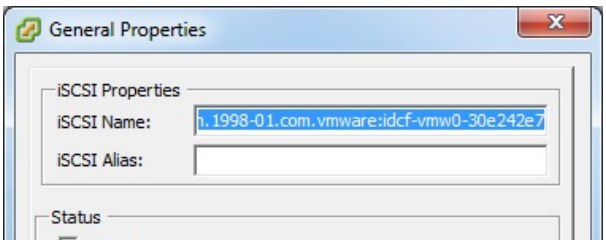
1. In vCenter, go to hosts and Clusters/Configuration, and click Storage Adapters link. You will see:

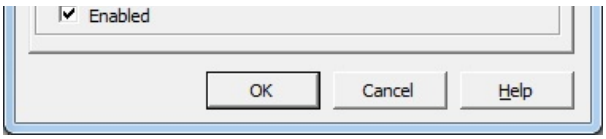


2. Select iSCSI software adapter and click Properties.



3. Click the Configure... button.

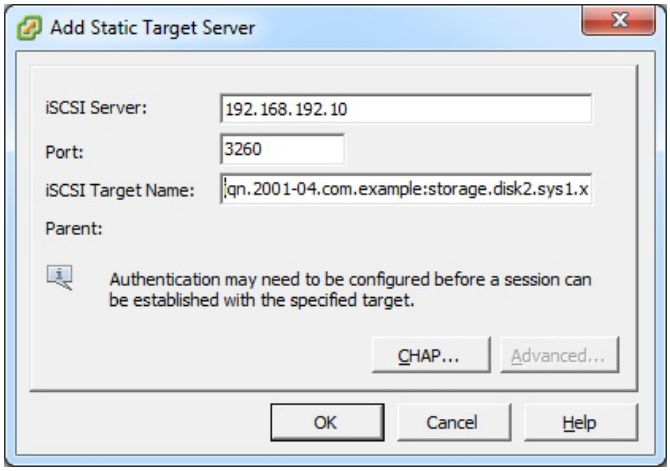




4. Check Enabled to enable the initiator.
5. 保存するために［OK］をクリックしてください。

8.3.6.2. iSCSI targetの追加

Under the properties dialog, add the iSCSI target info:



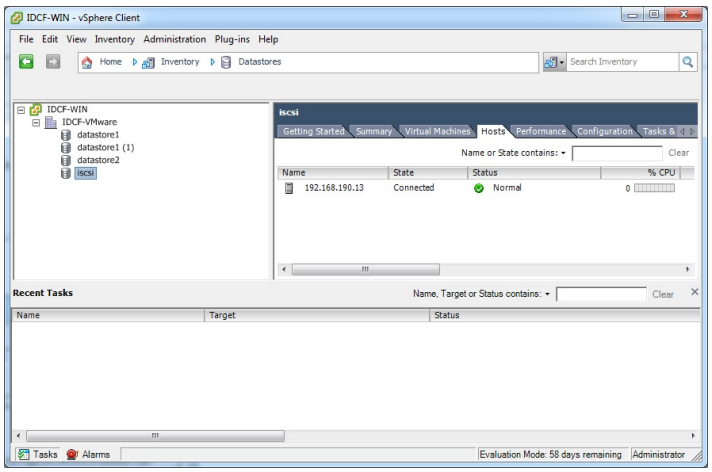
Repeat these steps for all ESXi hosts in the cluster.

8.3.6.3. iSCSIデータストアを作る

You should now create a VMFS datastore. Follow these steps to do so:

1. Select Home/Inventory/Datastores.
2. Right click on the datacenter node.
3. Choose Add Datastore... command.
4. Follow the wizard to create a iSCSI datastore.

This procedure should be done on one host in the cluster. It is not necessary to do this on all hosts.



8.3.6.4. Multipathing for vSphere (Optional)

Storage multipathing on vSphere nodes may be done according to the vSphere installation guide.

8.3.7. Add Hosts or Configure Clusters (vSphere)

Use vCenter to create a vCenter cluster and add your desired hosts to the cluster. You will later add the entire cluster to CloudStack. (see 「クラスターの追加:vSphere」).

8.3.8. Applying Hotfixes to a VMware vSphere Host

1. Disconnect the VMware vSphere cluster from CloudStack. It should remain disconnected long enough to apply the hotfix on the host.

a. root として CloudStack UI からログインします。
   See 「UIへのログイン」.
b. Navigate to the VMware cluster, click Actions, and select Unmanage.
c. [Unmanaged] が表示されるまで状態を監視します。

2. Perform the following on each of the ESXi hosts in the cluster:
   a. Move each of the ESXi hosts in the cluster to maintenance mode.
   b. Ensure that all the VMs are migrated to other hosts in that cluster.
   c. If there is only one host in that cluster, shutdown all the VMs and move the host into maintenance mode.
   d. Apply the patch on the ESXi host.
   e. 表示されたら再起動します。
   f. ホストのメンテナンスモードをキャンセルします。
3. クラスタをCloudStack に再接続します。
   a. root として CloudStack UI からログインします。
   b. Navigate to the VMware cluster, click Actions, and select Manage.
   c. Watch the status to see that all the hosts come up. It might take several minutes for the hosts to come up. Alternatively, verify the host state is properly synchronized and updated in the CloudStack database.

第9章 Additional Installation Options

The next few sections describe CloudStack features above and beyond the basic deployment options.

9.1. 使用状況測定サーバーのインストール(オプション)

管理サーバーを正しく構成したら、オプションで使用状況測定サーバーをインストールできます。使用状況測定サーバーでシステム内のイベントからデータを取得して、使用状況に基づいてアカウントに課金することができます。

複数の管理サーバーが存在する場合は、使用状況測定サーバーはそのいずれかにインストールできます。使用状況測定サーバーによって使用状況データの処理が調整されます。可用性が懸念されるサイトでは、使用状況測定サーバーを少なくとも2 台の管理サーバーにインストールする必要があります。

9.1.1. 使用状況測定サーバーのインストール要件

- 使用状況測定サーバーをインストールするときには、管理サーバーが動作している必要があります。
- 使用状況測定サーバーは管理サーバーと同じサーバーにインストールする必要があります。

9.1.2. 使用状況測定サーバーのインストール手順

1. ./install.sh を実行します。

   ```
   # ./install.sh
   ```

   インストーラーの準備が進むにつれていくつかのメッセージが表示され、その後に選択項目の一覧が表示されます。
2. 使用状況測定サーバーをインストールするため、S を選択します。

   ```
      > S
   ```

3. インストールが完了したら、次のコマンドを実行して使用状況測定サーバーを起動します。

   ```
   # service cloudstack-usage start
   ```

使用状況測定サーバーの詳細な構成について詳しくは、『管理ガイド』を参照してください。

9.2. SSL (Optional)

CloudStack provides HTTP access in its default installation. There are a number of technologies and sites which choose to implement SSL. As a result, we have left CloudStack to expose HTTP under the assumption that a site will implement its typical practice.

CloudStack uses Tomcat as its servlet container. For sites that would like CloudStack to terminate the SSL session, Tomcat's SSL access may be enabled. Tomcat SSL configuration is described at http://tomcat.apache.org/tomcat-6.0-doc/ssl-howto.html.

9.3. Database Replication (Optional)

CloudStack supports database replication from one MySQL node to another. This is achieved using standard MySQL replication. You may want to do this as insurance against MySQL server or storage loss. MySQL replication is implemented using a master/slave model. The master is the node that the Management Servers are configured to use. The slave is a standby node that receives all write operations from the master and applies them to a local, redundant copy of the database. The following steps are a guide to implementing MySQL replication.

注記

Creating a replica is not a backup solution. You should develop a backup procedure for the MySQL data that is distinct from replication.

1. Ensure that this is a fresh install with no data in the master.
2. Edit my.cnf on the master and add the following in the [mysqld] section below datadir.

   ```
   log_bin=mysql-bin
   server_id=1
   ```

   The server_id must be unique with respect to other servers. The recommended way to achieve this is to give the master an ID of 1 and each slave a sequential number greater than 1, so that the servers are numbered 1, 2, 3, etc.
3. Restart the MySQL service. On RHEL/CentOS systems, use:

   ```
   # service mysqld restart
   ```

   On Debian/Ubuntu systems, use:

   ```
   # service mysql restart
   ```
4. Create a replication account on the master and give it privileges. We will use the "cloud-repl" user with the password "password". This assumes that master and slave run on the 172.16.1.0/24 network.

   ```
   # mysql -u root
   mysql> create user 'cloud-repl'@'172.16.1.%' identified by 'password';
   mysql> grant replication slave on *.* TO 'cloud-repl'@'172.16.1.%';
   mysql> flush privileges;
   mysql> flush tables with read lock;
   ```
5. Leave the current MySQL session running.
6. In a new shell start a second MySQL session.
7. Retrieve the current position of the database.

   ```
   # mysql -u root
   mysql> show master status;
   +------------------+----------+--------------+------------------+
   | File             | Position | Binlog_Do_DB | Binlog_Ignore_DB |
   +------------------+----------+--------------+------------------+
   | mysql-bin.000001 |      412 |              |                  |
   +------------------+----------+--------------+------------------+
   ```
8. Note the file and the position that are returned by your instance.
9. Exit from this session.
10. Complete the master setup. Returning to your first session on the master, release the locks and exit MySQL.

    ```
    mysql> unlock tables;
    ```
11. Install and configure the slave. On the slave server, run the following commands.

    ```
    # yum install mysql-server
    # chkconfig mysqld on
    ```
12. Edit my.cnf and add the following lines in the [mysqld] section below datadir.

    ```
    server_id=2
    innodb_rollback_on_timeout=1
    innodb_lock_wait_timeout=600
    ```
13. Restart MySQL. Use "mysqld" on RHEL/CentOS systems:

    ```
    # service mysqld restart
    ```

    On Ubuntu/Debian systems use "mysql."

    ```
    # service mysql restart
    ```
14. Instruct the slave to connect to and replicate from the master. Replace the IP address, password, log file, and position with the values you have used in the previous steps.

    ```
    mysql> change master to
        -> master_host='172.16.1.217',
        -> master_user='cloud-repl',
        -> master_password='password',
        -> master_log_file='mysql-bin.000001',
        -> master_log_pos=412;
    ```
15. Then start replication on the slave.

    ```
    mysql> start slave;
    ```

```
mysql> start slave;
```

16. Optionally, open port 3306 on the slave as was done on the master earlier.

    This is not required for replication to work. But if you choose not to do this, you will need to do it when failover to the replica occurs.

9.3.1. Failover

This will provide for a replicated database that can be used to implement manual failover for the Management Servers. CloudStack failover from one MySQL instance to another is performed by the administrator. In the event of a database failure you should:

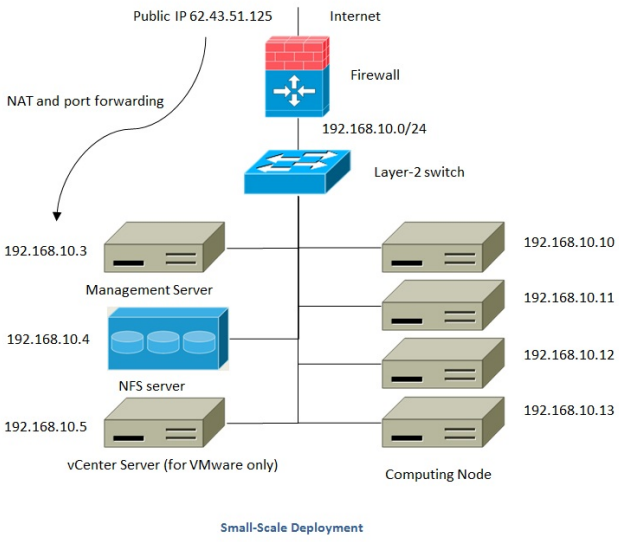
1. Stop the Management Servers (via service cloudstack-management stop).
2. Change the replica's configuration to be a master and restart it.
3. Ensure that the replica's port 3306 is open to the Management Servers.
4. Make a change so that the Management Server uses the new database. The simplest process here is to put the IP address of the new database server into each Management Server's /etc/cloudstack/management/db.properties.
5. Restart the Management Servers:

```
# service cloudstack-management start
```

第10章 展開アーキテクチャの選択

展開に使用するアーキテクチャは、展開の規模と目的によって異なります。ここでは、テストや試用展開に便利な小規模の展開や、実稼働環境への展開に適した完全に冗長な大規模セットアップなど、展開アーキテクチャの例を示します。

10.1. 小規模な展開

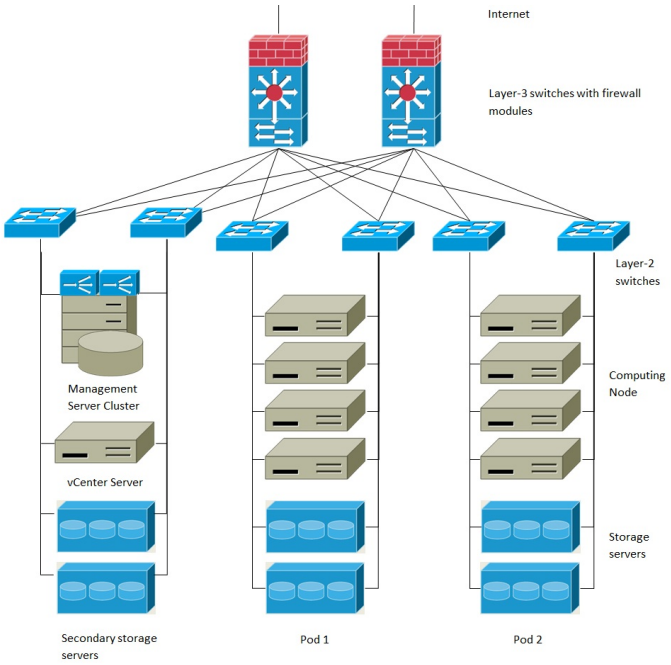


Small-Scale Deployment

この図は、CloudStack の小規模な展開のネットワークアーキテクチャを示しています。

- インターネットへの接続はファイアウォールを介して行われます。ファイアウォールは NAT モードで構成されます。ファイアウォールは、HTTP 要求および API 呼び出しをインターネットから管理サーバーに転送します。管理サー バーは管理ネットワーク上に存在します。
- レイヤー2 スイッチが、すべての物理サーバーとストレージを接続します。
- 1 台の NFS サーバーが、プライマリストレージおよびセカンダリストレージの両方として機能します。
- 管理サーバーは管理ネットワークに接続されます。

10.2. 大規模な冗長セットアップ



Large-Scale Redundant Deployment

この図は、CloudStack の大規模な展開のネットワークアーキテクチャを示しています。

- レイヤー3 スイッチレイヤーがデータセンターのコアにあります。VRRP のようなルーター冗長プロトコルを展開する必要があります。通常は、ハイエンドコアスイッチにファイアウォールモジュールも含まれます。レイヤー3 スイッチにファイアウォール機能が統合されていない場合は、別のファイアウォールアプライアンスを使用することもできます。 ファイアウォールは NAT モードで構成されます。ファイアウォールでは、次の機能が提供されます。

  HTTP 要求および API 呼び出しをインターネットから管理サーバーに転送します。管理サーバーは管理ネットワーク上に存在します。

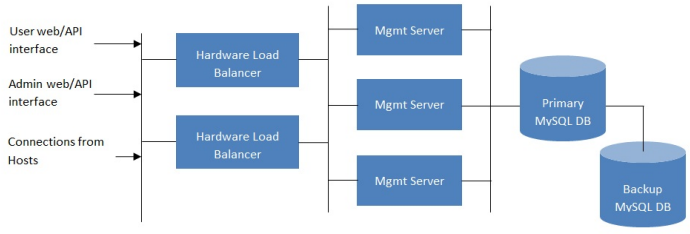
  クラウドに複数のゾーンが含まれる場合は、ファイアウォールでサイト間の VPN を許可して、異なるゾーンのサーバーが相互に直接通信できるようにする必要があります。
- レイヤー2 アクセススイッチレイヤーをポッドごとに設定します。複数のスイッチをスタックして、ポート数を増やすこと ができます。いずれの場合も、レイヤー2 スイッチの冗長ペアを展開する必要があります。
- 管理サーバークラスター(フロントエンド負荷分散装置、管理サーバーノード、MySQL データベースを含む)は、負荷分散装置のペアを通して管理ネットワークに接続されます。
- セカンダリストレージサーバーは管理ネットワークに接続されます。
- 各ポッドには、ストレージサーバーとコンピューティングサーバーが含まれます。各ストレージサーバーおよびコンピューティングサーバーには、異なるレイヤー2 アクセススイッチに接続する冗長な NIC が必要です。

10.3. 別個のストレージネットワーク

前のセクションで説明したような大規模な冗長セットアップでは、ストレージトラフィックによって管理ネットワークが過負荷状態になる可能性があります。このような展開では別個のストレージネットワークを使用できます。iSCSI のようなストレージプロトコルは、ネットワーク遅延によって大きな影響を受けます。ストレージネットワークを分離することにより、ゲストネッ トワークトラフィックの競合がストレージのパフォーマンスに影響を与えないようにすることができます。

10.4. 複数ノードの管理サーバー

CloudStack 管理サーバーは、単一の MySQL データベースに接続する 1 台以上のフロントエンドサーバーに展開します。オプションで、ペアにしたハードウェア負荷分散装置によって Web からの要求を分散することができます。リモートサイトに MySQL をレプリケートしてバックアップ管理サーバーのセットを展開し、障害回復機能を追加できます。



Multi-Node Management Server Deployment

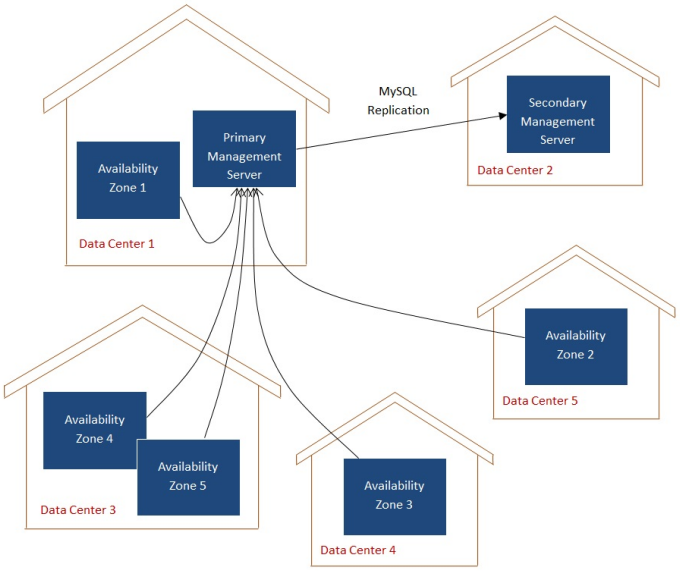
管理者は次のことを決定する必要があります。

- 負荷分散装置を使用するかどうか
- 展開する管理サーバーの数

- MySQL をレプリケートして障害回復を有効にするかどうか

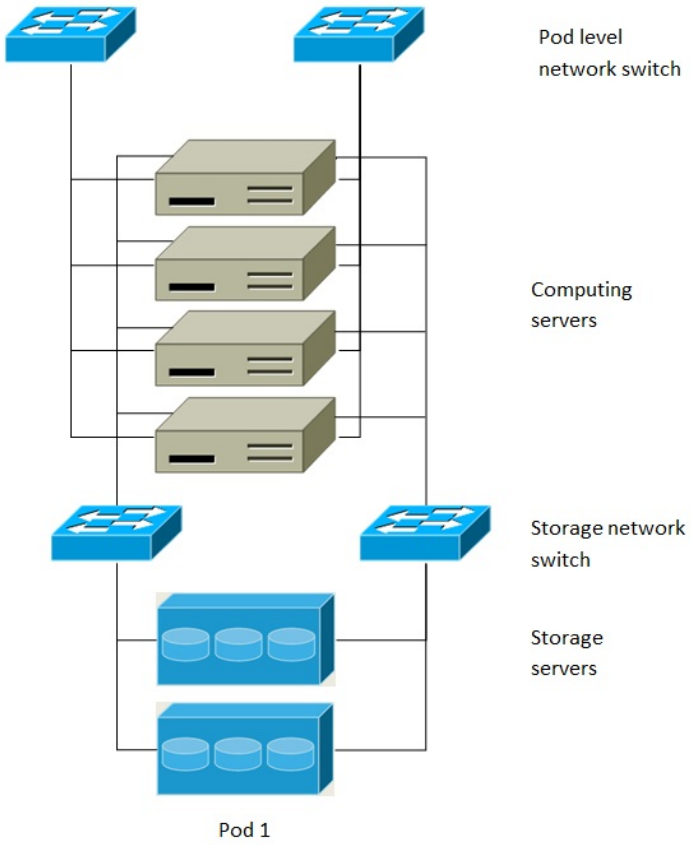
10.5. 複数サイトの展開

CloudStack は、ゾーンを使用することで複数のサイトに問題なく拡張できます。次の図は、複数サイトの展開例を示しています。



Example of a Multi-Site Deployment

データセンター1 には、プライマリ管理サーバーとゾーン 1 が含まれます。MySQL データベースは、データセンター2 のセカンダリ管理サーバーにリアルタイムでレプリケートされます。

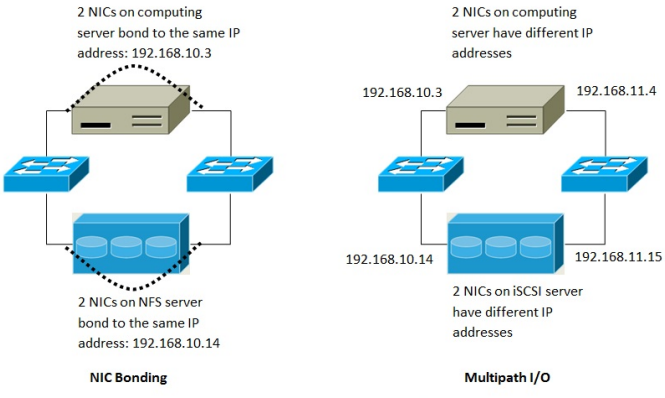


Separate Storage Network

この図は、別個のストレージネットワークのセットアップを示しています。各サーバーには 4 つの NIC があり、2 つはポッドレ ベルのネットワークスイッチに接続され、2 つはストレージネットワークスイッチに接続されています。

ストレージネットワークを構成するには、次の 2 つの方法があります。

- NFS の場合は、ボンドされた NIC と冗長なスイッチを展開できます。NFS 環境では、冗長なスイッチとボンドされた NIC により 1 つのネットワークを構成します(1 つの CIDR ブロックとデフォルトゲートウェイアドレス)。
- iSCSIの場合は、2つの独立したストレージネットワークを利用できます(2つのCIDRブロックとそれぞれに専用のデフォルトゲートウェイ)。マルチパス iSCSI クライアントは、異なるストレージネットワークの間でフェールオーバーと負荷分散を行うことができます。



NIC Bonding and Multipath I/O

この図は、NIC ボンディングとマルチパス I/O(MPIO)の違いを示しています。NIC ボンディングの構成に含まれるネットワークは 1 つだけです。MPIO には 2 つの異なるネットワークが含まれます。

第11章 Amazon Web Services Compatible Interface

11.1. Amazon Web Services Compatible Interface

CloudStack can translate Amazon Web Services (AWS) API calls to native CloudStack API calls so that users can continue using existing AWS-compatible tools. This translation service runs as a separate web application in the same tomcat server as the management server of CloudStack, listening on a different port. The Amazon Web Services (AWS) compatible interface provides the EC2 SOAP and Query APIs as well as the S3 REST API.

注記

This service was previously enabled by separate software called CloudBridge. It is now fully integrated with the CloudStack management server.

警告

The compatible interface for the EC2 Query API and the S3 API are Work In Progress. The S3 compatible API offers a way to store data on the management server file system, it is not an implementation of the S3 backend.

Limitations

- Supported only in zones that use basic networking.
- Available in fresh installations of CloudStack. Not available through upgrade of previous versions.
- Features such as Elastic IP (EIP) and Elastic Load Balancing (ELB) are only available in an infrastructure with a Citrix NetScaler device. Users accessing a Zone with a NetScaler device will need to use a NetScaler-enabled network offering (DefaultSharedNetscalerEIP and ELBNetworkOffering).

11.2. Supported API Version

- The EC2 interface complies with Amazon's WDSL version dated November 15, 2010, available at http://ec2.amazonaws.com/doc/2010-11-15/.
- The interface is compatible with the EC2 command-line tools *EC2 tools v. 1.3.6230*, which can be downloaded at http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip.

注記

Work is underway to support a more recent version of the EC2 API

11.3. EC2 と S3 の互換インターフェースの有効化

AWS API 互換のソフトウェアを CloudStack と同様にインストールします。利用するまえにまずセットアップを実施しサービスを有効化する必要があります。

1. グローバル設定で各サービスのパラメーターを true に設定します。*7章Global Configuration Parameters* を参照してください。
2. CloudStack サービスオファリングを Amazon のサービスオファリングと一致する名前で設定します。「管理者ガイド」で述べられているように CloudStack ユーザーインターフェイスから設定することができます。

   警告

   Amazon デフォルトの m1.small や利用する予定他の EC2 インスタンスタイプに対してのサービスオファリングが含まれることを確認してください。

3. 1 の手順にてグローバル構成パラメーターを変更した際、まだ再起動を実施していない場合は管理サーバーを再起動してください。

```
# service cloudstack-management restart
```

次のセクションではこらの手順を実施するための詳細について述べています。

11.3.1. サービスの有効化

EC2 や S3 の互換サービスを有効化するには構成変数である*enable.ec2.api*と*enable.s3.api*を true に設定する必要があります。同時に2つを有効化する必要はありません。有効化するには CloudStack GUI の *グローバル設定* もしくは API を利用して変更できます。

以下の画像はこれらのサービスを GUI から有効化している様子です。

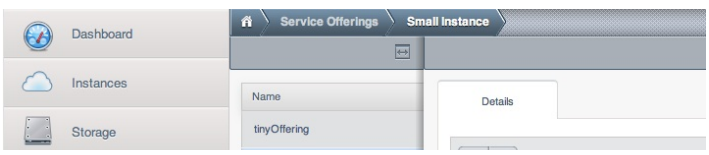
CloudStack API を利用する最も簡単な方法は認証の無いポートを利用することです。グローバル設定でポート番号を8096に設定した後、次のように*updateConfiguration*メソッドを呼び出します。\n次のURLは実際の利用例を示しています。

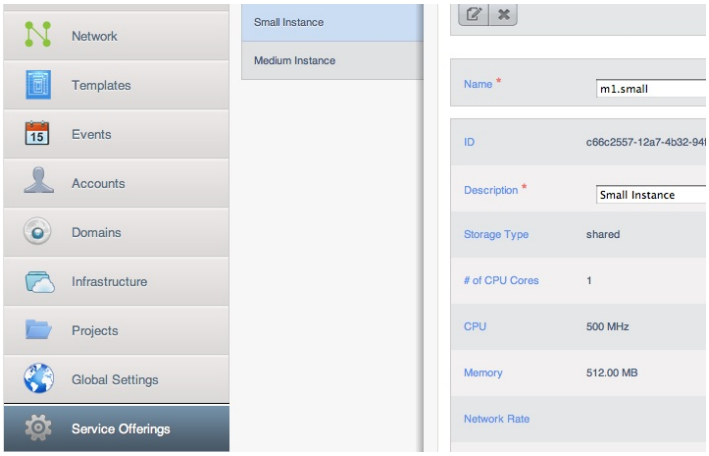
```
            http://localhost:8096/client/api?
command=updateConfiguration&name=enable.ec2.api&value=true
            http://localhost:8096/client/api?
command=updateConfiguration&name=enable.ec2.api&value=true
```

サービスを有効化した後、サーバーを再起動します。

11.3.2. EC2 互換サービスオファリングの作成

Amazon EC2 インスタンスタイプ の API 名(m1.small, m1.large など)に対応するコンピュートサービスオファリングを定義する必要があります。こちらは CloudStack GUI から設定することができます。 *サービスオファリング*から *コンピュートオファリング*を選択し、新しいコンピュートオファリングを作成するか既存のオファリングを変更します。この際 EC2 のインスタンスタイプ API 名と一致することを確認します。以下の画像はコンピュートオファリングを定義している様子です。





11.3.3. AWS API ポートの変更

注記

(オプション) AWS API はリクエストをポート番号 7080 でリッスンします。もし別のポートでリッスンしたい場合は以下の様に変更することができます。

a. Edit the files /etc/cloudstack/management/server.xml, /etc/cloudstack/management/server-nonssl.xml, and /etc/cloudstack/management/server-ssl.xml.
b. 各ファイルで <Service name="Catalina7080"> タグ配下にある <Connector executor="tomcatThreadPool-internal" port= ....< を検索します。
c. ポート番号を利用したいポート番号に変更しファイルを保存します。
d. 管理サーバーを再起動します。

CloudStack を再インストールした場合は再度サービスを有効化し必要に応じてポート番号を変更します。

11.4. AWS API User Setup

In general, users need not be aware that they are using a translation service provided by CloudStack. They only need to send AWS API calls to CloudStack's endpoint, and it will translate the calls to the native CloudStack API. Users of the Amazon EC2 compatible interface will be able to keep their existing EC2 tools and scripts and use them with their CloudStack deployment, by specifying the endpoint of the management server and using the proper user credentials. In order to do this, each user must perform the following configuration steps:

- Generate user credentials.
- Register with the service.
- For convenience, set up environment variables for the EC2 SOAP command-line tools.

11.4.1. AWS API User Registration

Each user must perform a one-time registration. The user follows these steps:

1. Obtain the following by looking in the CloudStack UI, using the API, or asking the cloud administrator:
   - The CloudStack server's publicly available DNS name or IP address
   - The user account's Access key and Secret key
2. Generate a private key and a self-signed X.509 certificate. The user substitutes their own desired storage location for /path/to/... below.

```
$ openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/path/to/private_key.pem -out /path/to/cert.pem
```

3. Register the user X.509 certificate and Access/Secret keys with the AWS compatible service. If you have the source code of CloudStack go to the awsapi-setup/setup directory and use the Python script cloudstack-aws-api-register. If you do not have the source then download the script using the following command.

```
wget -O cloudstack-aws-api-register "https://git-wip-us.apache.org/repos/asf?
p=cloudstack.git;a=blob_plain;f=awsapi-setup/setup/cloudstack-aws-api-
register;hb=4.1"
```

Then execute it, using the access and secret keys that were obtained in step 1. An example is shown below.

```
$ cloudstack-aws-api-register --apikey=User's CloudStack API key --secretkey=User's
CloudStack Secret key --cert=/path/to/cert.pem --
url=http://CloudStack.server:7080/awsapi
```

注記

A user with an existing AWS certificate could choose to use the same certificate with CloudStack, but note that the certificate would be uploaded to the CloudStack management server database.

11.4.2. AWS API Command-Line Tools Setup

To use the EC2 command-line tools, the user must perform these steps:

1. Be sure you have the right version of EC2 Tools. The supported version is available at http://s3.amazonaws.com/ec2-downloads/ec2-api-tools-1.3-62308.zip.
2. Set up the EC2 environment variables. This can be done every time you use the service or you can set them up in the proper shell profile. Replace the endpoint (i.e EC2_URL) with the proper address of your CloudStack management server and port. In a bash shell do the following.

```
$ export EC2_CERT=/path/to/cert.pem
$ export EC2_PRIVATE_KEY=/path/to/private_key.pem
$ export EC2_URL=http://localhost:7080/awsapi
$ export EC2_HOME=/path/to/EC2_tools_directory
```

11.5. Using Timeouts to Ensure AWS API Command Completion

The Amazon EC2 command-line tools have a default connection timeout. When used with CloudStack, a longer timeout might be needed for some commands. If you find that commands are not completing due to timeouts, you can specify a custom timeouts. You can add the following optional command-line parameters to any CloudStack-supported EC2 command:

`--connection-timeout TIMEOUT`	Specifies a connection timeout (in seconds). Example: `--connection-timeout 30`
`--request-timeout TIMEOUT`	Specifies a request timeout (in seconds). Example: `--request-timeout 45`

Example:

```
ec2-run-instances 2 –z us-test1 –n 1-3 --connection-timeout 120 --request-timeout 120
```

注記

The timeouts optional arguments are not specific to CloudStack.

11.6. サポートされる AWS API 呼び出し

次の Amazon EC2 コマンドは AWS API 互換インターフェースが有効になってる場合 CloudStack にてサポートされています。いくつかのコマンドは CloudStack と Amazon EC2 のバージョンによって若干の差異があり、これらの違いは別途記述されています。サポートされる各コマンドにおける SOAP 呼び出しはそれぞれのツールで利用されます。

表11.1 エラスティック IP に関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-allocate-address	AllocateAddress	associateIpAddress
ec2-associate-address	AssociateAddress	enableStaticNat
ec2-describe-addresses	DescribeAddresses	listPublicIpAddresses
ec2-diassociate-address	DisassociateAddress	disableStaticNat
ec2-release-address	ReleaseAddress	disassociateIpAddress

表11.2 アベイラビリティゾーンに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-describe-availability-zones	DescribeAvailabilityZones	listZones

表11.3 イメージに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-create-image	CreateImage	createTemplate
ec2-deregister	DeregisterImage	DeleteTemplate
ec2-describe-images	DescribeImages	listTemplates
ec2-register	RegisterImage	registerTemplate

表11.4 イメージ属性に関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-describe-image-attribute	DescribeImageAttribute	listTemplatePermissions
ec2-modify-image-attribute	ModifyImageAttribute	updateTemplatePermissions
ec2-reset-image-attribute	ResetImageAttribute	updateTemplatePermissions

表11.5 インスタンスに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-describe-instances	DescribeInstances	listVirtualMachines
ec2-run-instances	RunInstances	deployVirtualMachine
ec2-reboot-instances	RebootInstances	rebootVirtualMachine
ec2-start-instances	StartInstances	startVirtualMachine
ec2-stop-instances	StopInstances	stopVirtualMachine

ec2-stop-instances	StopInstances	stopVirtualMachine
ec2-terminate-instances	TerminateInstances	destroyVirtualMachine

表11.6 インスタンス属性に関するマッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-describe-instance-attribute	DescribeInstanceAttribute	listVirtualMachines

表11.7 キーペアに関するマッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-add-keypair	CreateKeyPair	createSSHKeyPair
ec2-delete-keypair	DeleteKeyPair	deleteSSHKeyPair
ec2-describe-keypairs	DescribeKeyPairs	listSSHKeyPairs
ec2-import-keypair	ImportKeyPair	registerSSHKeyPair

表11.8 パスワードに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-get-password	GetPasswordData	getVMPassword

表11.9 セキュリティグループに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-authorize	AuthorizeSecurityGroupIngress	authorizeSecurityGroupIngress
ec2-add-group	CreateSecurityGroup	createSecurityGroup
ec2-delete-group	DeleteSecurityGroup	deleteSecurityGroup
ec2-describe-group	DescribeSecurityGroups	listSecurityGroups
ec2-revoke	RevokeSecurityGroupIngress	revokeSecurityGroupIngress

表11.10 スナップショットに関数 API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-create-snapshot	CreateSnapshot	createSnapshot
ec2-delete-snapshot	DeleteSnapshot	deleteSnapshot
ec2-describe-snapshots	DescribeSnapshots	listSnapshots

表11.11 ボリュームに関する API マッピング

EC2 コマンド	SOAP 呼び出し	CloudStack の API 呼び出し
ec2-attach-volume	AttachVolume	attachVolume
ec2-create-volume	CreateVolume	createVolume
ec2-delete-volume	DeleteVolume	deleteVolume
ec2-describe-volume	DescribeVolume	listVolumes
ec2-detach-volume	DetachVolume	detachVolume

11.7. Examples

There are many tools available to interface with a AWS compatible API. In this section we provide a few examples that users of CloudStack can build upon.

11.7.1. Boto Examples

Boto is one of them. It is a Python package available at https://github.com/boto/boto. In this section we provide two examples of Python scripts that use Boto and have been tested with the CloudStack AWS API Interface.

First is an EC2 example. Replace the Access and Secret Keys with your own and update the endpoint.

例11.1 An EC2 Boto example

```
#!/usr/bin/env python

import sys
import os
import boto
import boto.ec2

region = boto.ec2.regioninfo.RegionInfo(name="ROOT",endpoint="localhost")
apikey='GwNnpUPrO6KgIdZu01z_ZhhZnKjtSdRwuYd4DvpzvFpyxGMvrzno2q05MB0ViBoFYtdqKd'
secretkey='t4eXLEYWw7chBhDlaKf38adCMSHx_wlds6JfSx3z9fSpSOm0AbP9Moj0oGIzy2LSC8iw'

def main():
 '''Establish connection to EC2 cloud'''
        conn =boto.connect_ec2(aws_access_key_id=apikey,
                        aws_secret_access_key=secretkey,
                        is_secure=False,
                        region=region,
                        port=7080,
                        path="/awsapi",
                        api_version="2010-11-15")

        '''Get list of images that I own'''
 images = conn.get_all_images()
 print images
 myimage = images[0]
```

```
 '''Pick an instance type'''
 vm_type='m1.small'
 reservation = myimage.run(instance_type=vm_type,security_groups=['default'])

if __name__ == '__main__':
 main()
```

Second is an S3 example. Replace the Access and Secret keys with your own, as well as the endpoint of the service. Be sure to also update the file paths to something that exists on your machine.

例11.2 An S3 Boto Example

```
#!/usr/bin/env python

import sys
import os
from boto.s3.key import Key
from boto.s3.connection import S3Connection
from boto.s3.connection import OrdinaryCallingFormat

apikey='ChOw-pwdcCFy6fpeyv6kUaR0NnhzmG3tE7HLN2z3OB_s-ogF5HjZtN4rnzKnq2UjtnHeg_yLA5gOw'
secretkey='IMY8R7CJQiSGFk4cHwfXXN3DUFXz07cCiU80eM3MCmfLs7kusgyOfm0g9qzXRXhoAPCH-IRxXc3w'

cf=OrdinaryCallingFormat()

def main():
 '''Establish connection to S3 service'''
        conn =S3Connection(aws_access_key_id=apikey,aws_secret_access_key=secretkey, \
                           is_secure=False, \
                           host='localhost', \
                           port=7080, \
                           calling_format=cf, \
                           path="/awsapi/rest/AmazonS3")

        try:
            bucket=conn.create_bucket('cloudstack')
            k = Key(bucket)
            k.key = 'test'
            try:
               k.set_contents_from_filename('/Users/runseb/Desktop/s3cs.py')
            except:
               print 'could not write file'
               pass
        except:
            bucket = conn.get_bucket('cloudstack')
            k = Key(bucket)
            k.key = 'test'
            try:
               k.get_contents_to_filename('/Users/runseb/Desktop/foobar')
            except:
               print 'Could not get file'
               pass

        try:
           bucket1=conn.create_bucket('teststring')
           k=Key(bucket1)
           k.key('foobar')
           k.set_contents_from_string('This is my silly test')
        except:
           bucket1=conn.get_bucket('teststring')
           k = Key(bucket1)
           k.key='foobar'
           k.get_contents_as_string()

if __name__ == '__main__':
 main()
```

11.7.2. JClouds Examples

第12章 ネットワークのセットアップ

CloudStack のインストールを成功させるには、ネットワークを正しくセットアップすることが不可欠です。ここでは、ネットワークを適切にセットアップするための正しい手順を決定し、その手順に従う方法について説明します。

12.1. 基本と拡張ネットワーク

CloudStack では基本と拡張の 2 種類のネットワーク設定を提供します

基本

AWS スタイルのネットワークシステムに対応します。セキュリティグループ(送信元 IP アドレスのフィルター)のようなレイヤー3 レベルの方法でゲストを分離できる単一のネットワークを提供します。

拡張

より高度なトポロジに対応します。このネットワークモデルを選択すると、より柔軟にゲストのネットワークを定義できますが基本ネットワークと比べより多くの設定手順が必要となります。

各ゾーンは基本ネットワークもしくは拡張ネットワークどちらかを持ちます。CloudStack で作成、設定されたゾーンに対し一度ネットワークモデルを選択すると以降変更することはできません。ゾーンは一生 基本ネットワークもしくは拡張ネットワークのどちらかに設定されることになります。

次の表は2つのネットワークモデルの機能比較を表します。

ネットワーク機能	基本ネットワーク	Advanced Network
Number of networks	Single network	Multiple networks
Firewall type	Physical	Physical and Virtual
Load balancer	Physical	Physical and Virtual
Isolation type	Layer 3	Layer 2 and Layer 3
VPN support	No	Yes
Port forwarding	Physical	Physical and Virtual
1:1 NAT	Physical	Physical and Virtual
送信元 NAT	No	Physical and Virtual
Userdata	Yes	Yes
Network usage monitoring	sFlow / netFlow at physical router	Hypervisor and Virtual Router
DNSとDHCP	Yes	Yes

The two types of networking may be in use in the same cloud. However, a given zone must use either Basic Networking or Advanced Networking.

Different types of network traffic can be segmented on the same physical network. Guest traffic can also be segmented by account. To isolate traffic, you can use separate VLANs. If you are using separate VLANs on a single physical network, make sure the VLAN tags are in separate numerical ranges.

12.2. VLAN 割り当ての例

パブリックトラフィックとゲストトラフィックには VLAN が必要です。VLAN 割り当て方式の例を次に示します。

VLAN ID	トラフィックの種類	スコープ
500以下	管理トラフィックです。管理用に予約されています。	CloudStack ソフトウェアはこの VLAN、ハイパー バイザー、およびシステム仮想マシンにアクセスできます。
500-599	パブリックトラフィックを伝送する VLAN です。	CloudStack アカウントです。
600-799	ゲストトラフィックを伝送する VLAN です。	CloudStack アカウントです。アカウント固有の VLAN はこのプールから選択します

		択します。
800-899	ゲストトラフィックを伝送する VLAN です。	CloudStack アカウントです。CloudStack 管理者が 選択する、個々のアカウントに割り当てる VLAN です。
900-999	ゲストトラフィックを伝送する VLAN です。	CloudStack アカウントです。プロジェクト、ドメイン、またはすべてのアカウントによって範囲を指定できます。
1000以上	将来用に予約されています。	

12.3. Example Hardware Configuration

This section contains an example configuration of specific switch models for zone-level layer-3 switching. It assumes VLAN management protocols, such as VTP or GVRP, have been disabled. The example scripts must be changed appropriately if you choose to use VTP or GVRP.

12.3.1. Dell 62xx

次の手順では、Dell 62xx をゾーンレベルのレイヤー3 スイッチ用に構成する方法を示します。この手順は、VLAN 201 を使用してポッド 1 のタグなしのプライベート IP アドレスをルーティングし、ポッド 1 のレイヤー2 スイッチがイーサネットポート 1/g1 に接続されていることを前提としています。

Dell 62xx シリーズスイッチは、最大で 1024 の VLAN をサポートします。

1. すべての VLAN をデータベースモードで構成します。

   ```
   vlan database
   vlan 200-999
   exit
   ```

2. イーサネットポート 1/g1 を構成します。

   ```
   interface ethernet 1/g1
   switchport mode general
   switchport general pvid 201
   switchport general allowed vlan add 201 untagged
   switchport general allowed vlan add 300-999 tagged
   exit
   ```

これらのコマンドにより、イーサネットポート 1/g1 が次のように構成されます。

- VLAN 201 は、ポート 1/g1 のタグなしネイティブ VLAN です。
- すべての VLAN(300~999)は、ポッドレベルのすべてのレイヤー2 スイッチに渡されます。

12.3.2. Cisco 3750

次の手順では、Cisco 3750 をゾーンレベルのレイヤー3 スイッチ用に構成する方法を示します。この手順は、VLAN 201 を使用してポッド 1 のタグなしのプライベート IP アドレスをルーティングし、ポッド 1 のレイヤー2 スイッチがギガビットイーサ ネット 1/0/1 に接続されていることを前提としています。

1. VTP のモードをトランスペアレントにすることにより、1000 を超える VLAN ID を使用することができます。ここでは最 大 999 個の VLAN しか使用しないため、VTP のモードをトランスペアレントにすることが絶対に必要というわけではありません。

   ```
   vtp mode transparent
   vlan 200-999
   exit
   ```

2. ギガビットイーサネット 1/0/1 を構成します。

   ```
   interface GigabitEthernet1/0/1
   switchport trunk encapsulation dot1q
   switchport mode trunk
   switchport trunk native vlan 201
   exit
   ```

これらのコマンドにより、ギガビットイーサネット 1/0/1 が次のように構成されます。

- VLAN 201 は、ギガビットイーサネット 1/0/1 のタグなしネイティブ VLAN です。
- Cisco ではデフォルトですべての VLAN が渡されます。その結果、すべての VLAN(300~999)は、ポッドレベルのすべてのレイヤー2 スイッチに渡されます。

12.4. レイヤー2スイッチ

レイヤー2スイッチは、ポッド内部のアクセススイッチレイヤーです。

- このスイッチは、すべてのVLANを各コンピューティングホストにトランク接続します。
- このスイッチは、コンピューティングホストとストレージホストが含まれる管理ネットワークのトラフィックを切り替えます。レイヤー3スイッチは、管理ネットワークのゲートウェイとして機能します。

構成例

ここでは、ポッドレベルのレイヤー2スイッチのための具体的なスイッチモデルの構成例を示します。VTPやGVRPなどのVLAN管理プロトコルが無効になっていることが前提です。VTPまたはGVRPを使用する場合は、スクリプトを適切に変更する必要があります。

12.4.1. Dell 62xx

次の手順では、Dell 62xx をポッドレベルのレイヤー2 スイッチ用に構成する方法を示します。

1. すべての VLAN をデータベースモードで構成します。

```
vlan database
vlan 300-999
exit
```

2. VLAN 201 を使用してポッド 1 のタグなしプライベート IP アドレスをルーティングします。ポッド 1 はこのレイヤー2 スイッチに接続されています。

```
interface range ethernet all
switchport mode general
switchport general allowed vlan add 300-999 tagged
exit
```

これらのコマンドにより、すべてのイーサネットポートが次のように機能するように構成されます。

- すべてのポートは同じように構成されます。
- すべての VLAN(300~999)は、レイヤー2 スイッチのすべてのポートを通じて渡されます。

12.4.2. Cisco 3750

次の手順では、Cisco 3750 をポッドレベルのレイヤー2 スイッチ用に構成する方法を示します。

1. VTP のモードをトランスペアレントにすることにより、1000 を超える VLAN ID を使用することができます。ここでは最 大 999 個の VLAN しか使用しないため、VTP のモードをトランスペアレントにすることが絶対に必要というわけではありません。

```
vtp mode transparent
vlan 300-999
exit
```

2. すべてのポートを dot1q に構成し、201 をネイティブ VLAN として設定します。

```
interface range GigabitEthernet 1/0/1-24
switchport trunk encapsulation dot1q
switchport mode trunk
switchport trunk native vlan 201
exit
```

Cisco ではデフォルトですべての VLAN が渡されます。Cisco のスイッチでは、2 つのポートが共に接続されているときに、 ネイティブ VLAN ID が異なるというエラーを記録します。そのため、VLAN 201 をレイヤー2 スイッチ上でネイティブ VLAN として指定します。

12.5. Hardware Firewall

All deployments should have a firewall protecting the management server; see Generic Firewall Provisions. Optionally, some deployments may also have a Juniper SRX firewall that will be the default gateway for the guest networks; see 「External Guest Firewall Integration for Juniper SRX (Optional)」.

12.5.1. Generic Firewall Provisions

The hardware firewall is required to serve two purposes:

- Protect the Management Servers. NAT and port forwarding should be configured to direct traffic from the public Internet to the Management Servers.
- Route management network traffic between multiple zones. Site-to-site VPN should be configured between multiple zones.

To achieve the above purposes you must set up fixed configurations for the firewall. Firewall rules and policies need not change as users are provisioned into the cloud. Any brand of hardware firewall that supports NAT and site-to-site VPN can be used.

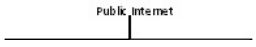
12.5.2. External Guest Firewall Integration for Juniper SRX (Optional)

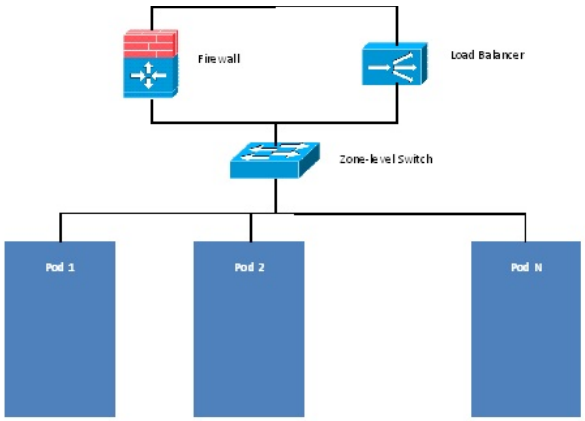
注記

Available only for guests using advanced networking.

CloudStack provides for direct management of the Juniper SRX series of firewalls. This enables CloudStack to establish static NAT mappings from public IPs to guest VMs, and to use the Juniper device in place of the virtual router for firewall services. You can have one or more Juniper SRX per zone. This feature is optional. If Juniper integration is not provisioned, CloudStack will use the virtual router for these services.

The Juniper SRX can optionally be used in conjunction with an external load balancer. External Network elements can be deployed in a side-by-side or inline configuration.





CloudStack requires the Juniper to be configured as follows:

注記

Supported SRX software version is 10.3 or higher.

1. Install your SRX appliance according to the vendor's instructions.
2. Connect one interface to the management network and one interface to the public network. Alternatively, you can connect the same interface to both networks and a use a VLAN for the public network.
3. Make sure "vlan-tagging" is enabled on the private interface.
4. Record the public and private interface names. If you used a VLAN for the public interface, add a ".[VLAN TAG]" after the interface name. For example, if you are using ge-0/0/3 for your public interface and VLAN tag 301, your public interface name would be "ge-0/0/3.301". Your private interface name should always be untagged because the CloudStack software automatically creates tagged logical interfaces.
5. Create a public security zone and a private security zone. By default, these will already exist and will be called "untrust" and "trust". Add the public interface to the public zone and the private interface to the private zone. Note down the security zone names.
6. Make sure there is a security policy from the private zone to the public zone that allows all traffic.
7. Note the username and password of the account you want the CloudStack software to log in to when it is programming rules.
8. Make sure the "ssh" and "xnm-clear-text" system services are enabled.
9. If traffic metering is desired:
    a. a. Create an incoming firewall filter and an outgoing firewall filter. These filters should be the same names as your public security zone name and private security zone name respectively. The filters should be set to be "interface-specific". For example, here is the configuration where the public zone is "untrust" and the private zone is "trust":

    ```
    root@cloud-srx# show firewall
    filter trust {
        interface-specific;
    }
    filter untrust {
        interface-specific;
    }
    ```

    b. Add the firewall filters to your public interface. For example, a sample configuration output (for public interface ge-0/0/3.0, public security zone untrust, and private security zone trust) is:

    ```
    ge-0/0/3 {
        unit 0 {
            family inet {
                filter {
                    input untrust;
                    output trust;
                }
                address 172.25.0.252/16;
            }
        }
    }
    ```

10. Make sure all VLANs are brought to the private interface of the SRX.
11. After the CloudStack Management Server is installed, log in to the CloudStack UI as administrator.
12. 左側のナビゲーションバーで [Infrastructure] をクリックします。
13. [Zones] で [View More]をクリックします。
14. 左側のナビゲーションバーで［Infrastructure］をクリックします。
15. [Network] タブをクリックします。
16. ダイアグラムの［Network Service Providers］ノードで［Configure］をクリックします（このノードを表示するには下にスクロールする必要がある可能性があります）。
17. Click SRX.
18. Click the Add New SRX button (+) and provide the following:

- IP address：デバイスのIPアドレスです。
- Username: The user name of the account on the SRX that CloudStack should use.
- Password: The password of the account.
- Public Interface. The name of the public interface on the SRX. For example, ge-0/0/2. A ".x" at the end of the interface indicates the VLAN that is in use.
- Private Interface: The name of the private interface on the SRX. For example, ge-0/0/1.
- Usage Interface: (Optional) Typically, the public interface is used to meter traffic. If you want to use a different interface, specify its name here
- Number of Retries: The number of times to attempt a command on the SRX before failing. The default value is 2.
- Timeout (seconds): The time to wait for a command on the SRX before considering it failed. Default is 300 seconds.
- Public Network: The name of the public network on the SRX. For example, trust.
- Private Network: The name of the private network on the SRX. For example, untrust.
- Capacity: The number of networks the device can handle
- Dedicated: When marked as dedicated, this device will be dedicated to a single account. When Dedicated is checked, the value in the Capacity field has no significance implicitly, its value is 1

19. [OK]をクリックします。
20. Click Global Settings. Set the parameter external.network.stats.interval to indicate how often you want CloudStack to fetch network usage statistics from the Juniper SRX. If you are not using the SRX to gather network usage statistics, set to 0.

12.5.3. 外部のゲスト負荷分散装置の統合（オプション）

CloudStackでは、オプションでCitrix NetScalerまたはF5 BigIPの負荷分散装置を使用して、ゲストに負荷分散サービスを提供することができます。このオプションを有効にしない場合は、CloudStackは、仮想ルーターのソフトウェア負荷分散機能を使用します。

CloudStack のために外部の負荷分散装置を設置して有効にするには、次の手順に従います。

1. 造元の指示に従って、アプライアンスをセットアップします。
2. パブリックトラフィックと管理トラフィックを伝送するネットワーク（同じネットワークである可能性があります）にアプライアンスを接続します。
3. IPアドレス、ユーザー名、パスワード、パブリックインターフェイス名、およびプライベートインターフェイス名を記録します。インターフェイス名は、「1.1」または「1.2」のような形式になります。
4. VLANが管理ネットワークインターフェイスにトランク接続されていることを確認します。
5. CloudStack管理サーバーをインストールした後で、CloudStackユーザーインターフェイスに管理者としてログオンします。
6. 左側のナビゲーションバーで [Infrastructure] をクリックします。
7. [Zones] で [View More]をクリックします。
8. 左側のナビゲーションバーで［Infrastructure］をクリックします。
9. [Network] タブをクリックします。
10. ダイアグラムの［Network Service Providers］ノードで［Configure］をクリックします（このノードを表示するには下にスクロールする必要がある可能性があります）。
11. ［NetScaler］または［F5］をクリックします。
12. Addボタン(+)をクリックして次の項目に入力します:

    NetScalerの場合
    - IP address：デバイスのIPアドレスです。
    - UsernameおよびPassword：デバイスにアクセスするための認証資格情報です。CloudStackは、この資格情報を使用してデバイスにアクセスします。
    - Type：追加するデバイスの種類です。［F5 Big Ip Load Balancer］。［NetScaler VPX］、［NetScaler MPX］、または［NetScaler SDX］のいずれかです。NetScalerの種類を比較するには、『CloudStack管理ガイド』を参照してください。
    - Public interface：パブリックネットワークの一部として構成されるデバイスのインターフェイスです。
    - Private interface：プライベートネットワークの一部として構成されるデバイスのインターフェイスです。
    - Number of retries：操作が失敗したとみなす前にデバイスに対してコマンドを試行する回数です。デフォルトは2です。
    - Capacity：このデバイスを共有するゲストネットワークの数です。
    - Dedicated：専用のデバイスは単一のアカウント専用になります。［Dedicated］チェックボックスをオンにすると、［Capacity］ボックスの値は無視され、暗黙的に1であるとみなされます。
13. [OK]をクリックします。

これで、外部の負荷分散装置の設置と準備は完了です。仮想マシンおよびNAT/負荷分散規則を追加できます。

12.6. Management Server Load Balancing

CloudStack can use a load balancer to provide a virtual IP for multiple Management Servers. The administrator is responsible for creating the load balancer rules for the Management Servers. The application requires persistence or stickiness across multiple sessions. The following chart lists the ports that should be load balanced and whether or not persistence is required.

Even if persistence is not required, enabling it is permitted.

Source Port	Destination Port	Protocol	Persistence Required?
80 or 443	8080 (or 20400 with AJP)	HTTP (or AJP)	Yes
8250	8250	TCP	Yes

8250	8250	TCP	Yes
8096	8096	HTTP	No

In addition to above settings, the administrator is responsible for setting the 'host' global config value from the management server IP to load balancer virtual IP address. If the 'host' value is not set to the VIP for Port 8250 and one of your management servers crashes, the UI is still available but the system VMs will not be able to contact the management server.

12.7. トポロジの要件

12.7.1. Security Requirements

The public Internet must not be able to access port 8096 or port 8250 on the Management Server.

12.7.2. Runtime Internal Communications Requirements

- The Management Servers communicate with each other to coordinate tasks. This communication uses TCP on ports 8250 and 9090.
- The console proxy VMs connect to all hosts in the zone over the management traffic network. Therefore the management traffic network of any given pod in the zone must have connectivity to the management traffic network of all other pods in the zone.
- The secondary storage VMs and console proxy VMs connect to the Management Server on port 8250. If you are using multiple Management Servers, the load balanced IP address of the Management Servers on port 8250 must be reachable.

12.7.3. ストレージネットワークトポロジの要件

セカンダリストレージNFSのエクスポートは、セカンダリストレージ仮想マシンによってマウントされます。セカンダリストレージトラフィックは、別個のストレージネットワークが存在する場合でも、管理トラフィックネットワークを介して伝送されます。プライマリストレージトラフィックは、（使用可能な場合は）ストレージネットワークを介して伝送されます。セカンダリストレージNFSサーバーをストレージネットワーク上に配置する場合は、管理トラフィックネットワークからストレージネットワークへのルートが存在することを確認してください。

12.7.4. 外部ファイアウォールトポロジの要件

外部ファイアウォールを統合する場合も、パブリックIPアドレスのVLANをホストにトランク接続する必要があります。これは、セカンダリストレージ仮想マシンとコンソールプロキシ仮想マシンをサポートするために必要です。

12.7.5. 拡張ゾーントポロジの要件

拡張ネットワーク設定では、プライベートネットワークとパブリックネットワークに、それぞれ別のサブネットを使用する必要があります。

12.7.6. XenServerトポロジの要件

管理サーバーは、ポート22（ssh）、と80（HTTP）、および443（HTTPS）でXenServerホストと通信します。

12.7.7. VMwareトポロジの要件

- 管理サーバーとセカンダリストレージ仮想マシンは、vCenterおよびゾーン内のすべてのESXiホストにアクセスできる必要があります。ファイアウォールを介した必要なアクセスを許可するために、ポート443を開放しておきます。
- 管理サーバーは、ポート443（HTTPS）でVMware vCenterサーバーと通信します。
- 管理サーバーは、管理トラフィックネットワーク上のポート3922（ssh）でシステム仮想マシンと通信します。

12.7.8. KVMトポロジの要件

管理サーバーは、ポート22（ssh）でKVMホストと通信します。

12.8. Guest Network Usage Integration for Traffic Sentinel

To collect usage data for a guest network, CloudStack needs to pull the data from an external network statistics collector installed on the network. Metering statistics for guest networks are available through CloudStack's integration with inMon Traffic Sentinel.

Traffic Sentinel is a network traffic usage data collection package. CloudStack can feed statistics from Traffic Sentinel into its own usage records, providing a basis for billing users of cloud infrastructure. Traffic Sentinel uses the traffic monitoring protocol sFlow. Routers and switches generate sFlow records and provide them for collection by Traffic Sentinel, then CloudStack queries the Traffic Sentinel database to obtain this information

To construct the query, CloudStack determines what guest IPs were in use during the current query interval. This includes both newly assigned IPs and IPs that were assigned in a previous time period and continued to be in use. CloudStack queries Traffic Sentinel for network statistics that apply to these IPs during the time period they remained allocated in CloudStack. The returned data is correlated with the customer account that owned each IP and the timestamps when IPs were assigned and released in order to create billable metering records in CloudStack. When the Usage Server runs, it collects this data.

To set up the integration between CloudStack and Traffic Sentinel:

1. On your network infrastructure, install Traffic Sentinel and configure it to gather traffic data. For installation and configuration steps, see inMon documentation at Traffic Sentinel Documentation.
2. In the Traffic Sentinel UI, configure Traffic Sentinel to accept script querying from guest users. CloudStack will be

the guest user performing the remote queries to gather network usage for one or more IP addresses.

Click File > Users > Access Control > Reports Query, then select Guest from the drop-down list.

3. On CloudStack, add the Traffic Sentinel host by calling the CloudStack API command addTrafficMonitor. Pass in the URL of the Traffic Sentinel as protocol + host + port (optional); for example, http://10.147.28.100:8080. For the addTrafficMonitor command syntax, see the API Reference at API Documentation.

   For information about how to call the CloudStack API, see the Developer's Guide at CloudStack API Developer's Guide.
4. CloudStackユーザーインターフェイスに管理者としてログオンします。
5. Select Configuration from the Global Settings page, and set the following:

   direct.network.stats.interval: How often you want CloudStack to query Traffic Sentinel.

12.9. Setting Zone VLAN and Running VM Maximums

In the external networking case, every VM in a zone must have a unique guest IP address. There are two variables that you need to consider in determining how to configure CloudStack to support this: how many Zone VLANs do you expect to have and how many VMs do you expect to have running in the Zone at any one time.

Use the following table to determine how to configure CloudStack for your deployment.

guest.vlan.bits	Maximum Running VMs per Zone	Maximum Zone VLANs
12	4096	4094
11	8192	2048
10	16384	1024
10	32768	512

Based on your deployment's needs, choose the appropriate value of guest.vlan.bits. Set it as described in Edit the Global Configuration Settings (Optional) section and restart the Management Server.

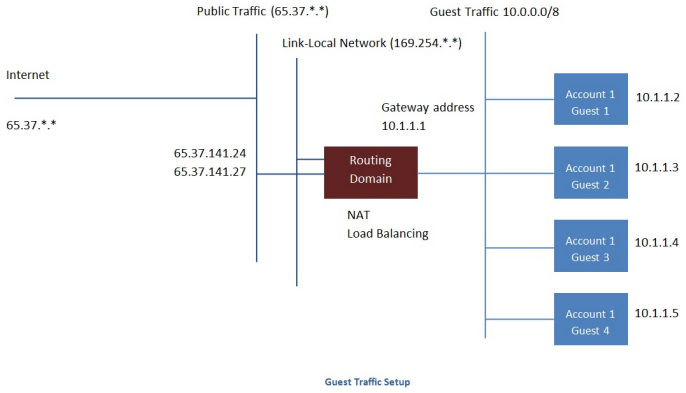
第13章 ネットワークとトラフィックの管理

CloudStackクラウドでは、セキュリティの設定された共有インフラストラクチャを使用し、プライベートLANでゲストを使用しているというユーザーの認識のもと、ゲスト仮想マシン間で相互に通信できます。\nCloudStackの仮想ルーターは、ゲストトラフィックのネットワーク設定機能を提供する主要コンポーネントです。

13.1. ゲスト トラフィック

A network can carry guest traffic only between VMs within one zone. Virtual machines in different zones cannot communicate with each other using their IP addresses; they must communicate with each other by routing through a public IP address.

This figure illustrates a typical guest traffic setup:



Guest Traffic Setup

The Management Server automatically creates a virtual router for each network. A virtual router is a special virtual machine that runs on the hosts. Each virtual router has three network interfaces. Its eth0 interface serves as the gateway for the guest traffic and has the IP address of 10.1.1.1. Its eth1 interface is used by the system to configure the virtual router. Its eth2 interface is assigned a public IP address for public traffic.

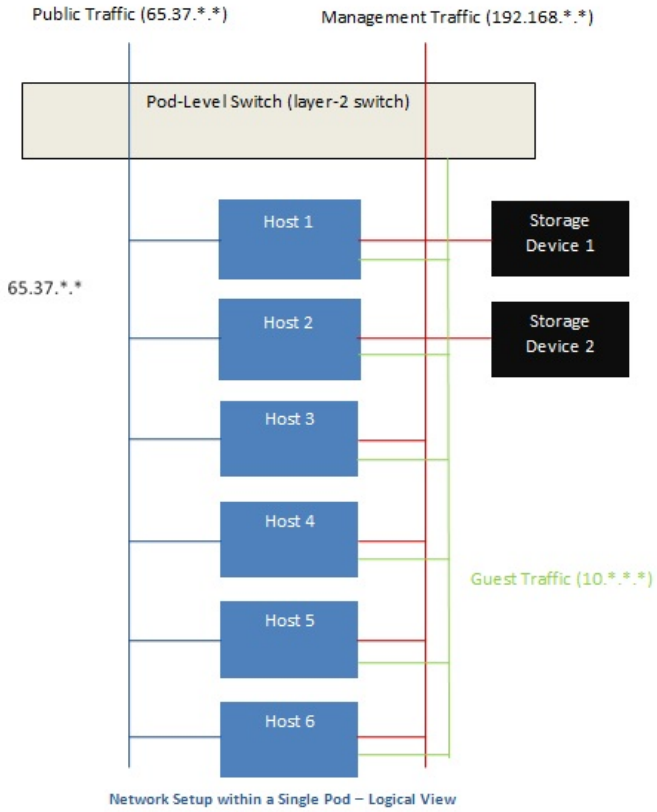
The virtual router provides DHCP and will automatically assign an IP address for each guest VM within the IP range assigned for the network. The user can manually reconfigure guest VMs to assume different IP addresses.

Source NAT is automatically configured in the virtual router to forward outbound traffic for all guest VMs

13.2. Networking in a Pod

13.2. Networking in a Pod

The figure below illustrates network setup within a single pod. The hosts are connected to a pod-level switch. At a minimum, the hosts should have one physical uplink to each switch. Bonded NICs are supported as well. The pod-level switch is a pair of redundant gigabit switches with 10 G uplinks.



Network Setup within a Single Pod – Logical View

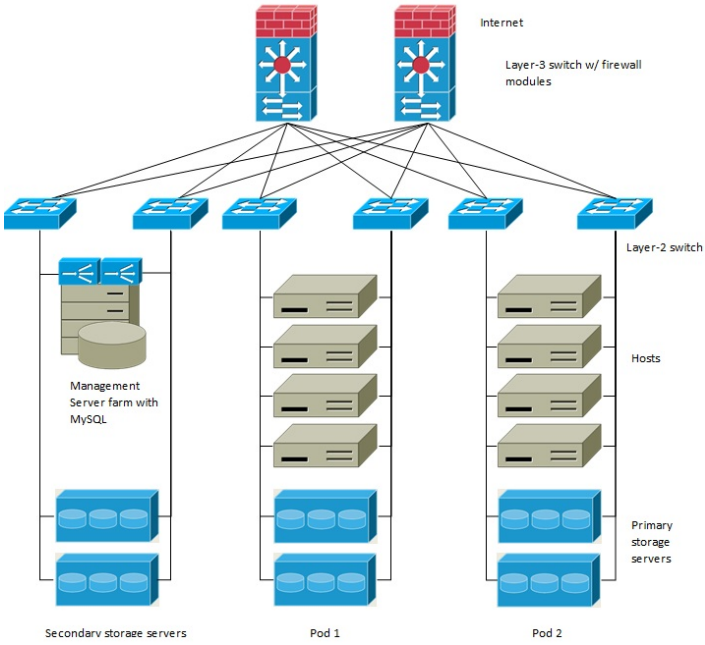
Servers are connected as follows:

- Storage devices are connected to only the network that carries management traffic.
- Hosts are connected to networks for both management traffic and public traffic.
- Hosts are also connected to one or more networks carrying guest traffic.

We recommend the use of multiple physical Ethernet cards to implement each network interface as well as redundant switch fabric in order to maximize throughput and improve reliability.

13.3. Networking in a Zone

The following figure illustrates the network setup within a single zone.



A firewall for management traffic operates in the NAT mode. The network typically is assigned IP addresses in the 192.168.0.0/16 Class B private address space. Each pod is assigned IP addresses in the 192.168.*.0/24 Class C private address space.

Each zone has its own set of public IP addresses. Public IP addresses from different zones do not overlap.

13.4. 基本ゾーンの物理ネットワーク構成

基本ネットワークの場合は、物理ネットワークの構成はごく簡単です。構成する必要があるのは、ゲスト仮想マシンが生成するトラフィックを伝送するための1つのゲストネットワークだけです。CloudStackに初めてゾーンを追加するときは、Add Zone の画面からゲストネットワークをセットアップします。

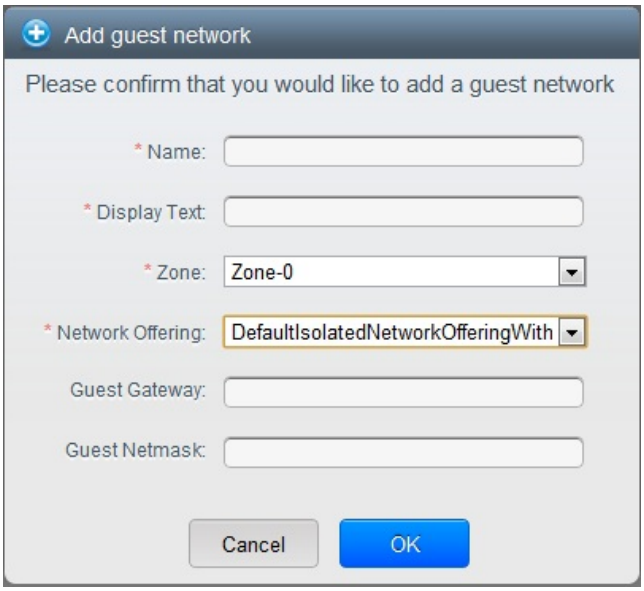
13.5. Advanced Zone Physical Network Configuration

Within a zone that uses advanced networking, you need to tell the Management Server how the physical network is set up to carry different kinds of traffic in isolation.

13.5.1. 拡張ゾーンのゲストトラフィックの構成

次の手順は、CloudStack ユーザーインターフェイスにログオン済みであることを前提としています。基本ゲストネットワークを構成するには、次の手順に従います。

1. 左側のナビゲーションバーで [Infrastructure] をクリックします。[Zones] で [View More] をクリックし、ネットワークを追加するゾーンを選択します。
2. [Network] タブをクリックします。
3. [Add guest network]をクリックします。
   ゲストネットワークの追加ウインドウが表示されます。



4. 次の情報を指定します。
   - **Name :** ネットワークの名前です。これはユーザーに表示されます。
   - **Display Text :** ネットワークの説明です。これはユーザーに表示されます。
   - **Zone :** ゲストネットワークを構成したいゾーン名です。
   - **Network offering :** もし管理者が複数のネットワークオファリングを設定している場合、利用したいネットワークオファリングを選択します。
   - **Guest Gateway :** ゲストが使用するゲートウェイです。
   - **Guest Netmask :** ゲストの使用するサブネット上で使用されるネットマスクです。
5. 「OK」をクリックします。

13.5.2. 拡張ゾーンのパブリックトラフィックの構成

拡張ネットワーク設定を使用するゾーンでは、インターネットトラフィックの IP アドレスの範囲を少なくとも 1 つ構成する必要があります。

13.6. Using Multiple Guest Networks

In zones that use advanced networking, additional networks for guest traffic may be added at any time after the initial installation. You can also customize the domain name associated with the network by specifying a DNS suffix for each network.

A VM's networks are defined at VM creation time. A VM cannot add or remove networks after it has been created, although the user can go into the guest and remove the IP address from the NIC on a particular network.

Each VM has just one default network. The virtual router's DHCP reply will set the guest's default gateway as that for the default network. Multiple non-default networks may be added to a guest in addition to the single, required default network. The administrator can control which networks are available as the default network.

Additional networks can either be available to all accounts or be assigned to a specific account. Networks that are available to all accounts are zone-wide. Any user with access to the zone can create a VM with access to that network. These zone-wide networks provide little or no isolation between guests.Networks that are assigned to a specific account provide strong isolation.

13.6.1. ゲストネットワークの追加

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. [Add guest network] をクリックし、以下の情報を入力します。
   - **Name :** ネットワークの名前です。この名前はユーザーから見ることができます。
   - **Display Text :** ネットワークの詳細情報です。この情報はユーザーから見ることができます。
   - **Zone :** ネットワークを適用するゾーンの名前です。各ゾーンはゲストネットワークに対し違うIPレンジを持ったブロードキャストドメインに属します。管理者は各ゾーンに対しIPレンジを設定する必要があります。
   - **Network offering :** もし管理者によって複数のネットワークオファリングが設定されている場合、ここで利用したいネットワークを1つ選択します。
   - **Guest Gateway :** ゲストVMが利用するゲートウェイを設定します。
   - **Guest Netmask :** ゲストVMが利用するサブネットのネットマスクを設定します。
4. [Create] をクリックします。

13.6.2. ゲストネットワーク上のネットワークオファリングの変更

ユーザーまたは管理者は、既存のゲストネットワークに関連付けられているネットワークオファリングを変更できます。

- 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
- If you are changing from a network offering that uses the CloudStack virtual router to one that uses external devices as network service providers, you must first stop all the VMs on the network. See "Stopping and Starting Virtual Machines" in the Administrator's Guide.
- 左側のナビゲーションから [Network] を選択します。
- Click the name of the network you want to modify.
- In the Details tab, click Edit. 
- [Network Offering]ボックスの一覧で新しいネットワークオファリングを選択して、[Apply]をクリックします。
- A prompt is displayed asking whether you want to keep the existing CIDR. This is to let you know that if you change the network offering, the CIDR will be affected. Choose No to proceed with the change.
- Wait for the update to complete. Don't try to restart VMs until the network change is complete.
- If you stopped any VMs, restart them.

13.7. セキュリティグループ

13.7.1. セキュリティグループについて

Security groups provide a way to isolate traffic to VMs. A security group is a group of VMs that filter their incoming and outgoing traffic according to a set of rules, called ingress and egress rules. These rules filter network traffic according to the IP address that is attempting to communicate with the VM. Security groups are particularly useful in zones that use basic networking, because there is a single guest network for all guest VMs. In advanced zones, security groups are supported only on the KVM hypervisor.

注記

拡張ネットワークを使用すゾーンでは、代わりに複数のゲストネットワークを作成することで、仮想マシンへのトラフィックを隔離します。

各CloudStackアカウントには、すべての受信トラフィックを拒否し、すべての送信トラフィックを許可するデフォルトのセキュリティグループが用意されています。すべての新しい仮想マシンが望ましい規則セットを継承するように、デフォルトのセキュリティグループを変更できます。

CloudStackのユーザーは、任意の数のセキュリティグループを追加できます。新しい仮想マシンには、ユーザー定義のセキュリティグループが別に指定されていない限り、デフォルトのセキュリティグループが起動時に割り当てられます。仮想マシンは、任意の数のセキュリティグループのメンバーになることができます。仮想マシンをセキュリティグループに割り当てると、仮想マシンは有効である限りずっとそのグループに属します。実行中の仮想マシンを別のセキュリティグループに移動することはできません。

セキュリティグループは、任意の数の受信規則および送信規則を削除または追加することで変更できます。変更後の新しい規則は、実行中または停止中にかかわらず、グループ内のすべての仮想マシンに適用されます。

受信規則を指定しない場合は、送信規則によって送信が許可されているトラフィックへの応答を除いて、トラフィックの受信は許可されません。

13.7.2. セキュリティグループの追加

ユーザーもしくは管理者は新しいセキュリティグループを定義することができます。

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションバーで[Network]をクリックします。
3. [Select view]ボックスの一覧で[Security Groups]を選択します。

3. [Select view]ボックスの一覧で[Security Groups]を選択します。
4. [Add Security Group]をクリックします。
5. 名前と説明を入力します。
6. [OK]をクリックします。
   新しいセキュリティグループが[Security Groups Details]タブに表示されます。
7. セキュリティグループを使いやすくするには、「セキュリティグループへの受信規則と送信規則の追加」に進みます。

13.7.3. Security Groups in Advanced Zones (KVM Only)

CloudStack provides the ability to use security groups to provide isolation between guests on a single shared, zone-wide network in an advanced zone where KVM is the hypervisor. Using security groups in advanced zones rather than multiple VLANs allows a greater range of options for setting up guest isolation in a cloud.

Limitations

The following are not supported for this feature:

- Two IP ranges with the same VLAN and different gateway or netmask in security group-enabled shared network.
- Two IP ranges with the same VLAN and different gateway or netmask in account-specific shared networks.
- Multiple VLAN ranges in security group-enabled shared network.
- Multiple VLAN ranges in account-specific shared networks.

Security groups must be enabled in the zone in order for this feature to be used.

13.7.4. Enabling Security Groups

In order for security groups to function in a zone, the security groups feature must first be enabled for the zone. The administrator can do this when creating a new zone, by selecting a network offering that includes security groups. The procedure is described in Basic Zone Configuration in the Advanced Installation Guide. The administrator can not enable security groups for an existing zone, only when creating a new zone.

13.7.5. Adding Ingress and Egress Rules to a Security Group

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションバーで[Network]をクリックします。
3. In Select view, choose Security Groups, then click the security group you want .
4. To add an ingress rule, click the Ingress Rules tab and fill out the following fields to specify what network traffic is allowed into VM instances in this security group. If no ingress rules are specified, then no traffic will be allowed in, except for responses to any traffic that has been allowed out through an egress rule.
   - **Add by CIDR/Account**. Indicate whether the source of the traffic will be defined by IP address (CIDR) or an existing security group in a CloudStack account (Account). Choose Account if you want to allow incoming traffic from all VMs in another security group
   - **Protocol**. The networking protocol that sources will use to send traffic to the security group. TCP and UDP are typically used for data exchange and end-user communications. ICMP is typically used to send error messages or network monitoring data.
   - **Start Port, End Port**. (TCP, UDP only) A range of listening ports that are the destination for the incoming traffic. If you are opening a single port, use the same number in both fields.
   - **ICMP Type, ICMP Code**. (ICMP only) The type of message and error code that will be accepted.
   - **CIDR**. (Add by CIDR only) To accept only traffic from IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the incoming traffic. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
   - **Account, Security Group**. (Add by Account only) To accept only traffic from another security group, enter the CloudStack account and name of a security group that has already been defined in that account. To allow traffic between VMs within the security group you are editing now, enter the same name you used in step 7.

   The following example allows inbound HTTP access from anywhere:

5. To add an egress rule, click the Egress Rules tab and fill out the following fields to specify what type of traffic is allowed to be sent out of VM instances in this security group. If no egress rules are specified, then all traffic will be allowed out. Once egress rules are specified, the following types of traffic are allowed out: traffic specified in egress rules; queries to DNS and DHCP servers; and responses to any traffic that has been allowed in through an ingress rule
   - **Add by CIDR/Account**. Indicate whether the destination of the traffic will be defined by IP address (CIDR) or an existing security group in a CloudStack account (Account). Choose Account if you want to allow outgoing traffic to all VMs in another security group.
   - **Protocol**. The networking protocol that VMs will use to send outgoing traffic. TCP and UDP are typically used for data exchange and end-user communications. ICMP is typically used to send error messages or network monitoring data.

monitoring data.

- **Start Port, End Port**. (TCP, UDP only) A range of listening ports that are the destination for the outgoing traffic. If you are opening a single port, use the same number in both fields.
- **ICMP Type, ICMP Code**. (ICMP only) The type of message and error code that will be sent
- **CIDR**. (Add by CIDR only) To send traffic only to IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the destination. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
- **Account, Security Group**. (Add by Account only) To allow traffic to be sent to another security group, enter the CloudStack account and name of a security group that has already been defined in that account. To allow traffic between VMs within the security group you are editing now, enter its name.

6. [Add]をクリックします。

13.8. External Firewalls and Load Balancers

CloudStack is capable of replacing its Virtual Router with an external Juniper SRX device and an optional external NetScaler or F5 load balancer for gateway and load balancing services. In this case, the VMs use the SRX as their gateway.

13.8.1. About Using a NetScaler Load Balancer

Citrix NetScaler is supported as an external network element for load balancing in zones that use advanced networking (also called advanced zones). Set up an external load balancer when you want to provide load balancing through means other than CloudStack's provided virtual router.

The NetScaler can be set up in direct (outside the firewall) mode. It must be added before any load balancing rules are deployed on guest VMs in the zone.

The functional behavior of the NetScaler with CloudStack is the same as described in the CloudStack documentation for using an F5 external load balancer. The only exception is that the F5 supports routing domains, and NetScaler does not. NetScaler can not yet be used as a firewall.

The Citrix NetScaler comes in three varieties. The following table summarizes how these variants are treated in CloudStack.

NetScaler ADC Type	Description of Capabilities	CloudStack Supported Features
MPX	Physical appliance. Capable of deep packet inspection. Can act as application firewall and load balancer	In advanced zones, load balancer functionality fully supported without limitation. In basic zones, static NAT, elastic IP (EIP), and elastic load balancing (ELB) are also provided
VPX	Virtual appliance. Can run as VM on XenServer, ESXi, and Hyper-V hypervisors. Same functionality as MPX	Supported only on ESXi. Same functional support as for MPX. CloudStack will treat VPX and MPX as the same device type
SDX	Physical appliance. Can create multiple fully isolated VPX instances on a single appliance to support multi-tenant usage	CloudStack will dynamically provision, configure, and manage the lifecycle of VPX instances on the SDX. Provisioned instances are added into CloudStack automatically – no manual configuration by the administrator is required. Once a VPX instance is added into CloudStack, it is treated the same as a VPX on an ESXi host.

13.8.2. Configuring SNMP Community String on a RHEL Server

The SNMP Community string is similar to a user id or password that provides access to a network device, such as router. This string is sent along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device discards the request and does not respond.

The NetScaler device uses SNMP to communicate with the VMs. You must install SNMP and configure SNMP Community string for a secure communication between the NetScaler device and the RHEL machine.

1. Ensure that you installed SNMP on RedHat. If not, run the following command:

   ```
   yum install net-snmp-utils
   ```

2. Edit the /etc/snmp/snmpd.conf file to allow the SNMP polling from the NetScaler device.
   a. Map the community name into a security name (local and mynetwork, depending on where the request is coming from):

   
   注記

   Use a strong password instead of public when you edit the following table.

   ```
   #         sec.name   source         community
   com2sec    local      localhost      public
   com2sec   mynetwork   0.0.0.0        public
   ```

   
   注記

Setting to 0.0.0.0 allows all IPs to poll the NetScaler server.

b. Map the security names into group names:

```
#      group.name   sec.model  sec.name
group   MyRWGroup     v1         local
group   MyRWGroup     v2c        local
group   MyROGroup     v1        mynetwork
group   MyROGroup     v2c       mynetwork
```

c. Create a view to allow the groups to have the permission to:

```
incl/excl subtree mask view all included .1
```

d. Grant access with different write permissions to the two groups to the view you created.

```
# context     sec.model     sec.level     prefix     read     write     notif
  access      MyROGroup ""  any noauth     exact      all      none     none
  access      MyRWGroup ""  any noauth     exact      all      all      all
```

3. Unblock SNMP in iptables.

```
iptables -A INPUT -p udp --dport 161 -j ACCEPT
```

4. Start the SNMP service:

```
service snmpd start
```

5. Ensure that the SNMP service is started automatically during the system startup:

```
chkconfig snmpd on
```

13.8.3. 外部ファイアウォールとロードバランサーの初期セットアップ

When the first VM is created for a new account, CloudStack programs the external firewall and load balancer to work with the VM. The following objects are created on the firewall:

- A new logical interface to connect to the account's private VLAN. The interface IP is always the first IP of the account's private subnet (e.g. 10.1.1.1).
- A source NAT rule that forwards all outgoing traffic from the account's private VLAN to the public Internet, using the account's public IP address as the source address
- A firewall filter counter that measures the number of bytes of outgoing traffic for the account

The following objects are created on the load balancer:

- A new VLAN that matches the account's provisioned Zone VLAN
- A self IP for the VLAN. This is always the second IP of the account's private subnet (e.g. 10.1.1.2).

13.8.4. Ongoing Configuration of External Firewalls and Load Balancers

Additional user actions (e.g. setting a port forward) will cause further programming of the firewall and load balancer. A user may request additional public IP addresses and forward traffic received at these IPs to specific VMs. This is accomplished by enabling static NAT for a public IP address, assigning the IP to a VM, and specifying a set of protocols and port ranges to open. When a static NAT rule is created, CloudStack programs the zone's external firewall with the following objects:

- A static NAT rule that maps the public IP address to the private IP address of a VM.
- A security policy that allows traffic within the set of protocols and port ranges that are specified.
- A firewall filter counter that measures the number of bytes of incoming traffic to the public IP.

The number of incoming and outgoing bytes through source NAT, static NAT, and load balancing rules is measured and saved on each external element. This data is collected on a regular basis and stored in the CloudStack database.

13.8.5. Configuring AutoScale

AutoScaling allows you to scale your back-end services or application VMs up or down seamlessly and automatically according to the conditions you define. With AutoScaling enabled, you can ensure that the number of VMs you are using seamlessly scale up when demand increases, and automatically decreases when demand subsides. Using AutoScaling, you can automatically shut down instances you don't need, or launch new instances, depending on demand.

NetScaler AutoScaling is designed to seamlessly launch or terminate VMs based on user-defined conditions. Conditions for triggering a scaleup or scaledown action can vary from a simple use case like monitoring the CPU usage of a server to a complex use case of monitoring a combination of server's responsiveness and its CPU usage. For example, you can configure AutoScaling to launch an additional VM whenever CPU usage exceeds 80 percent for 15 minutes, or to remove a VM whenever CPU usage is less than 20 percent for 30 minutes.

CloudStack uses the NetScaler load balancer to monitor all aspects of a system's health and work in unison with CloudStack to initiate scale-up or scale-down actions.

注記

AutoScale is supported on NetScaler Release 10 Build 73.e and beyond.

事前準備

Before you configure an AutoScale rule, consider the following:

- Ensure that the necessary template is prepared before configuring AutoScale. When a VM is deployed by using a template and when it comes up, the application should be up and running.

  注記

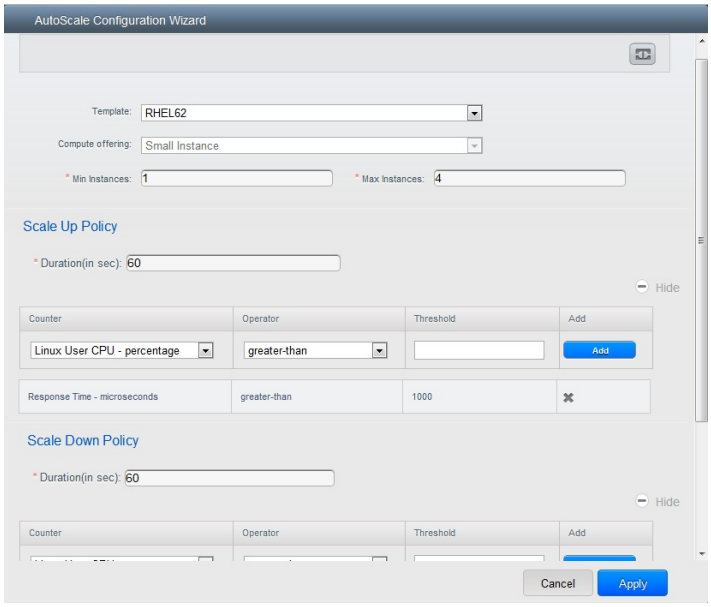
  If the application is not running, the NetScaler device considers the VM as ineffective and continues provisioning the VMs unconditionally until the resource limit is exhausted.

- Deploy the templates you prepared. Ensure that the applications come up on the first boot and is ready to take the traffic. Observe the time requires to deploy the template. Consider this time when you specify the quiet time while configuring AutoScale.
- The AutoScale feature supports the SNMP counters that can be used to define conditions for taking scale up or scale down actions. To monitor the SNMP-based counter, ensure that the SNMP agent is installed in the template used for creating the AutoScale VMs, and the SNMP operations work with the configured SNMP community and port by using standard SNMP managers. For example, see 「Configuring SNMP Community String on a RHEL Server」 to configure SNMP on a RHEL machine.
- Ensure that the endpointe.url parameter present in the Global Settings is set to the Management Server API URL. For example, http://10.102.102.22:8080/client/api. In a multi-node Management Server deployment, use the virtual IP address configured in the load balancer for the management server's cluster. Additionally, ensure that the NetScaler device has access to this IP address to provide AutoScale support.

  If you update the endpointe.url, disable the AutoScale functionality of the load balancer rules in the system, then enable them back to reflect the changes. For more information see Updating an AutoScale Configuration
- If the API Key and Secret Key are regenerated for an AutoScale user, ensure that the AutoScale functionality of the load balancers that the user participates in are disabled and then enabled to reflect the configuration changes in the NetScaler.
- In an advanced Zone, ensure that at least one VM should be present before configuring a load balancer rule with AutoScale. Having one VM in the network ensures that the network is in implemented state for configuring AutoScale.

Configuration

以下の要素を指定します。



- **Template**: A template consists of a base OS image and application. A template is used to provision the new instance of an application on a scaleup action. When a VM is deployed from a template, the VM can start taking the traffic from the load balancer without any admin intervention. For example, if the VM is deployed for a Web service, it should have the Web server running, the database connected, and so on.
- **Compute offering**: A predefined set of virtual hardware attributes, including CPU speed, number of CPUs, and RAM size, that the user can select when creating a new virtual machine instance. Choose one of the compute offerings to be used while provisioning a VM instance as part of scaleup action.
- **Min Instance**: The minimum number of active VM instances that is assigned to a load balancing rule. The active VM instances are the application instances that are up and serving the traffic, and are being load balanced. This parameter ensures that a load balancing rule has at least the configured number of active VM instances are available to serve the traffic.

  注記

  If an application, such as SAP, running on a VM instance is down for some reason, the VM is then not counted as part of Min Instance parameter, and the AutoScale feature initiates a scaleup action if the number of active

VM instances is below the configured value. Similarly, when an application instance comes up from its earlier down state, this application instance is counted as part of the active instance count and the AutoScale process initiates a scaledown action when the active instance count breaches the Max instance value.

- **Max Instance**: Maximum number of active VM instances that **should be assigned to** a load balancing rule. This parameter defines the upper limit of active VM instances that can be assigned to a load balancing rule.

  Specifying a large value for the maximum instance parameter might result in provisioning large number of VM instances, which in turn leads to a single load balancing rule exhausting the VM instances limit specified at the account or domain level.

注記

If an application, such as SAP, running on a VM instance is down for some reason, the VM is not counted as part of Max Instance parameter. So there may be scenarios where the number of VMs provisioned for a scaleup action might be more than the configured Max Instance value. Once the application instances in the VMs are up from an earlier down state, the AutoScale feature starts aligning to the configured Max Instance value.

Specify the following scale-up and scale-down policies:

- **Duration**: The duration, in seconds, for which the conditions you specify must be true to trigger a scaleup action. The conditions defined should hold true for the entire duration you specify for an AutoScale action to be invoked.
- **Counter**: The performance counters expose the state of the monitored instances. By default, CloudStack offers four performance counters: Three SNMP counters and one NetScaler counter. The SNMP counters are Linux User CPU, Linux System CPU, and Linux CPU Idle. The NetScaler counter is ResponseTime. The root administrator can add additional counters into CloudStack by using the CloudStack API.
- **Operator**: The following five relational operators are supported in AutoScale feature: Greater than, Less than, Less than or equal to, Greater than or equal to, and Equal to.
- **Threshold**: Threshold value to be used for the counter. Once the counter defined above breaches the threshold value, the AutoScale feature initiates a scaleup or scaledown action.
- **Add**: Click Add to add the condition.

Additionally, if you want to configure the advanced settings, click Show advanced settings, and specify the following:

- **Polling interval**: Frequency in which the conditions, combination of counter, operator and threshold, are to be evaluated before taking a scale up or down action. The default polling interval is 30 seconds.
- **Quiet Time**: This is the cool down period after an AutoScale action is initiated. The time includes the time taken to complete provisioning a VM instance from its template and the time taken by an application to be ready to serve traffic. This quiet time allows the fleet to come up to a stable state before any action can take place. The default is 300 seconds.
- **Destroy VM Grace Period**: The duration in seconds, after a scaledown action is initiated, to wait before the VM is destroyed as part of scaledown action. This is to ensure graceful close of any pending sessions or transactions being served by the VM marked for destroy. The default is 120 seconds.
- **Security Groups**: Security groups provide a way to isolate traffic to the VM instances. A security group is a group of VMs that filter their incoming and outgoing traffic according to a set of rules, called ingress and egress rules. These rules filter network traffic according to the IP address that is attempting to communicate with the VM.
- **Disk Offerings**: A predefined set of disk size for primary data storage.
- **SNMP Community**: The SNMP community string to be used by the NetScaler device to query the configured counter value from the provisioned VM instances. Default is public.
- **SNMP Port**: The port number on which the SNMP agent that run on the provisioned VMs is listening. Default port is 161.
- **User**: This is the user that the NetScaler device use to invoke scaleup and scaledown API calls to the cloud. If no option is specified, the user who configures AutoScaling is applied. Specify another user name to override.
- **Apply**: Click Apply to create the AutoScale configuration.

Disabling and Enabling an AutoScale Configuration

If you want to perform any maintenance operation on the AutoScale VM instances, disable the AutoScale configuration. When the AutoScale configuration is disabled, no scaleup or scaledown action is performed. You can use this downtime for the maintenance activities. To disable the AutoScale configuration, click the Disable AutoScale  button.

The button toggles between enable and disable, depending on whether AutoScale is currently enabled or not. After the maintenance operations are done, you can enable the AutoScale configuration back. To enable, open the AutoScale configuration page again, then click the Enable AutoScale  button.

Updating an AutoScale Configuration

You can update the various parameters and add or delete the conditions in a scaleup or scaledown rule. Before you update an AutoScale configuration, ensure that you disable the AutoScale load balancer rule by clicking the Disable AutoScale button.

After you modify the required AutoScale parameters, click Apply. To apply the new AutoScale policies, open the AutoScale configuration page again, then click the Enable AutoScale button.

Runtime Considerations

- An administrator should not assign a VM to a load balancing rule which is configured for AutoScale.
- Before a VM provisioning is completed if NetScaler is shutdown or restarted, the provisioned VM cannot be a part of

- Before a VM provisioning is completed if NetScaler is shutdown or restarted, the provisioned VM cannot be a part of the load balancing rule though the intent was to assign it to a load balancing rule. To workaround, rename the AutoScale provisioned VMs based on the rule name or ID so at any point of time the VMs can be reconciled to its load balancing rule.
- Making API calls outside the context of AutoScale, such as destroyVM, on an autoscaled VM leaves the load balancing configuration in an inconsistent state. Though VM is destroyed from the load balancer rule, NetScaler continues to show the VM as a service assigned to a rule.

13.9. 負荷分散のルール

CloudStack ユーザーもしくは管理者はパブリックIPから1つもしくは複数の仮想マシンへの受信トラフィックの分散のため負荷分散ルールを作成するかもしれません。ユーザーは特定のアルゴリズムに基づきルールを作成し仮想マシンのセットに対して割り当てます。

注記

もし、負荷分散ルールを作成する際 NetScaler のような外部デバイスを含んだネットワークサービスオファリングを利用していた場合、また後にネットワークサービスオファリングを CloudStack の仮想ルーターを利用するよう変更を加える場合、継続して機能を利用するためには全ての負荷分散ルールに対しファイアウォールルールを追加しなければなりません。

13.9.1. ロードバランサールールの追加

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. トラフィックの負荷分散をしたいしたいネットワークの名前をクリックします。
4. [View IP Addresses] をクリックします。
5. ルールを作成したい IP アドレスをクリックし、[Configuration] タブをクリックします。
6. 構成図のロードバランサーをクリックし、[View All] をクリックします。
   基本ゾーンでは IP アドレスを選択せずに負荷分散ルールを作成することもできます。 CloudStack は負荷分散ルールの作成時に内部的に IP を割り当て、ルール作成時に割り当てられた IP アドレスがリスト表示されます。
   ネットワークの名前を選択し、[Add Load Balancer] タブをクリックします。詳細は 7 を参照してください。
7. 次の項目を入力します。
   - **Name :** 負荷分散ルールの名前です。
   - **Public Port :** 負荷分散のための入力トラフィックを受信するポート番号です。
   - **Private Port :** 仮想マシンがトラフィックを受信するポート番号です。
   - **Algorithm :** CloudStack で利用したい負荷分散アルゴリズムを選択します。 CloudStack では様々なアルゴリズムをサポートしています。 これらのアルゴリズムに関して詳細を知りたい場合はインターネット上でより多くの情報を取得できます。
   - **Stickiness :** (オプション) [Configure] をクリックし、スティックネスポリシーを選択します。詳細は「Sticky Session Policies for Load Balancer Rules」を参照してください。
   - **AutoScale**: [Configure] をクリックし「Configuring AutoScale」に従ってオートスケールの設定を完了します。
8. [Add VMs] をクリックした後入力トラフィックの負荷を分散する2つ以上の仮想マシンを選択し、[Apply] をクリックします。
   新しい負荷分散ルールがリスト表示され、IP アドレスに対する負荷分散ルールを引き続き追加することができます。

13.9.2. Sticky Session Policies for Load Balancer Rules

Sticky sessions are used in Web-based applications to ensure continued availability of information across the multiple requests in a user's session. For example, if a shopper is filling a cart, you need to remember what has been purchased so far. The concept of "stickiness" is also referred to as persistence or maintaining state.

Any load balancer rule defined in CloudStack can have a stickiness policy. The policy consists of a name, stickiness method, and parameters. The parameters are name-value pairs or flags, which are defined by the load balancer vendor. The stickiness method could be load balancer-generated cookie, application-generated cookie, or source-based. In the source-based method, the source IP address is used to identify the user and locate the user's stored data. In the other methods, cookies are used. The cookie generated by the load balancer or application is included in request and response URLs to create persistence. The cookie name can be specified by the administrator or automatically generated. A variety of options are provided to control the exact behavior of cookies, such as how they are generated and whether they are cached.

For the most up to date list of available stickiness methods, see the CloudStack UI or call listNetworks and check the SupportedStickinessMethods capability.

13.10. Guest IP Ranges

The IP ranges for guest network traffic are set on a per-account basis by the user. This allows the users to configure their network in a fashion that will enable VPN linking between their guest network and their clients.

13.11. 新しい IP アドレスの取得

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 変更したいネットワークの名前をクリックします。

4. [View IP Addresses] をクリックします。
5. [Acquire New IP] をクリックし、確認ダイアログで [Yes] をクリックします。
   一般的に IP アドレスは有限のリソースであるため確認を求められます。しばらくするとステータスが「Allocated」となり新しい IP アドレスが表示されます。これで新しい IP アドレスをポートフォワーディングやスタティック NAT ルールに利用できます。

13.12. IP アドレスの開放

When the last rule for an IP address is removed, you can release that IP address. The IP address still belongs to the VPC; however, it can be picked up for any guest network again.

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 変更したいネットワークの名前をクリックします。
4. [View IP Addresses] をクリックします。
5. 開放したい IP アドレスをクリックします。
6. Click the Release IP button. 

13.13. 静的 NAT

A static NAT rule maps a public IP address to the private IP address of a VM in order to allow Internet traffic into the VM. The public IP address always remains the same, which is why it is called “static” NAT. This section tells how to enable or disable static NAT for a particular IP address.

13.13.1. スタティック NAT の有効化、無効化

もし、すでにポートフォワーディングのルールが IP アドレスに反映されている場合、IP に対してスタティック NAT を有効化することができません。

仮想マシンがいくつかのネットワークに所属している場合、スタティック NAT のルールは デフォルトネットワークでしか機能しません。

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 変更したいネットワークの名前をクリックします。
4. [View IP Addresses] をクリックします。
5. 変更したい IP アドレスをクリックします。
6. Click the Static NAT  button.
   The button toggles between Enable and Disable, depending on whether static NAT is currently enabled for the IP address.
7. If you are enabling static NAT, a dialog appears where you can choose the destination VM and click Apply.

13.14. IP Forwarding and Firewalling

By default, all incoming traffic to the public IP address is rejected. All outgoing traffic from the guests is also blocked by default.

To allow outgoing traffic, follow the procedure in 「Creating Egress Firewall Rules in an Advanced Zone」.

To allow incoming traffic, users may set up firewall rules and/or port forwarding rules. For example, you can use a firewall rule to open a range of ports on the public IP address, such as 33 through 44. Then use port forwarding rules to direct traffic from individual ports within that range to specific ports on user VMs. For example, one port forwarding rule could route incoming traffic on the public IP's port 33 to port 100 on one user VM's private IP. For more information, see 「ファイアウォールルール」 and 「ポート転送」.

13.14.1. Creating Egress Firewall Rules in an Advanced Zone

注記

The egress firewall rules are supported only on virtual routers.

The egress traffic originates from a private network to a public network, such as the Internet. By default, the egress traffic is blocked, so no outgoing traffic is allowed from a guest network to the Internet. However, you can control the egress traffic in an Advanced zone by creating egress firewall rules. When an egress firewall rule is applied, the traffic specific to the rule is allowed and the remaining traffic is blocked. When all the firewall rules are removed the default policy, Block, is applied.

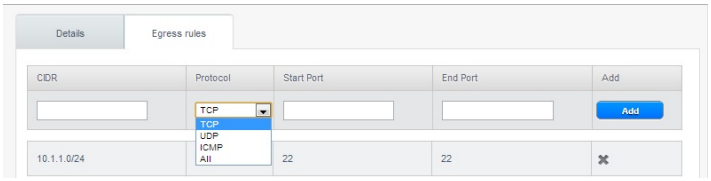
Consider the following scenarios to apply egress firewall rules:

- Allow the egress traffic from specified source CIDR. The Source CIDR is part of guest network CIDR.
- Allow the egress traffic with destination protocol TCP,UDP,ICMP, or ALL.
- Allow the egress traffic with destination protocol and port range. The port range is specified for TCP, UDP or for ICMP type and code.

To configure an egress firewall rule:

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。

2. 左側のナビゲーションから [Network] を選択します。
3. In Select view, choose Guest networks, then click the Guest network you want.
4. To add an egress rule, click the Egress rules tab and fill out the following fields to specify what type of traffic is allowed to be sent out of VM instances in this guest network:



   - **CIDR**: (Add by CIDR only) To send traffic only to the IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the destination. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
   - **Protocol**: The networking protocol that VMs uses to send outgoing traffic. The TCP and UDP protocols are typically used for data exchange and end-user communications. The ICMP protocol is typically used to send error messages or network monitoring data.
   - **Start Port, End Port**: (TCP, UDP only) A range of listening ports that are the destination for the outgoing traffic. If you are opening a single port, use the same number in both fields.
   - **ICMP Type, ICMP Code**: (ICMP only) The type of message and error code that are sent.
5. [Add]をクリックします。

13.14.2. ファイアウォールルール

デフォルトではパブリック IP に対する全ての入力トラフィックはファイアウォールで排除されます。外部からのトラフィックを許可するには特定のファイアウォールルールによりファイアウォールのポートを開放することができます。また、オプションとして接続元 IP をフィルタリングするため CIDR を指定することもできます。これは特定の IP アドレスからの入力リクエストのみを許可する場合に有効です。

エラスティックな IP アドレスに対してポートを開放するためにファイアウォールルールを利用することはできません。エラスティック IP を使用している際は外部からのアクセスは代わりにセキュリティグループにより制御します。詳細は「セキュリティグループの追加」 を参照してください。

拡張ゾーンでは仮想ルーターを用いて出力用ファイアウォールルールを作成できます。詳細は「Creating Egress Firewall Rules in an Advanced Zone」 を参照してください。

ファイアウォールのルールは管理サーバー UI の [Firewall] タブから作成することができます。このタブは CloudStack がインストールされた時点ではデフォルトで表示されません。[Firewall] タブを表示するには CloudStack 管理者がグローバル設定パラメーターで「firewall.rule.ui.enabled」を "true" に設定する必要があります。

ファイアウォールルールの作成方法

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 変更したいネットワークの名前をクリックします。
4. [View IP Addresses] をクリックします。
5. 変更したい IP アドレスをクリックします。
6. [Configuration] タブをクリクし次の値を入力します。
   - **Source CIDR :** (オプション) 特定のアドレスブロックに含まれる IP アドレスのみを許可するには CIDR かカンマで区切られた CIDR のリストを入力します。 例として 192.168.0.0/22 などが挙げられます。また、空欄にすると全ての CIDR を許可します。
   - **Protocol :** 開放されたポートで利用される通信プロトコルです。
   - **Start Port と End Port :** ファイアウォールで開放したいポート番号です。単一のポートを開放したい場合、両方のフィールドに同一の番号を入力してください。
   - **ICMP Type と ICMP Code :** プロトコルに ICMP を設定した場合のみ利用されます。ICMP プロトコルにおいて必要な ICMP ヘッダーに埋め込まれるタイプとコードを入力してください。何を入力するべきか詳細に関しては「ICMP ドキュメント」を参照してください。
7. [Add]をクリックします。

13.14.3. ポート転送

ポート転送サービスは、ポリシーを定義するポート転送規則のセットです。ポート転送サービスは、1 台または複数のゲスト仮想マシンに適用されます。これにより、ゲスト仮想マシンに、ポート転送サービスで定義するポリシーに従って管理される受信ネットワークアクセス権が付与されます。オプションで、CIDR を指定して送信元 IP アドレスをフィルターすることもで きます。これは、特定の IP アドレスからの受信要求の転送のみを許可する場合に役立ちます。

任意の数のポート転送サービスを、ゲスト仮想マシンに適用できます。ポート転送サービスは定義できますが、メンバーを持つものではありません。

エラスティック IP に対してはポートを開放するためにポート転送を利用することができません。エラスティック IP を使っている場合は代わりにセキュリティグループを使って外部からのアクセスをコントロールします。詳細は「セキュリティグループ」を参照してください。

ポート転送を設定するには

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. もし、完了しない場合は CloudStack でパブリック IP アドレスの範囲をゾーンに追加します。詳細はインストールガイドの「ゾーンとポッドの追加」を参照してください。

3. 1 台または複数のゲスト仮想マシンを CloudStack に追加してください。
4. 左側のナビゲーションバーで[Network]をクリックします。
5. 仮想マシンを実行しているゲストネットワークの名前をクリックします。
6. 既存の IP アドレスを選択するか、新しい IP アドレスを取得します(「新しい IP アドレスの取得」 を参照)。一覧内の IP アドレスをクリックします。
7. [Configuration]タブをクリックします。
8. ダイアグラムの[Port Forwarding]ノードの[View All]をクリックします。
9. 次の項目を入力します。
   - **Public Port :** パブリックトラフィックが送信される、前の手順で取得した IP アドレスのポートです。
   - **Private Port :** 転送されたパブリックトラフィックをインスタンスがリッスンするポートです。
   - **Protocol**: 2 つのポートの間で使用される通信プロトコルです。
10. [Add]をクリックします。

13.15. IP Load Balancing

The user may choose to associate the same public IP for multiple guests. CloudStack implements a TCP-level load balancer with the following policies.

- ラウンドロビン
- Least connection
- Source IP

This is similar to port forwarding but the destination may be multiple IP addresses.

13.16. DNSと DHCP

The Virtual Router provides DNS and DHCP services to the guests. It proxies DNS requests to the DNS server configured on the Availability Zone.

13.17. VPN

CloudStack アカウントの所有者は、仮想マシンにアクセスするためのVPN(Virtual Private Network:仮想プライベートネットワーク)を作成できます。リモートアクセス VPN サービスを提供するネットワークオファリングからゲストネットワークのインスタンスを作成すると、システム仮想マシンに基づいて、仮想ルーターによってサービスが提供されます。\nCloudStack は、L2TP over IPsec ベースのリモートアクセス VPN サービ スをゲスト仮想ネットワークに提供します。各ネットワークに仮想ルー\nターがあるため、VPN はネットワーク間で共有されません。Windows、Mac OS X、および iOS のネイティブ VPN クライアントを使用して、ゲストネットワークに接続できます。アカウント所有者は VPN ユーザーを作成して管理することができます。このために、CloudStack のアカウントデータベースではなく別のテーブルが使用されます。VPN ユーザーデータベースは、 特定のアカウント所有者が作成するすべての VPN で共有されます。すべての VPN ユーザーはそのアカウント所有者が作成するすべての VPN にアクセスできます。

注記

トラフィックのすべてが VPN を経由するわけ はないことに注意してください。つまり、 VPN によって構築されるルートはゲストネットワーク専用にする必要があり、すべてのトラフィックに使用できるわけではありません。

- **モバイルユーザー/リモートアクセス :** ユーザーは、自宅または事務所からクラウド内のプライベートネットワークに安全に接続することを望んでいます。通常、接続するクライアントの IP アドレスは動的であり、VPN サーバーで事前構成することはできません。
- **Site to Site**. In this scenario, two private subnets are connected over the public Internet with a secure VPN tunnel. The cloud user's subnet (for example, an office network) is connected through a gateway to the network in the cloud. The address of the user's gateway must be preconfigured on the VPN server in the cloud. Note that although L2TP-over-IPsec can be used to set up Site-to-Site VPNs, this is not the primary intent of this feature. For more information, see 「Setting Up a Site-to-Site VPN Connection」

13.17.1. VPN の構成

クラウドの VPN をセットアップするには

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションバーで [Global Settings] をクリックします。
3. 次のグローバル構成パラメーターを設定します。
   - remote.access.vpn.client.ip.range – The range of IP addresses to be allocated to remote access VPN clients. The first IP in the range is used by the VPN server.
   - remote.access.vpn.psk.length – IPSec キーの長さです。
   - remote.access.vpn.user.limit – アカウントあたりの VPN ユーザーの最大数です。

特定のネットワークの VPN を有効にするには

1. ユーザーまたは管理者として CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションバーで[Network]をクリックします。
3. 設定するネットワークの名前をクリックします。
4. [View IP Addresses] をクリックします。
5. 表示される IP アドレスの 1 つをクリックします。
6. [Enable VPN]アイコンをクリックします。 

ポップアップウィンドウに IPsec キーが表示されます。

13.17.2. Windows での VPN の使用方法

VPN を使用する手順は、Windows のバージョンによって異なります。一般に、ユーザーは VPN プロパティを編集し、デフォルトのルートが VPN ではないことを確認する必要があります。次の手順は Windows Vista 上の Windows L2TP クライアントを対象にしています。ほかのバージョンの Windows でもコマンドは同様のはずです。

1. CloudStack ユーザーインターフェイスにログオンして、アカウントの送信元 NAT IP アドレスをクリックします。[VPN] タブに IPsec 事前共有キーが表示されます。これと送信元 NAT IP アドレスを記録します。ユーザーインターフェイスに、ユーザーとパスワードも表示されます。ユーザーを選択するか、ユーザーが存在しない場合はユーザーとパスワードを追加します。
2. Windows コンピューターでコントロールパネルの[ネットワークと共有センター]を開きます。[接続またはネットワークのセットアップ]をクリックします。
3. 次に開くダイアログボックスで、[いいえ]をクリックして新しい接続を作成します。
4. 次に開くダイアログボックスで、[インターネット接続(VPN)を使用します]をクリックします。
5. In the next dialog, enter the source NAT IP from step 1 and give the connection a name. Check Don't connect now.
6. In the next dialog, enter the user name and password selected in step 1.
7. [Create] をクリックします。
8. コントロールパネルに戻り、[ネットワーク接続]をクリックして新しい接続を表示します。接続はまだアクティブになっていません。
9. 新しい接続を右クリックし、[プロパティ]を選択します。[プロパティ]ダイアログボックスで[ネットワーク]タブをクリックします。
10. In Type of VPN, choose L2TP IPsec VPN, then click IPsec settings. Select Use preshared key. Enter the preshared key from Step 1.
11. これで、接続をアクティブにする準備ができました。コントロールパネルに戻り、[ネットワーク接続]を開いて作成した接続をダブルクリックします。
12. Enter the user name and password from Step 1.

13.17.3. Using VPN with Mac OS X

First, be sure you've configured the VPN settings in your CloudStack install. This section is only concerned with connecting via Mac OS X to your VPN.

Note, these instructions were written on Mac OS X 10.7.5. They may differ slightly in older or newer releases of Mac OS X.

1. On your Mac, open System Preferences and click Network.
2. Make sure Send all traffic over VPN connection is not checked.
3. If your preferences are locked, you'll need to click the lock in the bottom left-hand corner to make any changes and provide your administrator credentials.
4. You will need to create a new network entry. Click the plus icon on the bottom left-hand side and you'll see a dialog that says "Select the interface and enter a name for the new service." Select VPN from the Interface drop-down menu, and "L2TP over IPSec" for the VPN Type. Enter whatever you like within the "Service Name" field.
5. You'll now have a new network interface with the name of whatever you put in the "Service Name" field. For the purposes of this example, we'll assume you've named it "CloudStack." Click on that interface and provide the IP address of the interface for your VPN under the Server Address field, and the user name for your VPN under Account Name.
6. Click Authentication Settings, and add the user's password under User Authentication and enter the pre-shared IPSec key in the Shared Secret field under Machine Authentication. Click OK.
7. You may also want to click the "Show VPN status in menu bar" but that's entirely optional.
8. Now click "Connect" and you will be connected to the CloudStack VPN.

13.17.4. Setting Up a Site-to-Site VPN Connection

A Site-to-Site VPN connection helps you establish a secure connection from an enterprise datacenter to the cloud infrastructure. This allows users to access the guest VMs by establishing a VPN connection to the virtual router of the account from a device in the datacenter of the enterprise. Having this facility eliminates the need to establish VPN connections to individual VMs.

The supported endpoints on the remote datacenters are:

- Cisco ISR with IOS 12.4 or later
- Juniper J-Series routers with JunOS 9.5 or later

注記

In addition to the specific Cisco and Juniper devices listed above, the expectation is that any Cisco or Juniper device running on the supported operating systems are able to establish VPN connections.

To set up a Site-to-Site VPN connection, perform the following:

1. Create a Virtual Private Cloud (VPC).
   See 「VPC の構成」.
2. Create a VPN Customer Gateway.
3. Create a VPN gateway for the VPC that you created.
4. Create VPN connection from the VPC VPN gateway to the customer VPN gateway.

注記

Appropriate events are generated on the CloudStack UI when status of a Site-to-Site VPN connection changes from connected to disconnected, or vice versa. Currently no events are generated when establishing a VPN connection fails or pending.

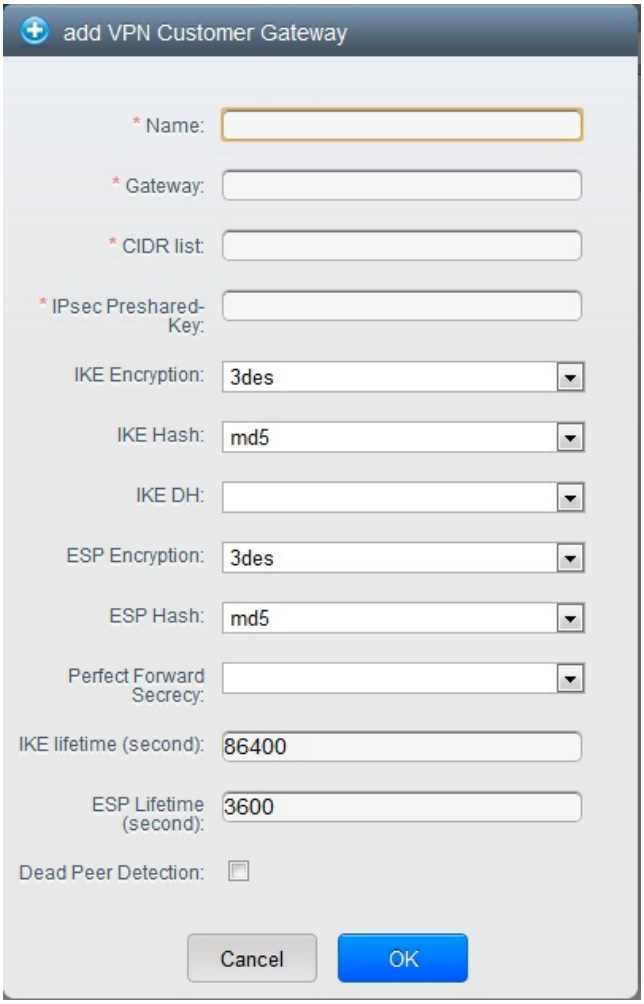
13.17.4.1. Creating and Updating a VPN Customer Gateway

注記

A VPN customer gateway can be connected to only one VPN gateway at a time.

To add a VPN Customer Gateway:

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. In the Select view, select VPN Customer Gateway.
4. Click Add site-to-site VPN.



次の情報を指定します。

- **Name**: A unique name for the VPN customer gateway you create.
- **Gateway**: The IP address for the remote gateway.
- **CIDR list**: The guest CIDR list of the remote subnets. Enter a CIDR or a comma-separated list of CIDRs. Ensure that a guest CIDR list is not overlapped with the VPC's CIDR, or another guest CIDR. The CIDR must be RFC1918-compliant.
- **IPsec Preshared Key**: Preshared keying is a method where the endpoints of the VPN share a secret key. This key value is used to authenticate the customer gateway and the VPC VPN gateway to each other.

注記

The IKE peers (VPN end points) authenticate each other by computing and sending a keyed hash of data that includes the Preshared key. If the receiving peer is able to create the same hash independently by using its Preshared key, it knows that both peers must share the same secret, thus authenticating the customer gateway.

- **IKE Encryption**: The Internet Key Exchange (IKE) policy for phase-1. The supported encryption algorithms are AES128, AES192, AES256, and 3DES. Authentication is accomplished through the Preshared Keys.

  注記

  The phase-1 is the first phase in the IKE process. In this initial negotiation phase, the two VPN endpoints agree on the methods to be used to provide security for the underlying IP traffic. The phase-1 authenticates the two VPN gateways to each other, by confirming that the remote gateway has a matching Preshared Key.

- **IKE Hash**: The IKE hash for phase-1. The supported hash algorithms are SHA1 and MD5.
- **IKE DH**: A public-key cryptography protocol which allows two parties to establish a shared secret over an insecure communications channel. The 1536-bit Diffie-Hellman group is used within IKE to establish session keys. The supported options are None, Group-5 (1536-bit) and Group-2 (1024-bit).
- **ESP Encryption**: Encapsulating Security Payload (ESP) algorithm within phase-2. The supported encryption algorithms are AES128, AES192, AES256, and 3DES.

  注記

  The phase-2 is the second phase in the IKE process. The purpose of IKE phase-2 is to negotiate IPSec security associations (SA) to set up the IPSec tunnel. In phase-2, new keying material is extracted from the Diffie-Hellman key exchange in phase-1, to provide session keys to use in protecting the VPN data flow.

- **ESP Hash**: Encapsulating Security Payload (ESP) hash for phase-2. Supported hash algorithms are SHA1 and MD5.
- **Perfect Forward Secrecy**: Perfect Forward Secrecy (or PFS) is the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised. This property enforces a new Diffie-Hellman key exchange. It provides the keying material that has greater key material life and thereby greater resistance to cryptographic attacks. The available options are None, Group-5 (1536-bit) and Group-2 (1024-bit). The security of the key exchanges increase as the DH groups grow larger, as does the time of the exchanges.

  注記

  When PFS is turned on, for every negotiation of a new phase-2 SA the two gateways must generate a new set of phase-1 keys. This adds an extra layer of protection that PFS adds, which ensures if the phase-2 SA's have expired, the keys used for new phase-2 SA's have not been generated from the current phase-1 keying material.

- **IKE Lifetime (seconds)**: The phase-1 lifetime of the security association in seconds. Default is 86400 seconds (1 day). Whenever the time expires, a new phase-1 exchange is performed.
- **ESP Lifetime (seconds)**: The phase-2 lifetime of the security association in seconds. Default is 3600 seconds (1 hour). Whenever the value is exceeded, a re-key is initiated to provide a new IPsec encryption and authentication session keys.
- **Dead Peer Detection**: A method to detect an unavailable Internet Key Exchange (IKE) peer. Select this option if you want the virtual router to query the liveliness of its IKE peer at regular intervals. It's recommended to have the same configuration of DPD on both side of VPN connection.

5. 「OK」をクリックします。

Updating and Removing a VPN Customer Gateway

You can update a customer gateway either with no VPN connection, or related VPN connection is in error state.

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. In the Select view, select VPN Customer Gateway.
4. Select the VPN customer gateway you want to work with.
5. To modify the required parameters, click the Edit VPN Customer Gateway button 
6. To remove the VPN customer gateway, click the Delete VPN Customer Gateway button 
7. 「OK」をクリックします。

13.17.4.2. VPC での VPN ゲートウェイの作成

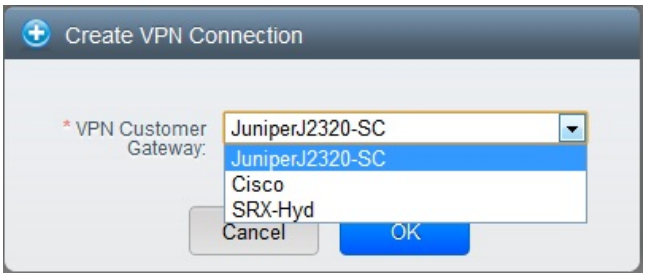
1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。

- IP アドレス
- ゲートウェイ
- サイト間 VPN
- ネットワーク ACL

6. サイト間 VPN を選択します。
   既に VPN ゲートウェイを作成している場合は表示された VPN ゲートウェイからサイト間 VPN を選択します。
7. 確認ダイアログで [Yes] を選択します。
   しばらく経つと VPN ゲートウェイが作成されます。その後、作成したVPN ゲートウェイの詳細が表示されます。
   次に [Yes] をクリックします。
   VPN ゲートウェイ情報ページでは以下の詳細情報が表示されます。
   - IP アドレス
   - アカウント
   - ドメイン

13.17.4.3. VPC 接続の作成

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対し作成した全ての VPC がページに表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. サイト間 VPN を選択します。
   サイト間 VPN のページが表示されます。
7. セレクトビューのドロップダウンから VPN 接続を選択します。
8. [Create VPN Connection] をクリックします。
   VPN 接続のダイアログが表示されます。



9. 必要なカスタマーゲートウェイを選択し、 [OK] をクリックします。
   しばらくすると VPN 接続が表示されます。
   VPN 接続に関して以下の情報が表示されます。
   - IP アドレス
   - ゲートウェイ
   - 状態
   - IPSec の事前共有鍵
   - IKE 規則
   - ESP 規則

13.17.4.4. VPN 接続の再起動と削除

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. サイト間 VPN を選択します。

サイト間 VPN のページが表示されます。

7. セレクトビューのドロップダウンから VPN 接続を選択します。
   作成した全ての VPN 接続が表示されます。
8. 対象となる VPN 接続を選択します。
   [詳細] タブが表示されます。
9. VPN 接続を削除するには [Delete VPN Connection] ボタンをクリックします。

   VPN 接続を再起動するには [詳細] タブにある [Reset VPN Connection] ボタンをクリックします。

13.18. About Inter-VLAN Routing

Inter-VLAN Routing is the capability to route network traffic between VLANs. This feature enables you to build Virtual Private Clouds (VPC), an isolated segment of your cloud, that can hold multi-tier applications. These tiers are deployed on different VLANs that can communicate with each other. You provision VLANs to the tiers your create, and VMs can be deployed on different tiers. The VLANs are connected to a virtual router, which facilitates communication between the VMs. In effect, you can segment VMs by means of VLANs into different networks that can host multi-tier applications, such as Web, Application, or Database. Such segmentation by means of VLANs logically separate application VMs for higher security and lower broadcasts, while remaining physically connected to the same device.

This feature is supported on XenServer and VMware hypervisors.

The major advantages are:

- The administrator can deploy a set of VLANs and allow users to deploy VMs on these VLANs. A guest VLAN is randomly alloted to an account from a pre-specified set of guest VLANs. All the VMs of a certain tier of an account reside on the guest VLAN allotted to that account.

  注記

  A VLAN allocated for an account cannot be shared between multiple accounts.

- The administrator can allow users create their own VPC and deploy the application. In this scenario, the VMs that belong to the account are deployed on the VLANs allotted to that account.
- Both administrators and users can create multiple VPCs. The guest network NIC is plugged to the VPC virtual router when the first VM is deployed in a tier.
- The administrator can create the following gateways to send to or receive traffic from the VMs:

  VPN Gateway: For more information, see 「VPC での VPN ゲートウェイの作成」.

  Public Gateway: The public gateway for a VPC is added to the virtual router when the virtual router is created for VPC. The public gateway is not exposed to the end users. You are not allowed to list it, nor allowed to create any static routes.

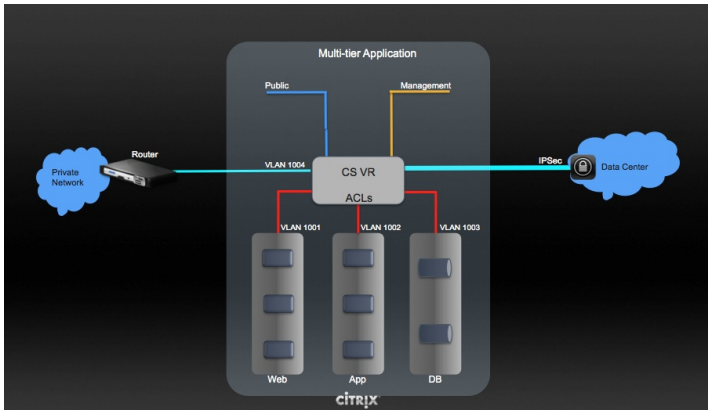
  Private Gateway: For more information, see 「VPC へのプライベートゲートウェイの追加」.
- Both administrators and users can create various possible destinations-gateway combinations. However, only one gateway of each type can be used in a deployment.

  For example:

  VLANs and Public Gateway: For example, an application is deployed in the cloud, and the Web application VMs communicate with the Internet.

  VLANs, VPN Gateway, and Public Gateway: For example, an application is deployed in the cloud; the Web application VMs communicate with the Internet; and the database VMs communicate with the on-premise devices.
- The administrator can define Access Control List (ACL) on the virtual router to filter the traffic among the VLANs or between the Internet and a VLAN. You can define ACL based on CIDR, port range, protocol, type code (if ICMP protocol is selected) and Ingress/Egress type.

The following figure shows the possible deployment scenarios of a Inter-VLAN setup:



To set up a multi-tier Inter-VLAN deployment, see 「VPC の構成」.

13.19. VPC の構成

13.19.1. VPC(Virtual Private Cloud) の概要

CloudStack 仮想プライベートクラウドは CloudStack の機能の一部です。 VPC は一般的な物理ネットワークに似た独自の仮想ネットワークトポロジを持ち、ユーザーはプライベードアドレスを持つ仮想マシンをその仮想ネットワーク上で起動することができます。例: 10.0.0.0/16。 IP のアドレス範囲に準じた仮想マシングループに対し VPC のネットワークを有効化し、層を定義することができます。

例として、VPC がプライベートなアドレス範囲である 10.0.0.0/16 を持っていた場合、ゲストネットワークは 10.0.1.0/24, 10.0.2.0/24, 10.0.3.0/24 といったアドレスを持つことができます。

VPC の主要コンポーネント。

VPC は以下のネットワークコンポーネントから構成されます。

- **VPC**: VPC は仮想ルーターを介し通信することができる、複数の独立したネットワークのコンテナとして動作します。
- **Network Tiers**: 各層はそれぞれ独立したネットワークとして VLAN 情報やCIDR情報を持ち、VLAN によってセグメント化されます。各層の NIC はゲートウェイとして動作します。
- **Virtual Router**: 仮想ルーターは自動的に作成され VPC 作成とともに起動します。仮想ルーターは各層とパブリックなゲートウェイから受信する直接のトラフィック、VPN ゲートウェイ、NAT インスタンスに接しています。各層は NIC や 仮想ルーターの IP と連携しDNS や DHCP といったサービスを提供します。
- **Public Gateway**: インターネットと VPC との通信はパブリックゲートウェイを介して処理されます。VPC ではパブリックゲートウェイはエンドユーザーに対し不可視であるため静的ルーティングはパブリックゲートウェイではサポートされていません。
- **Private Gateway**: プライベートネットワークと VPC との通信は全てルーティングされます。詳細な情報は 「VPC へのプライベートゲートウェイの追加」 を参照して下さい。
- **VPN Gateway**: VPC に付与される VPN 接続です。
- **Site-to-Site VPN Connection**: VPC とデータセンターやホームネットワーク、コロケーション環境とを接続するハードウェアベースの VPN 接続です。詳細な情報は 「Setting Up a Site-to-Site VPN Connection」 を参照して下さい。
- **Customer Gateway**: VPN 接続の利用者側ゲートウェイです。詳細な情報は 「Creating and Updating a VPN Customer Gateway」 を参照して下さい。
- **NAT Instance**: インターネットからパブリックゲートウェイを介しての仮想マシンアクセスのためのポートアドレス転送を提供するインスタンスです。詳細な情報は 「VPC での静的 NAT の有効化、無効化」 を参照して下さい。

VPC のネットワークアーキテクチャ

VPC では次のネットワークアーキテクチャの基本的なオプションが提供されます。

- パブリックゲートウェイのみの VPC
- パブリック、プライベートゲートウェイを持つ VPC
- パブリック、プライベートゲートウェイとサイト間 VPN アクセスを持つ VPC
- プライベートゲートウェイのみとサイト間 VPN アクセスを持つ VPC

VPC の接続オプション

次のように VPC に接続することができます。

- パブリックゲートウェイを介してインターネットから接続。
- VPN ゲートウェイを介しサイト間 VPN 接続を利用して会社のデータセンターから接続
- パブリックゲートウェイと VPN ゲートウェイを利用してインターネット、会社のデータセンター双方から接続

VPC ネットワークの考慮点

VPC を作成する前に次のことを考慮しておきます。

- VPC はデフォルトで作成された際に有効化されます。
- VPC は拡張ゾーンでのみ作成可能で、同時に複数ゾーンに所属させることは出来ません。
- デフォルトの VPC の作成可能数はアカウント毎に20個です。しかし、グローバル設定の max.account.vpcs を変更することでアカウント毎に作成可能な VPC の最大数を制御することができます。
- デフォルトの VPC 上の層の作成可能数はアカウント毎に3個です。vpc.max.networks を変更することで最大数を制御することができます。
- 各層は VPC 上で一意な CIDR を設定すべきです。また、層の CIDR は VPC の CIDR 内に収まっているべきです。
- 層は単一の VPC にのみ所属します。
- VPC 内の全てのネットワーク層は同一アカウントに紐付けられるべきです。
- デフォルトでは VPC が作成された際、送信元 NAT 用 IP が割り当てられます。送信元 NAT 用 IP は VPC が削除された時のみ開放されます。
- パブリック IP は同時に1つだけ利用することができます。IP が送信元 NAT 用である場合静的 NAT や ポート転送用に割り当てることはできません。
- 展開された仮想マシンはプライベート IP のみ利用することができます。インターネットへの通信を行う場合、展開した VPC で仮想マシンに対しての NAT を有効化する必要があります。
- 新しいネットワークのみが VPC に対して追加できます。VPC 毎のネットワークの最大値は vpc.max.networks によって制限されており、デフォルト値は3です。
- 負荷分散サービスは VPC 内の単一の層に対してのみサポートされます。
- 層に IP アドレスが割り当てられた場合

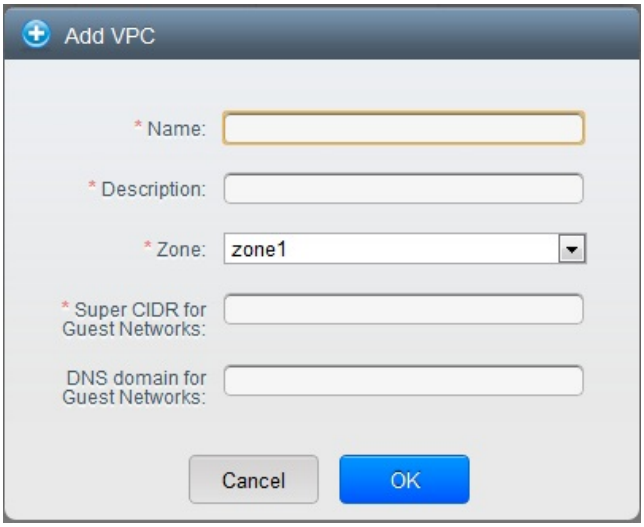
  IP は VPC 内の複数の層で同時に利用することはできません。例としてA層とB層を持ちパブリック IPを1つ持っている場合、IP を用いたポート転送ルールはA、Bに対し作成することはできますが双方同時には作成できません。

  IP は VPC 内の他のゲストネットワークに対しての静的NATや負荷分散、ポート転送ルールに利用できません。
- リモートアクセス VPN は VPCではサポートされていません。

13.19.2. VPC の追加

VPC を作成する場合、ゾーンと VPC 対しての IP アドレスが必要になります。この際、クラスレス内部ドメインルーティングを CIDR のブロックとして指定する必要があります。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
4. [Add VPC] をクリックすると VPC 追加ページでは以下の情報が表示されます。



次の情報を指定します。

- **Name**: 作成した VPC の名称です。
- **Description**: VPC の詳細情報です。
- **Zone**: VPC を利用可能にしたいゾーンを選択します。
- **Super CIDR for Guest Networks**: VPC における全ての層(ゲストネットワーク)に対する CIDR を定義します。層を作成した際はそれが入力したスーパー CIDR の内部に所属することを確認します。また、CIDR が RFC1918 を満たしていることを確認します。
- **DNS domain for Guest Networks**: 特別なドメイン名を割り当てたい場合には DNS サフィックスを指定します。このパラメーターは VPC 上の全ての層に対し適用され、これは VPC 上に作成された全ての層は同じ DNS ドメインに所属することを意味します。パラメーターを指定しない場合は DNS 名は自動的に生成されます。

13.19.3. 層の追加

層は VPC 上で明確に区別でき各ネットワークを分離しデフォルトで他の層とのアクセスを禁止します。層は異なった VLAN 上に構成され仮想ルーターを介することで互いに通信することができます。層は VPC 上に他の層に対し安価で低遅延のネットワーク接続を提供します。

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページ上にリスト表示されます。

> **注記**
>
> エンドユーザーはそれぞれの VPC を確認することができ、ROOT管理者やドメイン管理者は権限を許可されている全ての VPC を確認することができます。

4. セットアップしたい層を含む VPC の [Configure] ボタンをクリックします。
   次のように層の追加ダイアログが表示されます。

既に層を作成済みの場合 VPC のダイアログが表示されるので新しい層を追加するため [Create Tier] をクリックします。

5. 以下の要素を指定します。
   全ての項目が必須となります。
   - **Name**: 作成した層に対する唯一の名前です。
   - **Network Offering**: 以下のデフォルトのネットワークオファリングがリスト表示されます。DefaultIsolatedNetworkOfferingForVpcNetworksNoLB, DefaultIsolatedNetworkOfferingForVpcNetworks。
     VPC では LB-enabled ネットワークオファリングだけが作成されます。
   - **Gateway**: 作成された層のゲートウェイです。VPC 作成時に指定したスーパー CIDR 内に収まり、VPC 内の他の層と重複しないことを確認します。
   - **Netmask**: 作成された層のネットマスクです。
     例として、もし VPC の CIDR を10.0.0.0/16とした場合、層の CIDR は10.0.1.0/24となり、ゲートウェイは 10.0.1.1 となります。またその際のネットマスクは255.255.255.0となります。
6. 「OK」をクリックします。
7. 層のアクセス制御リストを設定する場合は引き続き設定を続けます。

13.19.4. Configuring Access Control List

Define Network Access Control List (ACL) on the VPC virtual router to control incoming (ingress) and outgoing (egress) traffic between the VPC tiers, and the tiers and Internet. By default, all incoming and outgoing traffic to the guest networks is blocked. To open the ports, you must create a new network ACL. The network ACLs can be created for the tiers only if the NetworkACL service is supported.

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
5. Select Network ACLs.
   The Network ACLs page is displayed.
6. Click Add Network ACLs.
   To add an ACL rule, fill in the following fields to specify what kind of network traffic is allowed in this tier.
   - **CIDR**: The CIDR acts as the Source CIDR for the Ingress rules, and Destination CIDR for the Egress rules. To accept traffic only from or to the IP addresses within a particular address block, enter a CIDR or a comma-separated list of CIDRs. The CIDR is the base IP address of the incoming traffic. For example, 192.168.0.0/22. To allow all CIDRs, set to 0.0.0.0/0.
   - **Protocol**: The networking protocol that sources use to send traffic to the tier. The TCP and UDP protocols are typically used for data exchange and end-user communications. The ICMP protocol is typically used to send error messages or network monitoring data.
   - **Start Port**, **End Port** (TCP, UDP only): A range of listening ports that are the destination for the incoming traffic. If you are opening a single port, use the same number in both fields.
   - **Select Tier**: Select the tier for which you want to add this ACL rule.
   - **ICMP Type**, **ICMP Code** (ICMP only): The type of message and error code that will be sent.
   - **Traffic Type**: Select the traffic type you want to apply.
     Egress: To add an egress rule, select Egress from the Traffic type drop-down box and click Add. This specifies what type of traffic is allowed to be sent out of VM instances in this tier. If no egress rules are specified, all traffic from the tier is allowed out at the VPC virtual router. Once egress rules are specified, only the traffic specified in egress rules and the responses to any traffic that has been allowed in through an ingress rule are allowed out. No egress rule is required for the VMs in a tier to communicate with each other.
     Ingress: To add an ingress rule, select Ingress from the Traffic type drop-down box and click Add. This specifies what network traffic is allowed into the VM instances in this tier. If no ingress rules are specified, then no traffic will be allowed in, except for responses to any traffic that has been allowed out through an egress rule.

注記

By default, all incoming and outgoing traffic to the guest networks is blocked. To open the ports, create a new network ACL.

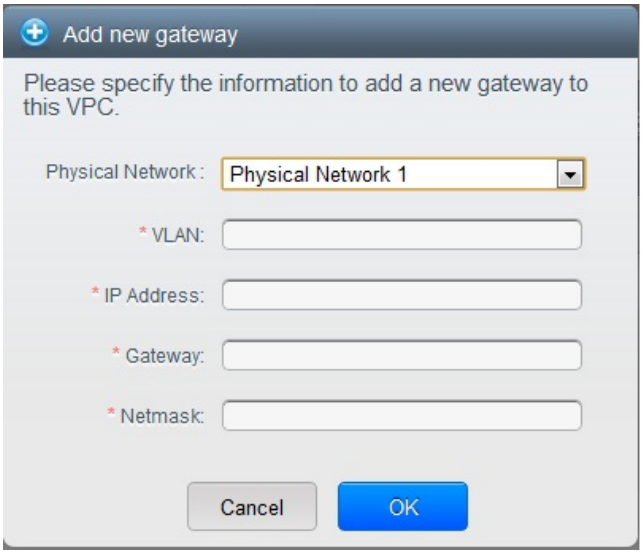
7. Click Add. The ACL rule is added.
   To view the list of ACL rules you have added, click the desired tier from the Network ACLs page, then select the Network ACL tab.

You can edit the tags assigned to the ACL rules and delete the ACL rules you have created. Click the appropriate button in the Actions column.

13.19.5. VPC へのプライベートゲートウェイの追加

プライベートゲートウェイはルート管理者のみ追加することができます。VPCのプライベートネットワークは物理ネットワークの NIC と1対1の関係があり、同一データセンター上でゲートウェイを持たない重複しない VLAN や IP が許容されます。

1. 管理者もしくはエンドユーザーとして CloudStack UI にログインします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 負荷分散ルールを構成したい VPC の構成ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - プライベートゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. プライベートゲートウェイを選択します。
   ゲートウェイのページに表示されます。
7. [Add new gateway]をクリックします。



8. 以下の要素を指定します。
   - **物理ネットワーク**: \nゾーンに作成された物理ネットワークです。
   - **IP アドレス**: \nVPC ゲートウェイに割り当てられた IP アドレスです。
   - **ゲートウェイ**: \nトラフィックが VPC に対し(もしくは VPC から)ルーティングされるゲートウェイです。
   - **ネットマスク**: \nVPC ゲートウェイに割り当てられた IP に対してのネットマスクです。
   - **VLAN**: \nVPC ゲートウェイに割り当てられた VLAN です。

   新しいゲートウェイがリスト上に表示されます。VPC に対しゲートウェイを追加するためこれらの手順を繰り返すこともできます。

13.19.6. 層への仮想マシンの展開

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。

4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC のページが表示され作成済みの全ての層がリスト表示されます。
5. 仮想マシンを追加したい層で [Add VM] ボタンをクリックします。
   インスタンスの追加ページが表示されます。
   この場面でインスタンスを追加するにはページの指示に従います。インスタンスの追加に関してはインストールガイドの「インスタンスの追加」の章を参照して下さい。

13.19.7. VPC に対しての新しい IP アドレスの取得

IP アドレスを取得するとゲストネットワークを除く全ての IP アドレスが VPC に割り当てられます。ゲストネットワークへの IP アドレスは IP やネットワークに対して初めてポート転送、負荷分散、静的NATルールを作成した際に割り当てられます。また、IP は複数のネットワークに対して同時には割り当てることができません。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから [VPC] を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. IP アドレスを選択します。
   IP アドレスのページが表示されます。
7. [Acquire New IP] をクリックし、確認ダイアログで [Yes] をクリックします。
   一般的に IP アドレスは限りあるリソースであるため確認用ページが表示されます。しばらく経つと状態が [Allocated] に変化し新しい IP アドレスが表示されます。これでポート転送や負荷分散、静的NATルールに対し IP アドレスを利用することができます。

13.19.8. VPC に割り当てられた IP アドレスの開放

IP アドレスは限られたリソースであり、特定の IP をこれ以上利用することが無い場合は VPC から IP を開放し利用可能アドレスのプールに返却することができます。IP アドレスに対し全てのネットワーク機能(ポート転送、負荷分散、静的NATルール)を削除している場合には層から IP アドレスを開放することができます。ここで開放された IP アドレスは同一の VPC に属し続けます。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 開放したい IP を持つ VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. IP アドレスを選択します。
   IP アドレスのページが表示されます。
7. 開放したい IP をクリックします。
8. 詳細タブで [Release IP] ボタンをクリックします。 

13.19.9. VPC での静的 NAT の有効化、無効化

静的 NAT ルールは VPC 内の仮想マシンに割り当てられたプライベート IP に対しインターネットからのトラフィックを渡すためパブリック IP と関連付けられます。この章では VPC 上の特定 IP アドレスに対してどのように静的 NAT の有効化、無効化するか説明しています。

もし、すでにポートフォワーディングのルールが IP アドレスに反映されている場合、IP に対して静的 NAT を有効化することができません。

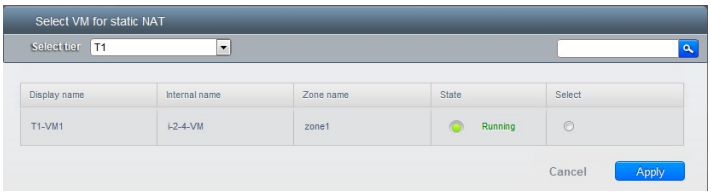
仮想マシンがいくつかのネットワークに所属している場合、静的 NAT のルールは デフォルトネットワークでしか機能しません。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。

以下のオプションが表示されます。

- IP アドレス
- ゲートウェイ
- サイト間 VPN
- ネットワーク ACL

6. IP アドレスを選択します。
   IP アドレスのページが表示されます。
7. 設定したい IP をクリックします。
8. 詳細タブで [Static NAT] ボタンをクリックします。  ボタンは有効、無効のトグルボタンになっており、表示される状態は IP アドレスに対して現在静的 NAT が有効化されているかどうかによって変化します。
9. 静的 NAT を有効化すると以下のようなダイアログが表示されます。



10. 層と対象となる仮想マシンを選択して [Apply] ボタンを押して下さい。

13.19.10. VPC への負荷分散ルールの追加

CloudStack のユーザーや管理者はパブリック IP で受信されたトラフィックを負荷分散サービスが提供されているネットワーク層に所属する複数の仮想マシンに対して負荷分散するためのルールを作成することができます。ユーザーはアルゴリズムに基づいたルールを作成し、それらのルールを VPC 内の仮想マシンに割り当てることができます。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 負荷分散ルールを構成したい VPC の構成ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. IP アドレスを選択します。
   IP アドレスのページが表示されます。
7. ルールを作成したい IP アドレスをクリックし、[Configuration] タブをクリックします。
8. 構成図のロードバランサーをクリックし、[View All] をクリックします。
9. ルールを適用したい層を選択します。

> **注記**
>
> VPC 内では単一の層に対して負荷分散サービスがサポートされます。

10. 以下の要素を指定します。
    - **Name :** 負荷分散ルールの名前です。
    - **Public Port**: 負荷分散用に受信されるトラッフィク用ポート
    - **Private Port :** 仮想マシンがトラフィックを受信するポート番号です。
    - **Algorighm**\nCloudStack で利用したい負荷分散アルゴリズムを選択します。以下のアルゴリズムがサポートされます。
      ラウンドロビン
      直近での接続
      接続元
    - **Stickness**. (オプション) Click Configure and choose the algorithm for the stickiness policy. See Sticky Session Policies for Load Balancer Rules.\n[Configure] をクリックし、スティックネス規則用のアルゴリズムを選択します。負荷分散ルール用スティッキーセッション規則を参照して下さい。
    - **Add VMs**: Click Add VMs, then select two or more VMs that will divide the load of incoming traffic, and click Apply.\n[Add VMs] をクリックし受信トラフィックを負荷分散したい2つ以上の仮想マシンを選択します。その後、[Apply] をクリックします。

新しい負荷分散ルールがリスト表示され、さらに IP アドレスに対しての負荷分散ルールを追加することができます。

13.19.11. VPC へのポート転送ルールの追加

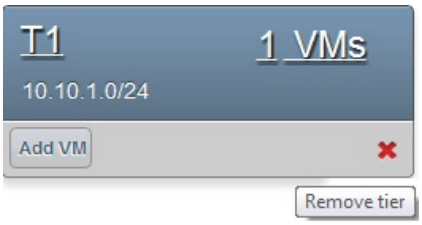
1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。

2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 仮想マシンを展開したい VPC の [Configure] ボタンをクリックします。
   VPC ページではダイアグラム上にリストされる作成された全ての層が表示されます。
5. 設定アイコンをクリックします。
   以下のオプションが表示されます。
   - IP アドレス
   - ゲートウェイ
   - サイト間 VPN
   - ネットワーク ACL
6. 既存の IP アドレスを選択するか新しい IP アドレスを取得します。リスト表示された IP アドレス名をクリックします。
   IP アドレスのページが表示されます。
7. ルールを作成したい IP アドレスをクリックし、[Configuration] タブをクリックします。
8. ダイアグラムの[Port Forwarding]ノードの[View All]をクリックします。
9. ルールを適用したい層を選択します。
10. 以下の要素を指定します。
    - **Public Port**: The port to which public traffic will be addressed on the IP address you acquired in the previous step.以前の手順で取得したどの IP アドレスへのパブリックトラフィックを受信するポートを指定します。
    - **Private Port**: 仮想マシンが転送されたパブリックトラッフィクをリッスンするポートを指定します。
    - **Protocol**: それぞれのポートで利用する通信プロトコルを指定します。
      TCP
      UDP
    - **Add VM**: [Add VM] をクリックします。その後、ルールを適用したい仮想マシン名を選択し [Apply] をクリックします。
      仮想マシンへの ssh セッションを作成することでルールをテストすることができます。

13.19.12. 層の削除

VPC から層を削除することができ、削除された層は無効化することができません。層を削除した場合、層に設定したリソースのみ削除されます。全てのネットワークルール(ポート転送や負荷分散、静的 NAT など)と IP アドレスは削除された層に割り当てられたままになります。その際、IP アドレスは VPC に所属し続けます。

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページ上にリスト表示されます。
4. 層を設定したい VPC の [Configure] ボタンをクリックします。
   VPC の設定画面が表示され、設定したい層の情報が表示されます。
5. [Remove VPC] ボタンをクリックします。



層を削除するにはしばらく待ちます。

13.19.13. VPC の編集と再起動、削除

注記

VPC 削除前の全ての層の確認

1. 管理者またはユーザーとして CloudStack ユーザーインターフェイスにログオンします。
2. 左側のナビゲーションから [Network] を選択します。
3. 選択ビューから VPC を選択します。
   アカウントに対して作成された全ての VPC がページにリスト表示されます。
4. 対象の VPC を選択します。
5. 削除するには [Remove VPC] ボタンをクリックします。 

   VPCの名前と詳細情報を編集することができ、それには VPC を選択し [Edit] ボタンをクリックします。 

   To restart a VPC, select the VPC, then click the Restart button.  i

13.20. Persistent Networks

The network that you can provision without having to deploy any VMs on it is called a persistent network. A persistent network can be part of a VPC or a non-VPC environment.

When you create other types of network, a network is only a database entry until the first VM is created on that network. When the first VM is created, a VLAN ID is assigned and the network is provisioned. Also, when the last VM is destroyed, the VLAN ID is released and the network is no longer available. With the addition of persistent network, you will have the ability to create a network in CloudStack in which physical devices can be deployed without having to run any VMs. Additionally, you can deploy physical devices on that network.

One of the advantages of having a persistent network is that you can create a VPC with a tier consisting of only physical devices. For example, you might create a VPC for a three-tier application, deploy VMs for Web and Application tier, and use physical machines for the Database tier. Another use case is that if you are providing services by using physical hardware, you can define the network as persistent and therefore even if all its VMs are destroyed the services will not be discontinued.

13.20.1. Persistent Network Considerations

- Persistent network is designed for isolated networks.
- All default network offerings are non-persistent.
- A network offering cannot be editable because changing it affects the behavior of the existing networks that were created using this network offering.
- When you create a guest network, the network offering that you select defines the network persistence. This in turn depends on whether persistent network is enabled in the selected network offering.
- An existing network can be made persistent by changing its network offering to an offering that has the Persistent option enabled. While setting this property, even if the network has no running VMs, the network is provisioned.
- An existing network can be made non-persistent by changing its network offering to an offering that has the Persistent option disabled. If the network has no running VMs, during the next network garbage collection run the network is shut down.
- When the last VM on a network is destroyed, the network garbage collector checks if the network offering associated with the network is persistent, and shuts down the network only if it is non-persistent.

13.20.2. Creating a Persistent Guest Network

To create a persistent network, perform the following:

1. Create a network offering with the Persistent option enabled.
   See the Administration Guide.
2. Select Network from the left navigation pane.
3. Select the guest network that you want to offer this network service to.
4. Click the Edit button.
5. From the Network Offering drop-down, select the persistent network offering you have just created.
6. [OK]をクリックします。

Revision History

改訂 1-0	**October 5 2012**	**Tomechak Jessica [FAMILY Given], PC Radhika [FAMILY Given], den Hollander Wido [FAMILY Given]**
	Initial publication	